(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2024 (12.12.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/253795 A1

(51) International Patent Classification:
G06F 21/31 (2013.01) *G06V 40/16* (2022.01)

(21) International Application Number:
PCT/US2024/028362

(22) International Filing Date:
08 May 2024 (08.05.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
18/328,957 05 June 2023 (05.06.2023) US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US]; 1680 Capital One Drive, McLean, Virginia 22102 (US).

(72) Inventors: **PRIBBLE, Jason**; 1680 Capital One Drive, McLean, Virginia 22102 (US). **PATIL, Swapnil**; 1680 Capital One Drive, McLean, Virginia 22102 (US). **NEIGHBOUR, Erik**; 1680 Capital One Drive, McLean, Virginia 22102 (US).

(74) Agent: **UNDERWOOD, Steven D.**; 11350 Random Hills Road, Suite 600, Fairfax, Virginia 22030 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV,

(54) Title: ENHANCED AUTHENTICATION USING A SECURE DOCUMENT

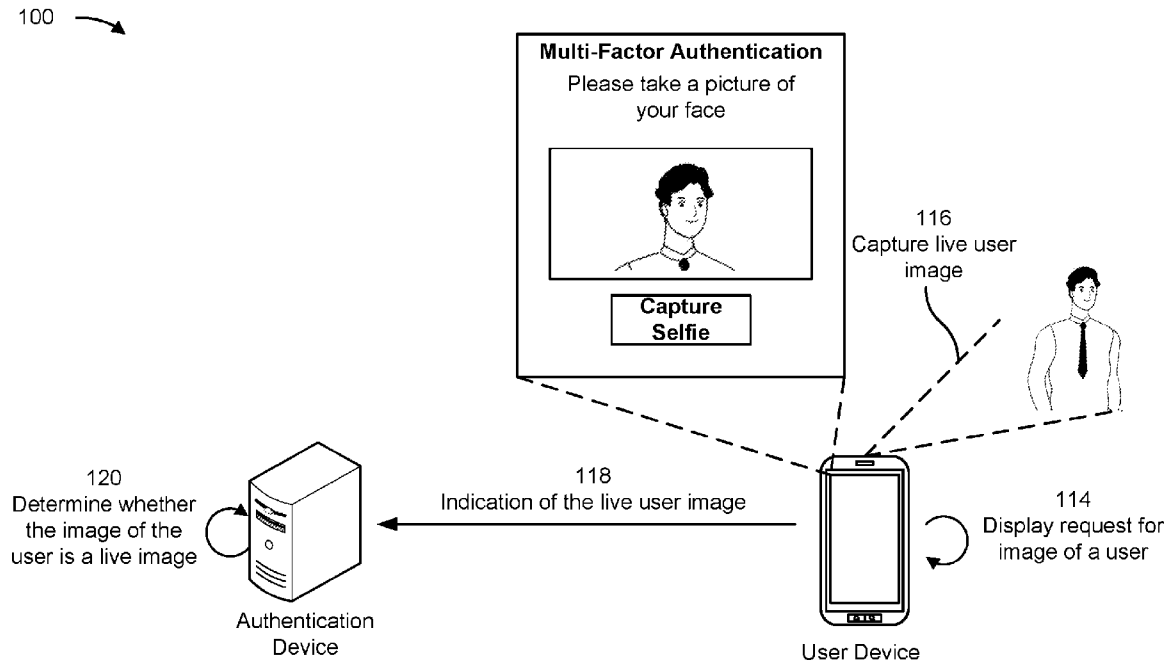

FIG. 1C

(57) Abstract: In some implementations, a device may obtain a document that includes an identification image depicting a face of a person associated with the document. The device may obtain a live user image that depicts an image of a user. The device may extract information from the document image that includes appearance information associated with the person. The appearance information may include one or more document appearance parameters. The device may analyze the identification image, the live user image, and the appearance information to determine whether the user is the person to which the document is issued. The device may perform an action based on determining whether the user is the person to which the document is issued.

WO 2024/253795 A1

[Continued on next page]

GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

ENHANCED AUTHENTICATION USING A SECURE DOCUMENT

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Nonprovisional Patent Application No. 18/328,957, filed on June 5, 2023, entitled "ENHANCED AUTHENTICATION USING A SECURE DOCUMENT," which is hereby expressly incorporated by reference herein.

BACKGROUND

[0002] An authentication process may be performed for various purposes. For example, if a user attempts to gain access to an account associated with the user, the authentication process may be performed to verify an identity of the user to enable the user to access the account.

SUMMARY

[0003] Some implementations described herein relate to a system for enhanced authentication using image analysis of an identification document and appearance information associated with the identification document. The system may include one or more memories and one or more processors communicatively coupled to the one or more memories. The one or more processors may be configured to detect an authentication event associated with an access attempt for an account. The one or more processors may be configured to obtain a document image based on detecting the authentication event, the document image being an image of the identification document. The one or more processors may be configured to obtain a live user image associated with the authentication event based on detecting the authentication event, the live user image being a live image of the user. The one or more processors may be configured to extract information from the document image, the information including the appearance information associated with the document, the appearance information including one or more document appearance parameters. The one or more processors may be configured to analyze, using a machine learning model, the document image, the live user image, and the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document, the analyzing including determining whether the live user image depicts the one or more document appearance parameters. The one or more processors may be configured to authenticate the access attempt based on the confidence score satisfying a threshold.

[0004] Some implementations described herein relate to a method of image analysis of an identification document and appearance information associated with the identification document. The method may include obtaining, by a device, a document image, the document being the identification

document, and the document including an identification image depicting a face of a person associated with the document. The method may include obtaining, by the device, a live user image, the live user image being a live image of the user. The method may include extracting, by the device, information from the document image, the information including appearance information associated with the person, the appearance information including one or more document appearance parameters. The method may include analyzing, by the device, the identification image, the live user image, and the appearance information to determine whether the user is the person to which the document is issued, the analyzing including, comparing the identification image to the live user image, and identifying whether the one or more document appearance parameters are included in the live user image. The method may include performing, by the device, an action based on determining whether the user is the person to which the document is issued.

[0005] Some implementations described herein relate to a non-transitory computer-readable medium that stores a set of instructions for a device. The set of instructions, when executed by one or more processors of the device, may cause the device to detect an authentication event associated with an access attempt for an account, the account being associated with a trusted user. The set of instructions, when executed by one or more processors of the device, may cause the device to obtain a document image based on detecting the authentication event, the document being an identification document issued by a trusted entity. The set of instructions, when executed by one or more processors of the device, may cause the device to obtain a live user image associated with the access attempt based on detecting the authentication event. The set of instructions, when executed by one or more processors of the device, may cause the device to extract information from the document image, the information including appearance information associated with the document, the appearance information including one or more document appearance parameters. The set of instructions, when executed by one or more processors of the device, may cause the device to analyze the document image, the live user image, and the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document. The set of instructions, when executed by one or more processors of the device, may cause the device to authenticate the access attempt based on the confidence score satisfying a threshold.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Figs. 1A-1E are diagrams of an example associated with enhanced authentication using a secure document, in accordance with some embodiments of the present disclosure.

[0007] Fig. 2 is a diagram illustrating an example of training and using a machine learning model in connection with enhanced authentication using a secure document, in accordance with some embodiments of the present disclosure.

[0008] Fig. 3 is a diagram of an example environment in which systems and/or methods described herein may be implemented, in accordance with some embodiments of the present disclosure.

[0009] Fig. 4 is a diagram of example components of a device associated with enhanced authentication using a secure document, in accordance with some embodiments of the present disclosure.

[0010] Fig. 5 is a flowchart of an example process associated with enhanced authentication using a secure document, in accordance with some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0011] The following detailed description of example implementations refers to the accompanying drawings. The same reference numbers in different drawings may identify the same or similar elements.

[0012] Some actions associated with a user may be based on authentication of information associated with the user. For example, a website may use an authentication system to authenticate an identity of the user before granting the user access to the website. As an example, the authentication system may authenticate the identity of the user based on an identification document that is issued to a person, such as a driver's license. For example, multi-factor authentication (MFA) is an authentication technique in which a device of the user is granted access to a resource (e.g., a computing resource, an application, and/or a page associated with an account) only after successfully presenting two or more factors to the authentication system. The two or more factors may include knowledge (e.g., something only the user knows), possession (e.g., something only the user has), and/or inherence (e.g., something only the user is), among other examples.

[0013] For example, the authentication system may authenticate an access attempt (e.g., to access a resource) using a document, such as an identification document. In some cases, the user may provide an image of the identification document to the authentication system. The authentication system may analyze the image of the identification document to determine whether to authenticate the identity of the user. For example, the authentication system may authenticate the identity of the user based on determining that the identification document is valid or authenticate. As an example, the authentication system may read a barcode and/or a machine-readable code depicted in the identification document that encodes information that indicates whether the identification is valid or authenticate. The authentication system may decode the information to determine whether the identification document is valid or authentic.

[0014] However, in some cases, the authentication system is unable to determine whether the user that provides the image of the identification document is the person to which the identification document is issued. For example, a malicious actor may steal a valid identification document from another person and may provide the valid identification document to the authentication system. Because the identification document is valid (e.g., as indicated by the information encoded in the bar code and/or the machine-readable code), the authentication system may incorrectly authenticate the identity of the user and grant the malicious actor access to a resource.

[0015] As a result, the authentication system may consume resources (e.g., computing resources, memory resources, networking resources, and/or other resources) associated with granting the malicious actor access to a resource based on the incorrect authentication determination. For example, the authentication system may consume resources to perform a forensic examination associated with the resource to determine whether the malicious actor caused any adverse effects to the resource. As another example, the authentication system may consume resources to provide notifications associated with the improper access to the resource.

[0016] In some cases, the identification document may include an image of a person to which the identification document is issued, and the user may provide a live user image of the user (e.g., an image of a live person rather than an image of an image) to the authentication system. As an example, the authentication system may analyze the image of the person to which the document is issued and the live user image to determine whether to authenticate the identity of the user. In some cases, the authentication system may compare the image of the person to which the document is issued and the live user image to determine whether the user is the person to which the document is issued.

[0017] However, in some cases, the authentication system is unable to determine whether the user is the person to which the document is issued. For example, a malicious actor may steal an identification document from another person and may replace an original image of the person to which the document is issued with an image of the user (e.g., a live user image or an image of an image) to create an altered identification document. The user may provide the altered identification document and the live user image to the authentication system. The authentication system may incorrectly authenticate the identity of the user and grant the malicious actor access to the resource. As a result, the authentication system may consume resources associated with granting the malicious actor access to the resource based on the incorrect authentication determination.

[0018] Some implementations described herein provide enhanced authentication using a secure document. In some implementations, the secure document (also referred to as a "document" or an "identification document") may be associated with a particular person. The enhanced authentication may be based on image analysis of the document and/or information associated with the document. In some

implementations, the document may be an identification document issued to a person, such as a driver's license and/or a passport issued to the person, among other examples. As an example, the document may include an identification image that depicts a face of the person to which the document is issued.

[0019] In some implementations, a system may detect an authentication event associated with an access attempt for an account. For example, a user device may attempt to access the account by submitting credentials (e.g., submitted via a user input from a user), such as login credentials, to the system. The system may detect the login attempt as the authentication event. In some implementations, the system may transmit, and the user device may receive, a request for authentication information based on detecting the authentication event (e.g., as part of an MFA procedure associated with the access attempt). The system may obtain, from the user device, an image of the identification document based on the request for authentication information. In some implementations, the system may extract an identification image from the document, and the identification image may be an image of an owner of the document (e.g., the identification image may depict a face of a person that is a holder of the document).

[0020] In some implementations, the system may extract appearance information associated with the person to which the identification document is issued. For example, the system may extract the appearance information from text on the document, from a machine-readable code provided on the document, and/or by analyzing the identification image of the owner of the document. In some implementations, the appearance information may include one or more document appearance parameters associated with the owner of the document, such as an age, an eye color, a gender, a skin color, a facial characteristic, a weight, and/or a height, among other examples.

[0021] In some implementations, the system may obtain, from the user device, a live user image (e.g., an image that depicts a face of the user, which may be sometimes referred to as a "selfie"). In some implementations, the system may use a machine learning model to analyze the document image, the live user image, and the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document (e.g., that the user is the person to which the document is issued).

[0022] For example, the system may determine whether the user is the person to which the document is issued by comparing the identification image to the live user image (e.g., the selfie) to identify whether the one or more document appearance parameters (e.g., extracted from the machine-readable code and/or from the text on the document) are included in the live user image. In some implementations, the system may perform an action based on determining whether the user is the person to which the document is issued, such as authenticating an access attempt to the account by the user based on determining that the user is the person to which the document is issued. In some implementations, the enhanced authentication

may be based on a document that includes address information associated with an owner of the document and a device location, such as a location associated with the user device of the user.

[0023] In some implementations, the system may obtain, from the user device, location information associated with the user device. As an example, the location information may include information indicated via metadata associated with the document image and/or positioning information indicated by the user device. In some implementations, the system may determine a confidence score based on the address information and the location information. As an example, the confidence score may indicate a likelihood that the user device is associated with the owner of the document and the confidence score may be based on a correlation between the location information and the address information. In some implementations, the system may authenticate the access attempt based on the confidence score satisfying a threshold, as described in more detail elsewhere herein.

[0024] In this way, implementations described herein provide enhanced authentication techniques using a document and/or a device location, such as by indicating a likelihood that the user is the person to which the document is issued and/or by indicating a likelihood that the device is associated with the owner of the document. Because the system uses enhanced authentication techniques using the secure document, the system can determine when a valid or otherwise authenticate identification document is provided by a malicious actor. Thus, the system consumes less resources compared to other authentication techniques (e.g., by avoiding a need to perform actions associated with incorrect authentication determinations, such as forensic examination of data, generating notifications, and/or transmitting notifications associated with a malicious actor).

[0025] Figs. 1A-1E are diagrams of an example 100 associated with enhanced authentication using a secure document. As shown in Figs. 1A-1E, example 100 includes an authentication device and a user device. These devices are described in more detail in connection with Figs. 3 and 4.

[0026] In some implementations, the authentication device may be associated with an entity, such as an organization, a merchant, and/or a financial institution, that generates, provides, manages, and/or maintains an account (or other resource) associated with a user and/or that performs actions associated with the user. For example, the authentication device may be associated with an entity that generates, provides, manages, and/or maintains a credit card account, a loan account, a capital loan account, a checking account, a savings account, a reward account, a payment account, and/or a user account associated with the user, among other examples. As an example, the authentication device may authenticate an access attempt, performed by the user, to the account based on a confidence score satisfying a threshold and/or the authentication device may perform an action (e.g., authorize and/or enable an action of the user to be performed) based on determining whether the user is the person to which the document is issued, as described in more detail elsewhere herein.

[0027] As shown in Fig. 1A, and by reference number 102, the user device may obtain an indication of an access attempt associated with an account. For example, a user may attempt to access an account and/or may perform an action associated with the account. For example, the entity may be a credit card issuer that generates, provides, manages, and/or maintains a credit card account associated with the user, and the user may attempt to access the credit card account by performing a login associated with the credit card account. As an example, the user device may obtain credentials, such as login credentials, via a graphical user interface (GUI) of a website associated with the credit card issuer to perform the login associated with the credit card account.

[0028] As another example, the entity may be a merchant that operates an application that is executable on the user device of the user, such as a food delivery service application. For example, the merchant may generate, provide, manage, and/or maintain an account associated with the user. The user device may perform the action associated with the account by obtaining a payment associated with the application account, such as by obtaining credit card information into a GUI of the application associated with the application account. In other words, the attempt to access the account may include a login attempt, a payment attempt, and/or an attempt to access and/or modify information associated with the account (e.g., payment information), among other examples.

[0029] As shown by reference number 104, the authentication device may detect an authentication event. In some implementations, the authentication event may be an event that the authentication device detects that triggers the authentication device to perform an authentication protocol, as described in more detail elsewhere herein. For example, the authentication event may be associated with a multi-factor authentication protocol.

[0030] In some implementations, the authentication event may be associated with the attempt to access the account performed by the user. As an example, if the authentication device is associated with the credit card issuer and the user attempts to access the credit card account by performing the login associated with the credit card account, then the authentication device may detect the login associated with the credit card account, performed by the user, as the authentication event.

[0031] In some implementations, the authentication event may be associated with the action associated with the account performed by the user. As an example, if the authentication device is associated with the merchant that operates the application and the user performs the payment associated with the application account, then the authentication device may detect the payment, performed by the user, as the authentication event. In some implementations, the authentication event may be associated with multifactor authentication. For example, the access attempt to the account performed by the user may indicate valid login credentials, but the user may incorrectly answer a verification question. The authentication device may detect the incorrect answer provided by the user as the authentication event. In

this example, the authentication device may request an additional authentication factor from the user, such as the identification document.

[0032] As shown by reference number 106, the authentication device may transmit, and the user device may receive, a request for authentication information. For example, the authentication device may transmit, and the user device may receive, the request for the authentication information based on detecting the authentication event associated with the access attempt to the account and/or an action performed in connection with the account. In some implementations, the request for the authentication information may be based on information associated with the document, such as appearance information and/or address information. For example, the request for the authentication information may be a request for a document image to enable the authentication device to authenticate the document as a second authentication factor.

[0033] In some implementations, the document may be an identification document issued by a trusted entity (e.g., a government entity), such as a state driver's license, an identification card, a Territories driver's license, a tribal identification card that is signed by an associated bearer, a U.S. Military identification card that is signed by an associated bearer, a passport, a resident alien card, and employment authorization card, and/or a temporary resident card, among other examples. In some implementations, the document may be a check, a contract, a resume, a utility bill, and/or an envelope, among other examples.

[0034] Thus, in some implementations, the document may include information associated with the person to which the document is issued, such as appearance information and/or information associated with an image, a current address, a signature, and/or a unique identifier associated with the person to which the document is issued (e.g., the owner of the document), among other examples. In some implementations, the appearance information may be based on information that the user submits when applying for the document and may describe an appearance of the owner of the document. Thus, in some implementations, the appearance information may include one or more document appearance parameters associated with the person to which the document is issued.

[0035] As an example, the one or more document appearance parameters may include an age, an eye color, a gender, a skin color, a facial characteristic, a weight, and/or a height, among other examples, associated with the person to which the document is issued. In some implementations, the information associated with the document, such as the appearance information and/or address information, may be encoded in a machine-readable code, such as a barcode, that is provided on the document.

[0036] In some implementations, the machine-readable code may encode an image identifier associated with the identification image included in the document. As an example, the image identifier may be associated with a server that stores the identification image included in the document as a color

image, such as a high-resolution color image version of the identification image. In some implementations, the image identifier may be used to obtain the high-resolution color version of the identification image, as described in more detail elsewhere herein. In this way, if the identification image provided on the document is of poor quality and/or is a black and white image, then the authentication device may retrieve the high-resolution color version of the image for analysis, as described in more detail elsewhere herein. In this way, using the high-resolution color version of the image for analysis enables the authentication device to obtain more information and/or to obtain the information more accurately.

[0037] In some implementations, address information included in the document may be associated with the owner of the document (e.g., the address information may indicate a home address associated with the owner of the document). In some implementations, the authentication device may extract information associated with the appearance information and/or the address information from a document image and may compare the extracted information to information associated with a live user image (e.g., a selfie), as described in more detail elsewhere herein. Thus, in some implementations, the request for the authentication information may include a request for a document image and/or a request for a live user image.

[0038] In some implementations, the request for the authentication information may include an indication of a document object model (DOM) for a GUI that is associated with the authentication information. As an example, the DOM for the GUI may include a page, such as a webpage and/or a page associated with an application executing on the user device. In some implementations, the page may include an input option associated with the authentication information, such as an input option associated with capturing the document image and/or the live user image. As another example, the input option may be associated with uploading a file, such as a file that includes the document image, to the GUI via the user device. In some implementations, the authentication device may transmit, and the user device may receive, the request for the authentication information that includes the indication of the DOM for the GUI based on detecting the authentication event.

[0039] As shown in Fig. 1B, and by reference number 108, the authentication device may cause the user device to display a request for the document image. For example, the user device may display the GUI based on receiving the indication of the DOM for the GUI from the authentication device. In some implementations, the indication of the DOM for the GUI may include code for generating the GUI, and the user device may execute the code to display the GUI, such as in a web browser of the user device and/or in a page of an application executing on the user device. In some implementations, the user device may present the GUI for display to the user of the user device. As shown in Fig. 1B, the GUI may

include the input option of a "Capture" button that, when selected by a user, causes the user device to capture an image, as described in more detail elsewhere herein.

[0040] As shown by reference number 110, the user device may capture the document image. In some implementations, the user may provide an input to the user device to capture the document image. For example, the user may align a camera of the user device with the document and may press the "Capture" button on the GUI to capture the document image. Additionally, or alternatively, the user may use the user device to select an upload button (not shown) to upload the document image to the GUI.

[0041] In some implementations, the user device may generate metadata associated with the document image based on capturing the document image. As an example, the metadata associated with the document image may include geographic location information that corresponds to a location associated with the user device at a time that the document image is captured and/or timestamp information that corresponds to a time that the document image is captured, among other examples.

[0042] In some implementations, the geographic location information that corresponds to the location associated with the user device may be based on network connection information associated with the user device, such as wireless Internet connection information and/or mobile data connection information associated with the device, and/or coordinate information, such as latitude and longitude coordinates associated with a geographic location obtained by a global positioning system (GPS) of the user device. As an example, the authentication device may determine one or more locations associated with the user device based on the geographic location information, as described in more detail elsewhere herein.

[0043] As shown by reference number 112, the authentication device may obtain, and the user device may transmit, an indication of the document image. For example, the authentication device may obtain the indication of the document image from the user device based on capturing the document image. In some implementations, the user device may transmit, and the authentication device may receive, location information associated with the document image, such as the metadata associated with the document image and/or positioning information indicated by the user device. As an example, the indication of the document image may include the positioning information and the authentication device may obtain the positioning information based on receiving the indication of the document image. In some implementations, the positioning information may indicate geographic identifiers associated with a location, such as a geographical location of the device and/or an identifier associated with the device. As an example, the location may be based on GPS coordinates indicated by the user device. As another example, the identifier associated with the user device may be an internet protocol (IP) address associated with the user device.

[0044] As shown in Fig. 1C, and by reference number 114, the authentication device may cause the user device to display a request for an image of a user. For example, the user device may display the GUI

based on receiving the indication of the DOM for the GUI from the authentication device, as described above. As shown in Fig. 1C, the GUI includes the input option of a "Capture Selfie" button that the user presses to capture a live user image that depicts a face of the user, as described in more detail elsewhere herein.

[0045] As shown by reference number 116, the user device may capture the live user image. In some implementations, the user may provide an input to the user device to cause the user device to capture a live user image. For example, the user may align the camera of the user device with the face of the user and may press the "Capture Selfie" button on the GUI to capture the live user image that depicts the face of the user.

[0046] In some implementations, the user device may generate metadata associated with the live user image based on capturing the live user image. As an example, the metadata associated with the live user image generated by the user device may include geographic location information that corresponds to a location associated with the user device at a time that the live user image is captured and/or timestamp information that corresponds to a time that the live user image is captured.

[0047] As shown by reference number 118, the authentication device may obtain, from the user device, an indication of the live user image. For example, the authentication device may obtain the indication of the live user image from the user device based on capturing the image of the live user image.

[0048] As shown by reference number 120, the authentication device may determine whether the live user image is a live image (e.g., an image of a live person rather than an image of an image) of the user. In some implementations, the live user image is a live user image if the live user image is captured within a time period, such as a time period associated with a web session, an application session, and/or a capture period, among other examples. As an example, the web session may be a communication session associated with a web browser of the user device and a web server that hosts a website (e.g., a web server associated with the credit card issuer), the application session may be a communication session associated with a page of an application executing on the user device and a web server associated with the application executing on the user device (e.g., a web server associated with the food delivery service application), and/or the capture period may be a time period that includes a start time and an end time.

[0049] For example, the start time associated with the capture period may be a time when the user device initially displays the GUI, and the end time may be a subsequent time, such as five minutes after the user device initially displays the GUI. As an example, the authentication device may determine that the live user image is a live user image based on determining that the live user image is captured during the web session, during the application session, and/or at a time within the capture period. In some implementations, the authentication device may determine whether the live user image is an image of another image. For example, the authentication device may process the live user image to determine

whether the live user image is of a three-dimensional object (e.g., a person) or of a two-dimensional object (e.g., another image). In this way, the authentication device may determine when the user captures an image of an image rather than capturing the live user image.

[0050] In some implementations, the metadata associated with the live user image, generated by the user device, may include information associated with the web session, the application session, and/or the capture period. For example, the metadata associated with the live user image may include a time period associated with the web session, a time period associated with the application session, and/or the start time and the end time of the capture period.

[0051] Thus, in some implementations, the authentication device may determine whether live user image is a live user image the image by comparing the time stamp information that corresponds to the time that the live user image is captured to the information associated with the web session, the application session, and/or the capture period indicated by the metadata. For example, the authentication device may determine that the live user image is the live user image based on determining that the time that the live user image is captured is within the time period associated with the web session, the application session, and/or the capture period.

[0052] In some implementations, the authentication device may cause the "Capture Selfie" input option to be functional only during a predetermined time period, such as from a time that the user device initially displays the GUI to a subsequent time (e.g., the "Capture Selfie" input option may be function for five minutes after the user device initially displays the GUI). In this example, the authentication device may determine that the live user image is the live user image based on determining that the live user image is captured (e.g., because the Capture Selfie button is functional).

[0053] As shown in Fig. 1D, and by reference number 122, the authentication device may extract appearance information and/or address information from the document image. In some implementations, the authentication device may obtain an image of a machine-readable code included in the document image, such as by using a barcode detection technique, and may decode the machine-readable code to obtain the appearance information and/or the address information.

[0054] In some implementations, the authentication device may analyze the document image using a computer vision technique, such as an optical character recognition (OCR) technique, to obtain the appearance information and/or the address information. For example, the document image may include text that describes the appearance information and/or the address information, and the authentication device may use the OCR technique to identify and extract the appearance information and/or the address information.

[0055] In some implementations, the authentication device may decode a machine-readable code depicted (e.g., that is in the document image) to obtain the appearance information and/or the address

information. As an example, the authentication device may obtain, such as by scanning, an image of a machine-readable code that is included in the document image. The authentication device may decode the machine-readable code to obtain the appearance information and/or the address information.

[0056] In some implementations, the authentication device may determine an address location based on the address information. For example, the authentication device may use a text-parsing technique to identify an address associated with the owner of the document based on extracting the address information. In some implementations, the authentication device may perform an address geocoding technique associated with the address to determine geographic coordinates, such as latitude and longitude coordinates, based on the address.

[0057] In some implementations, the authentication device may obtain location information associated with the user device based on the information indicated via metadata associated with the image (e.g., described above) and/or the positioning information (e.g., described above) indicated by the user device. In some implementations, the authentication device may extract one or more geographic location identifiers from the information indicated via the metadata associated with the image and/or the positioning information indicated by the user device. For example, the one or more geographic location identifiers may include latitude and longitude coordinates, and the authentication device may determine a device location, such as a geographical position associated with the user device, based on the latitude and longitude coordinates.

[0058] In some implementations, the authentication device may determine a location distance that is a distance between the address location and the device location. As an example, if the distance between the address location and the device location is thirty miles, then the authentication device may determine that the location distance is thirty miles. As an example, the authentication device may determine a correlation between the location information and the address information based on the location distance, as described in more detail elsewhere herein.

[0059] In some implementations, the authentication device may determine a location region that is associated with the address location. In some implementations, the location region may be a geographical location that is at, or within, a region distance from the address location. For example, if the region distance is thirty miles, then the authentication device may determine that the location region is a geographical location that is at, or within, thirty miles from the address location. As an example, the authentication device may determine a correlation between the location information and the address information based on the location region distance, as described in more detail elsewhere herein.

[0060] In some implementations, the authentication device may determine a location region distance that is a distance between the address location and at least a portion of the location region. As an example, if the distance between the address location and the device location is sixty miles, and if the

region distance associated with the location region is thirty miles, then the authentication device may determine that the location region distance is thirty miles. In other words, for example, the authentication device may determine a distance between the device location and a portion of a geographical area associated with the address location.

[0061] In some implementations, the authentication device may determine one or more historical locations, such as historical locations associated with a transaction associated with the account, the owner of the document, and/or the user device. As an example, a historical location associated with the transaction associated with the account may be a location where the user performed an in-person purchase, such as an in-person purchase of coffee. As another example, a historical location associated with the owner of the document may be a previous home address associated with the owner of the document and/or a historical location associated with the user device may be a location associated with a previously localized geographic location of the user device, such as a previously localized geographic location of the user device based on multilateration of signals (e.g. radio-frequency signals). In some implementations, the authentication device may determine a distance between the one or more historical interactions and the address location and/or a distance between the one or more historical interactions and the device location.

[0062] In some implementations, the location information may not include the live user image, but the authentication device may determine and/or confirm the location information using the live user image. As an example, the authentication device may determine the device location based on identifying a geographical location identifier depicted in the live user image. For example, if the geographical location identifier is a landmark located at a geographical position, then the authentication device may determine the device location based on the geographical location of the landmark.

[0063] In some implementations, the authentication device may identify one or more location parameters associated with the live user image. As an example, the location parameter may be associated with a time of day and/or a weather condition, such as a daylight parameter (e.g., indicating whether daylight conditions are depicted in the live user image), a nighttime parameter (e.g., indicating whether nighttime conditions are depicted in the live user image), a sunlight parameter (e.g., indicating whether sunlight conditions are depicted in the live user image), a cloud parameter (e.g., indicating whether cloud conditions are depicted in the live user image), and/or a rain parameter (e.g., indicating whether rain conditions are depicted in the live user image), among other examples. In some implementations, the authentication device may use a computer vision technique to identify the location parameter associated with the live user image and may determine whether the location parameter corresponds to the device location. The authentication device may compare the one or more location parameters to conditions associated with the device location near a time at which the live user image is captured to determine

whether the live image is valid or authentic. For example, if the location parameter is a rain parameter, the authentication device may determine that the location parameter corresponds to the device location based on determining that a weather condition associated with the device location at the time that the live user image is captured is a rainy weather condition (e.g., based on a weather report associated with the device location at the associated time).

[0064] As another example, if the location parameter is a rain parameter, the authentication device may determine that the location parameter does not correspond to the device location by determining that a weather condition associated with the device location that corresponds to the time that the live user image is captured is a sunlight weather condition (e.g., based on the weather report associated with the device location at the associated time). Thus, in some implementations, the authentication case may use the location parameter as a factor for authentication.

[0065] For example, the authentication device may authenticate the access attempt to the account and/or perform the action based on determining that the location parameter corresponds to the device location (e.g., a weather condition indicated in the live user image matches a weather condition corresponding to the device location at the time that the live user image is captured). As another example, the authentication device may not authenticate the access attempt to the account and/or perform the action based on determining that the location parameter does not correspond to the device location (e.g., a weather condition indicated in the live user image does not match a weather condition corresponding to the device location at the time that the live user image is captured).

[0066] In some implementations, the user device may be a trusted device. For example, the user device may be a trusted device based on the user device being previously authenticated by a multi-factor authentication technique. In some implementations, the authentication device may identify a network identifier associated with the trusted device and the authentication device may determine the device location based on the network identifier. For example, the network identifier may be a network connection (e.g., a Bluetooth connection), and the authentication device may determine the device location based on the network connection.

[0067] As shown by reference number 124, the authentication device may analyze the document image and the live user image. For example, the authentication device may process and/or analyze the document image, information associated with the document image, the live user image, and/or information associated with the live user image by using various techniques, such as image analysis techniques and/or machine learning models, as described in more detail elsewhere herein. The authentication device may analyze the document image and the live user image to determine whether to authenticate the access attempt and/or action associated with the account, as described in more detail elsewhere herein.

[0068] As shown by reference number 126, the authentication device may extract an identification image from the document image. In some implementations, the identification image included in the document image may depict a face of the person to which the document is issued, and the authentication device may detect the identification image by using a computer vision technique, such as an object recognition technique. As an example, the authentication device may extract the identification image from the document image based on detecting the identification image in the document image via the object recognition technique.

[0069] In some implementations, the authentication device may obtain, such as by scanning, an image of a machine-readable code that is included in the document image and may decode the machine-readable code to obtain the image identifier associated with the identification image included in the document (e.g., as described above). For example, the system may perform OCR on the document image to obtain an image of the machine-readable code depicted in the document image.

[0070] In some implementations, the authentication device may obtain the high-resolution color version of the identification image based on decoding the machine-readable code. As an example, the authentication device may use the image identifier to retrieve the high-resolution color version from the web server that stores the high-resolution color version of the identification image. As another example, the image identifier may indicate a link, such as a link to a webpage that displays (e.g., via a web browser) the high-resolution color version of the identification image, and the authentication device may follow the link to retrieve the high-resolution color version of the image, such as by downloading the high-resolution color version of the identification image from the website. In this way, using the high-resolution color version of the image for analysis enables the authentication device to obtain more information and/or to obtain the information more accurately.

[0071] As shown by reference number 128, the authentication device may pre-process the identification image from the document image (e.g., may perform one or more image pre-processing operations). In some implementations, the authentication device may identify an issue date associated with the document from the document image. As an example, the authentication device may perform a computer vision technique on the document image, such as the OCR technique, to extract text from the document that indicates the issue date. In some implementations, the authentication device may use a machine learning technique, such as keyword-parsing technique, to identify and extract the issue date associated with the document based on extracting the text via the OCR technique.

[0072] In some implementations, the authentication device may perform an image manipulation operation, such as an age progression operation, to modify the identification image to a modified identification image based on an amount of time between the issue date and a current date. As an example, the authentication device may use a machine learning model to analyze the identification image

and the amount of time between the issue date and the current date to generate the modified identification image.

[0073] In some implementations, the modified identification image may be an estimated identification image at the current date. As an example, the estimated identification image at the current date may depict an estimated face of the owner associated with the document at the current date, such as an age progressed face of the owner associated with the document based on the amount of time between the issue date and the current date.

[0074] As another example, if the issue date associated with the document is January 1, 2020, and if the current date is January 1, 2023, then the identification image may depict a face of the owner associated with the document as the face appears on January 1, 2020, and the modified identification image may depict an age progressed face of the owner associated with the document based on three years (e.g., the amount of time between the issue date and the current date). In this way, the modified identification image may enable a more accurate analysis when comparing the modified identification image to the live user image relative to comparing the identification image to the live user image.

[0075] As shown by reference number 130, the authentication device may identify one or more features of the user from the live user image. In some implementations, the authentication device may identify one or more live user image appearance parameters from the live user image and one or more identification image appearance parameters from the identification image of the document.

[0076] In some implementations, the one or more live user image appearance parameters from the live user image may be based on the appearance of the person depicted in the live user image. In some implementations, the one or more identification image appearance parameters from the identification image of the document may be based on the appearance of the person depicted in the identification image from the document.

[0077] In some implementations, the one or more live user image appearance parameters from the live user image and/or the one or more identification image appearance parameters from the identification image may include one or more of an age, an eye color, a gender, a skin color, a facial characteristic, a weight, and/or a height associated with the user depicted in the live user image and/or the person depicted in the identification image. Thus, in some implementations, the one or more document appearance parameters, the one or more live user image appearance parameters, and/or the one or more identification image appearance parameters may be associated with one or more of an age, an eye color, a gender, a skin color, a facial characteristic, a weight, and/or a height

[0078] In some implementations, the authentication device may analyze the live user image to estimate one or more live user image values of the one or more live user image appearance parameters. In some implementations, the estimated one or more live user image values may be an estimated age, an estimated

eye color, an estimated gender, an estimated skin color, an estimated facial characteristic, an estimated weight, and/or an estimated height associated with the live user image (e.g., the face of the user depicted in the liver user image).

[0079] As an example, the authentication device may analyze, using a trained image classification model, the live user image to obtain the one or more live user image values. In some implementations, the authentication device may obtain one or more document values of the one or more document appearance parameters obtained via the document image and/or one or more identification values of the one or more identification image appearance parameters obtained via the identification image.

[0080] In some implementations, the authentication device may input the one or more live user image values, and the one or more document values, and/or the one or more identification values to obtain, from the machine learning model, a confidence score indicating a likelihood that the user is the person to which the document is issued, as described in more detail elsewhere herein.

[0081] As shown by reference number 132, the authentication device may compare the live user image to the identification image of the document. In some implementations, the authentication device may compare the one or more live user image appearance parameters from the live user image and the one or more identification image appearance parameters from the identification image of the document to the one or more document appearance parameters associated with the document to determine a confidence score that indicates a likelihood that the one or more live user image appearance parameters and/or the one or more identification image appearance parameters include the one or more document appearance parameters. In other words, the authentication device may extract the identification image from the document, obtain the live user image, analyze the identification image and the live user image to extract the one or more live user image appearance parameters and the one or more identification image appearance parameters, and compare the one or more live user image appearance parameters and the one or more identification image appearance parameters to the appearance information described by text provided on the document to determine the confidence score.

[0082] As an example, the one or more live user image appearance parameters, the one or more identification image appearance parameters, and the one or more document appearance parameters may include an eye color of blue and a gender of male. The authentication device may compare the one or more live user image appearance parameters and the one or more identification image appearance parameters to the one or more document appearance parameters associated with the document to determine the confidence score that indicates a likelihood that the one or more live user image appearance parameters and the one or more identification image appearance parameters include the one or more document appearance parameters. In this example, the confidence score may be a high confidence score that indicates a strong likelihood that the one or more live user image appearance parameters and the one

or more identification image appearance parameters include the one or more document appearance parameters (e.g., the confidence score may satisfy a threshold).

[0083] As another example, the one or more live user image appearance parameters may include an eye color of blue and a gender of male, the one or more identification image appearance parameters may include an eye color of brown and a gender of female, and the one or more document appearance parameters may include an eye color of green and a gender of male. The authentication device may compare the one or more live user image appearance parameters and the one or more identification image appearance parameters to the one or more document appearance parameters associated with the document to determine a confidence score that indicates a likelihood that the one or more live user image appearance parameters and the one or more identification image appearance parameters include the one or more document appearance parameters. In this example, the confidence score may be a low confidence score that indicates a weak likelihood that the one or more live user image appearance parameters and the one or more identification image appearance parameters include the one or more document appearance parameters (e.g., the confidence score may not satisfy the threshold).

[0084] In some implementations, the authentication device may compare the live user image to the modified identification image (described above) to determine a likelihood that the live user image and the modified identification image are associated with the user. In other words, for example, the authentication device may compare the age progressed face of the user depicted in the modified identification image to the face depicted in the live user image (e.g., the selfie) to determine a likelihood that the live user image and the modified identification image are associated with the user.

[0085] As shown by reference number 134, the authentication device may compare the one or more features to appearance information extracted from the document. In some implementations, the authentication device may identify one or more live user image appearance parameters from the live user image and compare the one or more document appearance parameters to the one or more live user image appearance parameters to determine a likelihood that the one or more document appearance parameters are included in the one or more live user image appearance parameters. In other words, the authentication device may obtain the live user image, may analyze the live user image to extract the one or more live user image appearance parameters, and may compare the one or more live user image appearance parameters to the appearance information described by text provided on the document to determine the confidence score, as described in more detail above.

[0086] As shown by reference number 136, the authentication device may compare the location information to one or more trusted locations. In some implementations, the authentication device may compare the device location to one or more trusted locations associated with the user device and/or one or more trusted locations associated with the user. For example, the one or more trusted locations may

include a recognized location, such as a historical location associated with the user device and/or a historical location associated with the user.

[0087] For example, the authentication device may determine that the device location is a trusted location based on determining that the device location is a same location as a trusted location of the one or more trusted locations associated with the user device and/or the user. As another example, the authentication device may determine that the device location is not a trusted location based on determining that the device location is not a same location as a trusted location of the one or more trusted locations associated with the user device and/or the user.

[0088] As shown by reference number 138, the authentication device may obtain a confidence score indicating a likelihood that the user is associated with the document. In some implementations, the authentication device may analyze the document image, the live user image, and/or the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document.

[0089] For example, the authentication device may analyze, using a machine learning model, the document image, the live user image, and/or the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document. As an example, the authentication device may use the machine learning model to determine whether the live user image depicts the one or more document appearance parameters, as described in more detail elsewhere herein.

[0090] In some implementations, the confidence score may indicate a likelihood that the one or more live user image appearance parameters from the live user image and the one or more identification image appearance parameters from the identification image of the document include the one or more document appearance parameters. In some implementations, the confidence score may include a first confidence score that indicates a likelihood that the live user image includes the one or more document appearance parameters, and a second confidence score that indicates a likelihood that the live user image matches the identification image from the document.

[0091] In some implementations, the live user image may match the identification image based on satisfying a threshold number of matching minutiae points between the live user image and the identification image, such as one or more live user image appearance parameters and/or the one or more identification image appearance parameters. As an example, the live user image may match the identification image based on a number of matching minutiae points being greater than a threshold number of matching minutiae points.

[0092] In some implementations, the authentication device may obtain, from an image classification model, one or more estimated live user image appearance parameters and respective likelihood scores based on the live user image. In some implementations, the authentication device may determine the

confidence score based on the one or more document appearance parameters, the one or more estimated live user image appearance parameters, and the respective likelihood scores. In other words, the authentication device may obtain, from the output of the image classification model, the estimated one or more liver user image appearance parameters and respective confidence scores associated with the estimated one or more liver user image appearance parameters. The authentication device may compare the estimated one or more liver user image appearance parameters and/or the respective confidence scores associated with the estimated one or more liver user image appearance parameters to the appearance information associated with the document to determine the confidence score that the user (e.g., depicted in the selfie image) is the owner of the document.

[0093] In some implementations, the authentication device may determine a confidence score, based on the address information and the location information, that indicates a likelihood that the device is associated with the owner of the document. In some implementations, the confidence score may be based on a correlation between the location information and the address information. In some implementations, the authentication device may determine that the correlation between the location information and the address information is a positive correlation, a negative correlation, a strong positive correlation, and/or a weak negative correlation, among other examples.

[0094] For example, the authentication device may determine that the correlation between the location information and the address information is a strong negative correlation based on determining that the location information and the address information have a negligible effect on the confidence score. As another example, the authentication device may determine that the correlation between the location information and the address information is a strong positive correlation based on determining that the location information and the address information have a significant effect on the confidence score.

[0095] Thus, in some implementations, the authentication device may determine whether to authenticate the access attempt to the account and/or to perform the action based on the correlation between the location information and the address information. In this way, the authentication device may use the correlation data between the location information and the address information to determine a risk level associated with the access attempt to the account and/or a risk level associated with performing the action.

[0096] In some implementations, the authentication device may determine the confidence score based on the address location, the device location, the location distance and/or the location region distance (e.g., as described above). In some implementations, the authentication device may determine one or more historical locations associated with one or more transactions associated with the account, the owner of the document, and/or the device. In some implementations, the authentication device may determine the confidence score based on determining that the device location does not correspond to the trusted

location. In some implementations, the authentication device may determine the confidence score based on two or more of the address location, the device location, or the one or more historical locations.

[0097] In some implementations, the authentication device may determine the device location based on the geographic identifiers and may determine the confidence score based on the address location and the device location. In some implementations, the authentication device may identify a location parameter associated with the identification image, such as, and may determine whether the location parameter corresponds to the device location. In some implementations, the authentication device may update the confidence score based on determining that the parameter does not correspond to the device location.

[0098] As shown in Fig. 1E, and by reference number 140, the authentication device may determine whether to authenticate the access attempt and/or the action based on analyzing the images. In some implementations, the authentication device may determine whether the confidence score satisfies a threshold. In some implementations, the threshold may include a first threshold and a second threshold. As an example, if the confidence score is greater than a first threshold, then the authentication device may determine that confidence score satisfies the first threshold. As another example, if the confidence score is less than the first threshold and greater than the second threshold, then the authentication device may determine that the confidence score does not satisfy the first threshold and does satisfy the second threshold. In some implementations, the authentication device may determine whether to authenticate the access attempt to the account and/or perform the action based on the confidence score satisfying the threshold (e.g., the first threshold or the second threshold).

[0099] In some implementations, the authentication device may determine whether the confidence score satisfies the threshold as one factor (e.g., of multiple factors) in determining whether to authenticate the access attempt to the account and/or perform the action. As an example, the authentication device may determine that the confidence score satisfies the threshold and may input this information into a machine learning model for further authentication analysis, as described in more detail elsewhere herein. For example, if the authentication device determines that the user is not in a location indicated by the document, the document may still be authenticated. In this example, the authentication device may request additional authentication information based on determining that the user is not in the location indicated by the document rather than not authenticating the access attempt to the account and/or not performing the action.

[0100] As shown by reference number 142, the authentication device may obtain feedback information from the authentication determination to re-train one or more models. In some implementations, the authentication device may provide feedback, to an age prediction model, that indicates the identification image, the modified identification image, the live user image, the issue date, the current date, and/or an

indication that the identification image and live user image are associated with a same user. In some implementations, the age prediction model may be associated with predicting an age of users depicted in images. In some implementations, the authentication device may provide the feedback based on determining that the live user image and the modified identification image are associated with the user. Thus, in some implementations, providing the feedback, such as live user images that have been authenticated and/or live user images that have not been, to the machine learning model may improve the machine learning model. For example, providing the feedback to the machine learning model may improve the accuracy of the machine learning model and/or may improve feature selection associated with the machine learning model.

[0101] As shown by reference number 144, the authentication device may grant or deny access to the account and/or enable the action to be performed. In some implementations, the authentication device may grant or deny access to the account and/or may enable the action to be performed based on the confidence score satisfying a threshold. As an example, the authentication device may authenticate the access attempt based on the confidence score satisfying a threshold. As another example, the authentication device may refrain from authenticating the access attempt to the account based and/or refrain from performing the action based on determining that the confidence score does not satisfy the threshold.

[0102] In some implementations, the authentication device may perform an action based on determining whether the user is the person to which the document is issued. For example, if the person is an authenticated user, the authentication device may authenticate an access attempt to the account by the user based on determining that the user is the person to which the document is issued. In some implementations, the authentication device may perform the action based on determining whether the confidence score satisfies the threshold. As an example, the authentication device may authenticate the access attempt to the account based on determining that the confidence score satisfies the threshold. As another example, the authentication device may perform an additional authentication operation based on determining that the confidence score does not satisfy the threshold, such as requesting an additional document (e.g., if the document image originally provided to the authentication device indicates that the document is expired).

[0103] As another example, if the confidence score satisfies the first threshold, then the authentication device may grant access and/or enable the action to be performed. If the confidence score satisfies the second threshold but does not satisfy the first threshold, then the authentication device may request additional information from the user to determine whether to grant or deny access and/or enable the action to be performed. For example, the authentication device may request additional authentication information from the user, such as biometric information associated with the user, a password, passcode,

an answer to a verification question, and/or an authentication token. If the confidence score does not satisfy the second threshold, then the authentication device may deny access, may refrain from enabling the action to be performed, and/or may perform a higher level of authentication operations. For example, the authentication device may request an additional live user image (e.g., if the live user image provided by the user is blurry).

[0104] In some implementations, the authentication device may use a multi-factor approach to determine whether to authenticate the access attempt to the account and/or perform the action (e.g., the authentication device may use one or more factors and/or one or more machine learning models). As an example, the authentication device may use a document authentication model to obtain an output that indicates a likelihood that the document is authentic and is associated with a trusted user of the account. The authentication device may provide the document as an input to the document authentication model and the document authentication model may output a document score that indicates the likelihood that the document is authentic and that the document is associated with the trusted user of the account.

[0105] In some implementations, the authentication device may use an authentication model to determine whether the access attempt is authentic based on the document score and/or a confidence score. As an example, the authentication device may determine the confidence score associated with an access attempt to the account, may determine the document score, and may provide the confidence score and the document score as an input to an authentication model. The authentication model may generate an output that indicates whether the access attempt is authentic. The authentication device may authenticate the access attempt based on an output of the authentication model indicating that the access attempt is authentic. In some implementations, the authentication device may store the live user image based on the confidence score satisfying the threshold and authenticate one or more future access attempts for the account using the live user image. In this way, because the live user image is a more recent image relative to the identification image, the live user image may provide a more accurate comparison point for the future authentication.

[0106] In some implementations, the authentication device may store a device location indicated by the location information based on the confidence score satisfying the threshold and may authenticate one or more future access attempts for the account using the device location. In this way, the device location may be stored as a trusted device location, and may streamline future access attempts based on the trusted device location.

[0107] In some implementations, the authentication device may obtain, from the authentication model, one or more estimated device location regions and respective confidence scores based on a device location indicated by the location information. In some implementations, the authentication device may

determine the confidence score based on the address information, the location information, and the estimated device location regions and the respective confidence scores.

[0108] In this way, some implementations described herein provide enhanced authentication techniques using a document and/or a device location, such as by indicating a likelihood that the user is the person to which the document is issued and/or by indicating a likelihood that the device is associated with the owner of the document. Because the system uses enhanced authentication techniques using the document, the system consumes less resources compared to other authentication techniques (e.g., by avoiding a need to perform actions associated with associated with incorrect authentication determinations, such as forensic examination of data, generating notifications, and/or transmitting the notifications).

[0109] As indicated above, Figs. 1A-1E are provided as an example. Other examples may differ from what is described with regard to Figs. 1A-1E.

[0110] Fig. 2 is a diagram illustrating an example 200 of training and using a machine learning model in connection with enhanced authentication using a secure document. The machine learning model training and usage described herein may be performed using a machine learning system. The machine learning system may include or may be included in a computing device, a server, a cloud computing environment, or the like, such as the authentication device described in more detail elsewhere herein.

[0111] As shown by reference number 205, a machine learning model may be trained using a set of observations. The set of observations may be obtained from training data (e.g., historical data), such as data gathered during one or more processes described herein. In some implementations, the machine learning system may receive the set of observations (e.g., as input) from the authentication device, as described elsewhere herein.

[0112] As shown by reference number 210, the set of observations may include a feature set. The feature set may include a set of variables, and a variable may be referred to as a feature. A specific observation may include a set of variable values (or feature values) corresponding to the set of variables. In some implementations, the machine learning system may determine variables for a set of observations and/or variable values for a specific observation based on input received from the authentication device. For example, the machine learning system may identify a feature set (e.g., one or more features and/or feature values) by extracting the feature set from structured data, by performing natural language processing to extract the feature set from unstructured data, and/or by receiving input from an operator.

[0113] As an example, a feature set for a set of observations may include a first feature of estimated feature, a second feature of extracted description, a third feature of likelihood score of the estimated feature, and so on. As shown, for a first observation, the first feature may have a value of blue eyes, the second feature may have a value of blue eyes, the third feature may have a value of 80, and so on. These

features and feature values are provided as examples, and may differ in other examples. For example, the feature set may include one or more of the following features: appearance parameters, such as an age, an eye color, a gender, a skin color, a facial characteristic, a weight, and/or a height, among other examples.

[0114] As shown by reference number 215, the set of observations may be associated with a target variable. The target variable may represent a variable having a numeric value, may represent a variable having a numeric value that falls within a range of values or has some discrete possible values, may represent a variable that is selectable from one of multiple options (e.g., one of multiples classes, classifications, or labels) and/or may represent a variable having a Boolean value. A target variable may be associated with a target variable value, and a target variable value may be specific to an observation. In example 200, the target variable is confidence score, which has a value of 95 for the first observation.

[0115] The target variable may represent a value that a machine learning model is being trained to predict, and the feature set may represent the variables that are input to a trained machine learning model to predict a value for the target variable. The set of observations may include target variable values so that the machine learning model can be trained to recognize patterns in the feature set that lead to a target variable value. A machine learning model that is trained to predict a target variable value may be referred to as a supervised learning model.

[0116] In some implementations, the machine learning model may be trained on a set of observations that do not include a target variable. This may be referred to as an unsupervised learning model. In this case, the machine learning model may learn patterns from the set of observations without labeling or supervision, and may provide output that indicates such patterns, such as by using clustering and/or association to identify related groups of items within the set of observations.

[0117] As shown by reference number 220, the machine learning system may train a machine learning model using the set of observations and using one or more machine learning algorithms, such as a regression algorithm, a decision tree algorithm, a neural network algorithm, a k-nearest neighbor algorithm, a support vector machine algorithm, or the like. After training, the machine learning system may store the machine learning model as a trained machine learning model 225 to be used to analyze new observations.

[0118] As an example, the machine learning system may obtain training data for the set of observations based on historical data associated with one or more appearance parameters, such as one or more appearance parameters associated with an image that depicts a face of a person.

[0119] As shown by reference number 230, the machine learning system may apply the trained machine learning model 225 to a new observation, such as by receiving a new observation and inputting the new observation to the trained machine learning model 225. As shown, the new observation may include a first feature of estimated feature, a second feature of extracted description, a third feature of

likelihood score of the estimated feature, and so on, as an example. The machine learning system may apply the trained machine learning model 225 to the new observation to generate an output (e.g., a result). The type of output may depend on the type of machine learning model and/or the type of machine learning task being performed. For example, the output may include a predicted value of a target variable, such as when supervised learning is employed. Additionally, or alternatively, the output may include information that identifies a cluster to which the new observation belongs and/or information that indicates a degree of similarity between the new observation and one or more other observations, such as when unsupervised learning is employed.

[0120] As an example, the trained machine learning model 225 may predict a value of 70 for the target variable of confidence score for the new observation, as shown by reference number 235. Based on this prediction, the machine learning system may provide a first recommendation, may provide output for determination of a first recommendation, may perform a first automated action, and/or may cause a first automated action to be performed (e.g., by instructing another device to perform the automated action), among other examples. The first recommendation may include, for example, a recommendation that the authentication device authenticates the access attempt and/or a recommendation that the authentication device performs the action. The first automated action may include, for example, causing the authentication device to authenticate the access attempt and/or causing the authentication device to perform the action.

[0121] As another example, if the machine learning system were to predict a value of 20 for the target variable of confidence score, then the machine learning system may provide a second (e.g., different) recommendation (e.g., recommendation that the authentication device does not authenticate the access attempt and/or a recommendation that the authentication device does not perform the action) and/or may perform or cause performance of a second (e.g., different) automated action (e.g., causing the authentication device to generate an alert).

[0122] In some implementations, the trained machine learning model 225 may classify (e.g., cluster) the new observation in a cluster, as shown by reference number 240. The observations within a cluster may have a threshold degree of similarity. As an example, if the machine learning system classifies the new observation in a first cluster (e.g., definitely authenticate), then the machine learning system may provide a first recommendation, such as the first recommendation described above. Additionally, or alternatively, the machine learning system may perform a first automated action and/or may cause a first automated action to be performed (e.g., by instructing another device to perform the automated action) based on classifying the new observation in the first cluster, such as the first automated action described above.

[0123] As another example, if the machine learning system were to classify the new observation in a second cluster (e.g., maybe authenticate), then the machine learning system may provide a second (e.g., different) recommendation (e.g., a recommendation that the authentication device requests additional authentication information from the user) and/or may perform or cause performance of a second (e.g., different) automated action, such as causing the authentication device to request additional authentication information from the user.

[0124] In some implementations, the recommendation and/or the automated action associated with the new observation may be based on a target variable value having a particular label (e.g., classification or categorization), may be based on whether a target variable value satisfies one or more threshold (e.g., whether the target variable value is greater than a threshold, is less than a threshold, is equal to a threshold, falls within a range of threshold values, or the like), and/or may be based on a cluster in which the new observation is classified.

[0125] The recommendations, actions, and clusters described above are provided as examples, and other examples may differ from what is described above. In some implementations, the machine learning model may be based on an age prediction model. For example, the age prediction model may predict an age of users depicted in images, and the feature set may include one or more features associated with the identification image, the modified identification image, the live user image, the issue date, the current date. As an example, the age prediction model may output an indication that the identification image and the live user image are associated with a same user.

[0126] In some implementations, the machine learning model may be based on the identification image and/or the live user image. For example, the machine learning model may compare the identification image to the live user image, and the feature set may include one or more features associated with the identification image and/or the live user image, such as the one or more document appearance parameters.

[0127] In some implementations, the machine learning model may be based on the location information and/or the address information. For example, the machine learning model may determine a correlation between the location information and the address information relative to the confidence score, and the features set may include one or more features associated with the location information and/or the address information, such as the location distance and/or the regions distance. In this example, the machine learning model may determine the confidence score based on the correlation between the location information and the address information.

[0128] In some implementations, the trained machine learning model 225 may be re-trained using feedback information. For example, feedback may be provided to the machine learning model. The feedback may be associated with actions performed based on the recommendations provided by the trained machine learning model 225 and/or automated actions performed, or caused, by the trained

machine learning model 225. In other words, the recommendations and/or actions output by the trained machine learning model 225 may be used as inputs to re-train the machine learning model (e.g., a feedback loop may be used to train and/or update the machine learning model). For example, the feedback information may include the identification image, the live user image, and/or an indication that the identification image and the live user image are associated with a same user. As an example, providing the feedback, such as live user images that have been authenticated and/or live user images that have not been, to the machine learning model may improve the machine learning model. For example, providing the feedback to the machine learning model may improve the accuracy of the machine learning model and/or may improve feature selection associated with the machine learning model.

[0129] In this way, the machine learning system may apply a rigorous and automated process to enhanced authentication using a secure document. The machine learning system may enable recognition and/or identification of tens, hundreds, thousands, or millions of features and/or feature values for tens, hundreds, thousands, or millions of observations, thereby increasing accuracy and consistency and reducing delay associated with enhanced authentication using a secure document relative to requiring computing resources to be allocated for tens, hundreds, or thousands of operators to manually authenticate access attempts and/or perform actions using the features or feature values.

[0130] As indicated above, Fig. 2 is provided as an example. Other examples may differ from what is described in connection with Fig. 2.

[0131] Fig. 3 is a diagram of an example environment 300 in which systems and/or methods described herein may be implemented. As shown in Fig. 3, environment 300 may include an authentication device 310, a user device 320, and/or a network 330. Devices of environment 300 may interconnect via wired connections, wireless connections, or a combination of wired and wireless connections.

[0132] The authentication device 310 may include one or more devices capable of receiving, generating, storing, processing, providing, and/or routing information associated with enhanced authentication using a secure document, as described elsewhere herein. The authentication device 310 may include a communication device and/or a computing device. For example, the authentication device 310 may include a server, such as an application server, a client server, a web server, a database server, a host server, a proxy server, a virtual server (e.g., executing on computing hardware), or a server in a cloud computing system. In some implementations, the authentication device 310 may include computing hardware used in a cloud computing environment.

[0133] The user device 320 may include one or more devices capable of receiving, generating, storing, processing, and/or providing information associated with enhanced authentication using a secure document, as described elsewhere herein. The user device 320 may include a communication device and/or a computing device. For example, the user device 320 may include a wireless communication

device, a mobile phone, a user equipment, a laptop computer, a tablet computer, a desktop computer, a wearable communication device (e.g., a smart wristwatch, a pair of smart eyeglasses, a head mounted display, or a virtual reality headset), or a similar type of device.

[0134] The network 330 may include one or more wired and/or wireless networks. For example, the network 330 may include a wireless wide area network (e.g., a cellular network or a public land mobile network), a local area network (e.g., a wired local area network or a wireless local area network (WLAN), such as a Wi-Fi network), a personal area network (e.g., a Bluetooth network), a near-field communication network, a telephone network, a private network, the Internet, and/or a combination of these or other types of networks. The network 330 enables communication among the devices of environment 300.

[0135] The number and arrangement of devices and networks shown in Fig. 3 are provided as an example. In practice, there may be additional devices and/or networks, fewer devices and/or networks, different devices and/or networks, or differently arranged devices and/or networks than those shown in Fig. 3. Furthermore, two or more devices shown in Fig. 3 may be implemented within a single device, or a single device shown in Fig. 3 may be implemented as multiple, distributed devices. Additionally, or alternatively, a set of devices (e.g., one or more devices) of environment 300 may perform one or more functions described as being performed by another set of devices of environment 300.

[0136] Fig. 4 is a diagram of example components of a device 400 associated with enhanced authentication using a secure document. The device 400 may correspond to the authentication device 310 and/or the user device 320. In some implementations, the authentication device 310 and/or the user device 320 may include one or more devices 400 and/or one or more components of the device 400. As shown in Fig. 4, the device 400 may include a bus 410, a processor 420, a memory 430, an input component 440, an output component 450, and/or a communication component 460.

[0137] The bus 410 may include one or more components that enable wired and/or wireless communication among the components of the device 400. The bus 410 may couple together two or more components of Fig. 4, such as via operative coupling, communicative coupling, electronic coupling, and/or electric coupling. For example, the bus 410 may include an electrical connection (e.g., a wire, a trace, and/or a lead) and/or a wireless bus. The processor 420 may include a central processing unit, a graphics processing unit, a microprocessor, a controller, a microcontroller, a digital signal processor, a field-programmable gate array, an application-specific integrated circuit, and/or another type of processing component. The processor 420 may be implemented in hardware, firmware, or a combination of hardware and software. In some implementations, the processor 420 may include one or more processors capable of being programmed to perform one or more operations or processes described elsewhere herein.

[0138] The memory 430 may include volatile and/or nonvolatile memory. For example, the memory 430 may include random access memory (RAM), read only memory (ROM), a hard disk drive, and/or another type of memory (e.g., a flash memory, a magnetic memory, and/or an optical memory). The memory 430 may include internal memory (e.g., RAM, ROM, or a hard disk drive) and/or removable memory (e.g., removable via a universal serial bus connection). The memory 430 may be a non-transitory computer-readable medium. The memory 430 may store information, one or more instructions, and/or software (e.g., one or more software applications) related to the operation of the device 400. In some implementations, the memory 430 may include one or more memories that are coupled (e.g., communicatively coupled) to one or more processors (e.g., processor 420), such as via the bus 410. Communicative coupling between a processor 420 and a memory 430 may enable the processor 420 to read and/or process information stored in the memory 430 and/or to store information in the memory 430.

[0139] The input component 440 may enable the device 400 to receive input, such as user input and/or sensed input. For example, the input component 440 may include a touch screen, a keyboard, a keypad, a mouse, a button, a microphone, a switch, a sensor, a global positioning system sensor, an accelerometer, a gyroscope, and/or an actuator. The output component 450 may enable the device 400 to provide output, such as via a display, a speaker, and/or a light-emitting diode. The communication component 460 may enable the device 400 to communicate with other devices via a wired connection and/or a wireless connection. For example, the communication component 460 may include a receiver, a transmitter, a transceiver, a modem, a network interface card, and/or an antenna.

[0140] The device 400 may perform one or more operations or processes described herein. For example, a non-transitory computer-readable medium (e.g., memory 430) may store a set of instructions (e.g., one or more instructions or code) for execution by the processor 420. The processor 420 may execute the set of instructions to perform one or more operations or processes described herein. In some implementations, execution of the set of instructions, by one or more processors 420, causes the one or more processors 420 and/or the device 400 to perform one or more operations or processes described herein. In some implementations, hardwired circuitry may be used instead of or in combination with the instructions to perform one or more operations or processes described herein. Additionally, or alternatively, the processor 420 may be configured to perform one or more operations or processes described herein. Thus, implementations described herein are not limited to any specific combination of hardware circuitry and software.

[0141] The number and arrangement of components shown in Fig. 4 are provided as an example. The device 400 may include additional components, fewer components, different components, or differently arranged components than those shown in Fig. 4. Additionally, or alternatively, a set of components (e.g.,

one or more components) of the device 400 may perform one or more functions described as being performed by another set of components of the device 400.

[0142] Fig. 5 is a flowchart of an example process 500 associated with enhanced authentication using a secure document. In some implementations, one or more process blocks of Fig. 5 may be performed by the authentication device 310. In some implementations, one or more process blocks of Fig. 5 may be performed by another device or a group of devices separate from or including the authentication device 310, such as the user device 320. Additionally, or alternatively, one or more process blocks of Fig. 5 may be performed by one or more components of the device 400, such as processor 420, memory 430, input component 440, output component 450, and/or communication component 460.

[0143] As shown in Fig. 5, process 500 may include obtaining a document image, the document being the identification document, and the document including an identification image depicting a face of a person associated with the document (block 510). For example, the authentication device 310 (e.g., using processor 420 and/or memory 430) may obtain a document image, the document being the identification document, and the document including an identification image depicting a face of a person associated with the document, as described above in connection with reference number 112 of Fig. 1B. As an example, the authentication device may obtain the indication of the document image from the user device based on the user capturing the document image with the user device.

[0144] As further shown in Fig. 5, process 500 may include obtaining a live user image, the live user image being a live image of the user (block 520). For example, the authentication device 310 (e.g., using processor 420 and/or memory 430) may obtain a live user image, the live user image being a live image of the user, as described above in connection with reference number 118 of Fig. 1C. As an example, the authentication device may obtain the indication of the live user image from the user device based on capturing the live user image.

[0145] As further shown in Fig. 5, process 500 may include extracting information from the document image, the information including appearance information associated with the person, the appearance information including one or more document appearance parameters (block 530). For example, the authentication device 310 (e.g., using processor 420 and/or memory 430) may extract information from the document image, the information including appearance information associated with the person, the appearance information including one or more document appearance parameters, as described above in connection with reference number 122 of Fig. 1D. As an example, the authentication device may obtain an image of the machine-readable code included in the document image and may decode the machine-readable code to obtain the appearance information including the one or more document appearance parameters.

[0146] As further shown in Fig. 5, process 500 may include analyzing the identification image, the live user image, and the appearance information to determine whether the user is the person to which the document is issued, the analyzing including: comparing the identification image to the live user image, and identifying whether the one or more document appearance parameters are included in the live user image (block 540). For example, the authentication device 310 (e.g., using processor 420 and/or memory 430) may analyze the identification image, the live user image, and the appearance information to determine whether the user is the person to which the document is issued, the analyzing including: comparing the identification image to the live user image, and identifying whether the one or more document appearance parameters are included in the live user image, as described above in connection with reference number 134 of Fig. 1D. As an example, the authentication device may identify one or more live user image appearance parameters from the live user image and compare the one or more document appearance parameters to the one or more live user image appearance parameters to determine a likelihood that the one or more document appearance parameters are included in the one or more live user image appearance parameters. In other words, the authentication device may obtain the live user image, may analyze the live user image to extract the one or more live user image appearance parameters, and may compare the one or more live user image appearance parameters to the appearance information described by text provided on the document to determine the confidence score, as described in more detail above.

[0147] As further shown in Fig. 5, process 500 may include performing an action based on determining whether the user is the person to which the document is issued (block 550). For example, the authentication device 310 (e.g., using processor 420 and/or memory 430) may perform an action based on determining whether the user is the person to which the document is issued, as described above in connection with reference number 144 of Fig. 1E. As an example, the authentication device may authenticate the account and/or may enable the action to be performed based on the confidence score satisfying a threshold.

[0148] Although Fig. 5 shows example blocks of process 500, in some implementations, process 500 may include additional blocks, fewer blocks, different blocks, or differently arranged blocks than those depicted in Fig. 5. Additionally, or alternatively, two or more of the blocks of process 500 may be performed in parallel. The process 500 is an example of one process that may be performed by one or more devices described herein. These one or more devices may perform one or more other processes based on operations described herein, such as the operations described in connection with Figs. 1A-1E. Moreover, while the process 500 has been described in relation to the devices and components of the preceding figures, the process 500 can be performed using alternative, additional, or fewer devices and/or

components. Thus, the process 500 is not limited to being performed with the example devices, components, hardware, and software explicitly enumerated in the preceding figures.

[0149] The foregoing disclosure provides illustration and description, but is not intended to be exhaustive or to limit the implementations to the precise forms disclosed. Modifications may be made in light of the above disclosure or may be acquired from practice of the implementations.

[0150] As used herein, the term "component" is intended to be broadly construed as hardware, firmware, or a combination of hardware and software. It will be apparent that systems and/or methods described herein may be implemented in different forms of hardware, firmware, and/or a combination of hardware and software. The hardware and/or software code described herein for implementing aspects of the disclosure should not be construed as limiting the scope of the disclosure. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code - it being understood that software and hardware can be used to implement the systems and/or methods based on the description herein.

[0151] As used herein, satisfying a threshold may, depending on the context, refer to a value being greater than the threshold, greater than or equal to the threshold, less than the threshold, less than or equal to the threshold, equal to the threshold, not equal to the threshold, or the like.

[0152] Although particular combinations of features are recited in the claims and/or disclosed in the specification, these combinations are not intended to limit the disclosure of various implementations. In fact, many of these features may be combined in ways not specifically recited in the claims and/or disclosed in the specification. Although each dependent claim listed below may directly depend on only one claim, the disclosure of various implementations includes each dependent claim in combination with every other claim in the claim set. As used herein, a phrase referring to "at least one of" a list of items refers to any combination and permutation of those items, including single members. As an example, "at least one of: a, b, or c" is intended to cover a, b, c, a-b, a-c, b-c, and a-b-c, as well as any combination with multiple of the same item. As used herein, the term "and/or" used to connect items in a list refers to any combination and any permutation of those items, including single members (e.g., an individual item in the list). As an example, "a, b, and/or c" is intended to cover a, b, c, a-b, a-c, b-c, and a-b-c.

[0153] No element, act, or instruction used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles "a" and "an" are intended to include one or more items, and may be used interchangeably with "one or more." Further, as used herein, the article "the" is intended to include one or more items referenced in connection with the article "the" and may be used interchangeably with "the one or more." Furthermore, as used herein, the term "set" is intended to include one or more items (e.g., related items, unrelated items, or a combination of related and unrelated items), and may be used interchangeably with "one or more." Where only one item is intended, the

phrase “only one” or similar language is used. Also, as used herein, the terms “has,” “have,” “having,” or the like are intended to be open-ended terms. Further, the phrase “based on” is intended to mean “based, at least in part, on” unless explicitly stated otherwise. Also, as used herein, the term “or” is intended to be inclusive when used in a series and may be used interchangeably with “and/or,” unless explicitly stated otherwise (e.g., if used in combination with “either” or “only one of”).

WHAT IS CLAIMED IS:

1. A system for enhanced authentication using image analysis of an identification document and appearance information associated with the identification document, the system comprising:

one or more memories; and

one or more processors, communicatively coupled to the one or more memories, configured to:

detect an authentication event associated with an access attempt for an account;

obtain a document image based on detecting the authentication event, the document image being an image of the identification document;

obtain a live user image associated with the authentication event based on detecting the authentication event, the live user image being a live image of the user;

extract information from the document image, the information including the appearance information associated with the document, the appearance information including one or more document appearance parameters;

analyze, using a machine learning model, the document image, the live user image, and the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document, the analyzing including determining whether the live user image depicts the one or more document appearance parameters; and

authenticate the access attempt based on the confidence score satisfying a threshold.

2. The system of claim 1, wherein the one or more processors, to analyze the document image, the live user image, and the appearance information, are configured to:

identify an identification image from the document image, the identification image being an image of an owner of the document;

identify one or more live user image appearance parameters from the live user image;

identify one or more identification image appearance parameters from the identification image; and

compare the one or more live user image appearance parameters and the one or more identification image appearance parameters to the one or more document appearance parameters,

wherein the confidence score indicates a likelihood that the one or more live user image appearance parameters and the one or more identification image appearance parameters include the one or more document appearance parameters.

3. The system of claim 1, wherein the one or more processors, to analyze the document image, the live user image, and the appearance information, are configured to:

identify one or more live user image appearance parameters from the live user image; and

compare the one or more live user image appearance parameters to the one or more document appearance parameters to determine a likelihood that the one or more live user image appearance parameters are included in the one or more document appearance parameters.

4. The system of claim 1, wherein the one or more processors, to analyze the document image, the live user image, and the appearance information, are configured to:

identify an issue date associated with the document from the document image;

identify an identification image from the document image, the identification image being an image of an owner of the document;

perform an image manipulation operation to modify the identification image to a modified identification image based on an amount of time between the issue date and a current date,

wherein the modified identification image is an estimated identification image at the current date; and

compare the live user image to the modified identification image to determine a likelihood that the live user image and the modified identification image are associated with the user.

5. The system of claim 4, wherein the one or more processors are further configured to:

provide feedback, to an age prediction model, indicating at least one of:

the identification image,

the modified identification image,

the live user image,

the issue date,

the current date, or

an indication that the identification image and the live user image are associated with a same user,

wherein the age prediction model is associated with predicting an age of users depicted in images, and

wherein providing the feedback is based on determining that the live user image and the modified identification image are associated with the user.

6. The system of claim 1, wherein the confidence score includes a first confidence score indicating a likelihood that the live user image includes the one or more document appearance parameters, and a second confidence score indicating a likelihood that the live user image matches an identification image from the document image.

7. The system of claim 1, wherein the one or more processors, to extract information from the document, are configured to:

obtain an image of a machine-readable code included in the document image; and

decode the machine-readable code to obtain the information.

8. The system of claim 1, wherein the one or more processors, to extract information from the document, are configured to:

analyze the document image using an optical character recognition (OCR) technique to obtain the information.

9. The system of claim 1, wherein the one or more document appearance parameters include at least one of:

an age,

an eye color,

a gender,

a skin color,

a facial characteristic,

a weight, or

a height.

10. A method of image analysis of an identification document and appearance information associated with the identification document, comprising:

obtaining, by a device, a document image, the document being the identification document, and the document including an identification image depicting a face of a person associated with the document;

obtaining, by the device, a live user image, the live user image being a live image of the user;

extracting, by the device, information from the document image, the information including appearance information associated with the person, the appearance information including one or more document appearance parameters;

analyzing, by the device, the identification image, the live user image, and the appearance information to determine whether the user is the person to which the document is issued, the analyzing including:

comparing the identification image to the live user image, and

identifying whether the one or more document appearance parameters are included in the live user image; and

performing, by the device, an action based on determining whether the user is the person to which the document is issued.

11. The method of claim 10, wherein the document is associated with an authenticated user of an account, and wherein performing the action comprises:

authenticating an access attempt to the account by the user based on determining that the user is the person to which the document is issued.

12. The method of claim 10, further comprising:

obtaining an image of a machine-readable code included in the document image;

decoding the machine-readable code; and

obtaining the identification image based on decoding the machine-readable code, wherein the identification image is a color image.

13. The method of claim 10, further comprising:

processing the document image to identify the identification image; and

extracting the identification image from the document image based on processing the document image.

14. The method of claim 13, further comprising:

performing one or more image pre-processing operations on the identification image to enhance a quality of the identification image.

15. The method of claim 10, wherein analyzing the identification image, the live user image, and the appearance information comprises:

estimating one or more live user image values of one or more live user image appearance parameters associated with the user from the live user image;

inputting, into a machine learning model, the one or more live user image values of the one or more live user image appearance parameters and one or more document values of the one or more document appearance parameters obtained via the document image; and

obtaining, from the machine learning model, a confidence score indicating a likelihood that the user is the person to which the document is issued.

16. The method of claim 15, wherein estimating the one or more live user image values comprises:

analyzing, using a trained image classification model, the live user image to obtain the one or more live user image values of the one or more live user image appearance parameters.

17. A non-transitory computer-readable medium storing a set of instructions, the set of instructions comprising:

one or more instructions that, when executed by one or more processors of a device, cause the device to:

detect an authentication event associated with an access attempt for an account, the account being associated with a trusted user;

obtain a document image based on detecting the authentication event, the document being an identification document issued by a trusted entity;

obtain a live user image associated with the access attempt based on detecting the authentication event;

extract information from the document image, the information including appearance information associated with the document, the appearance information including one or more document appearance parameters;

analyze the document image, the live user image, and the appearance information to determine a confidence score that indicates a likelihood that the user is associated with the document; and

authenticate the access attempt based on the confidence score satisfying a threshold.

18. The non-transitory computer-readable medium of claim 17, wherein the one or more instructions, that cause the device to authenticate the access attempt, are configured to:

obtain, from a document authentication model, a document score indicating a likelihood that the document is authentic and is associated with the trusted user of the account;

provide, to an authentication model, the document score and the confidence score; and

authenticate the access attempt based on an output of the authentication model indicating that the access attempt is authentic.

19. The non-transitory computer-readable medium of claim 17, wherein the one or more instructions, when executed by the one or more processors, further cause the device to:

store the live user image based on the confidence score satisfying the threshold; and

authenticating one or more future access attempts for the account using the live user image.

20. The non-transitory computer-readable medium of claim 17, wherein the one or more instructions, that cause the device to analyze the document image, the live user image, and the appearance information, cause the device to:

obtain, from an image classification model, one or more estimated live user image appearance parameters and respective likelihood scores based on the live user image; and

determine the confidence score based on the one or more document appearance parameters, the one or more estimated live user image appearance parameters, and the respective likelihood scores.

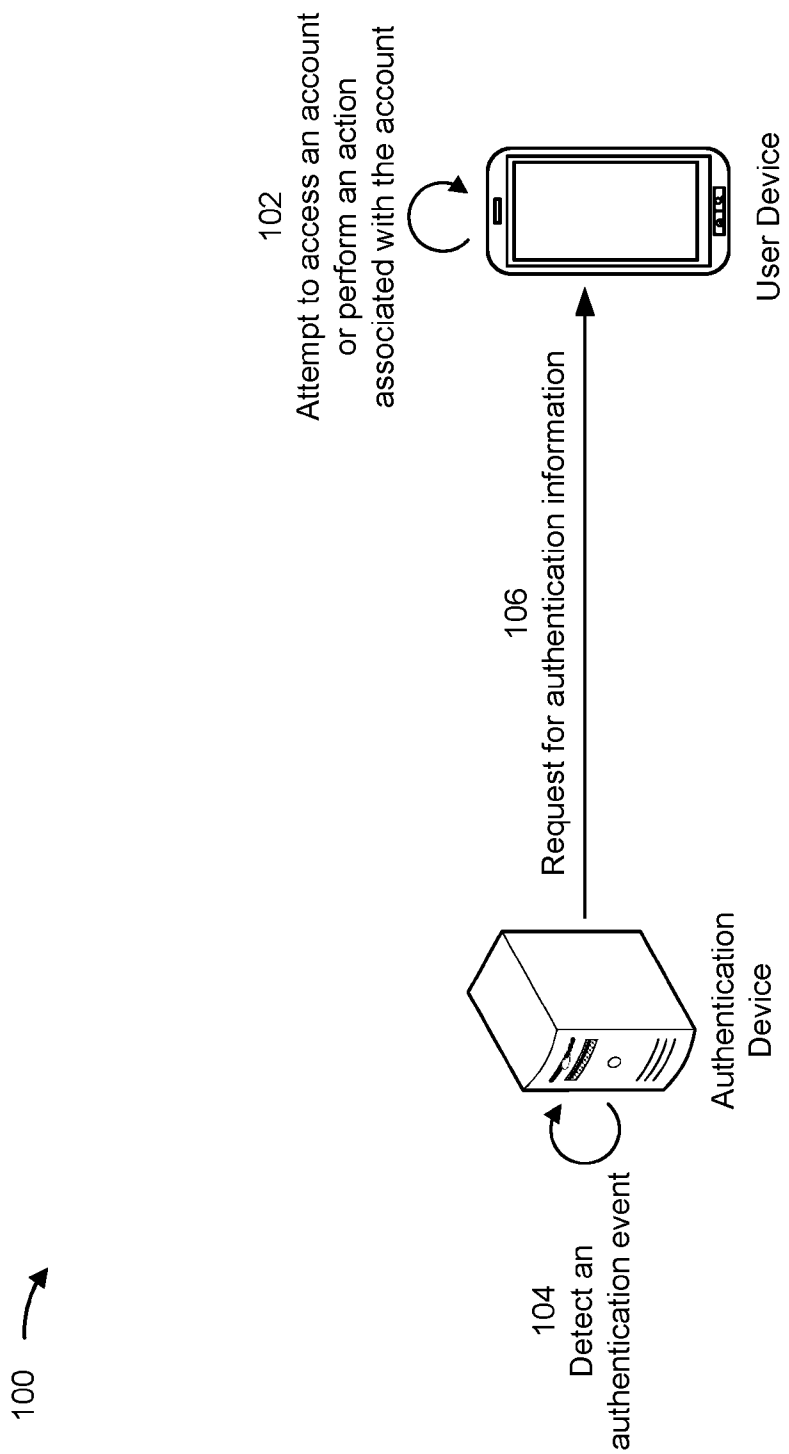
100
102
Attempt to access an account or perform an action associated with the account
User Device
106
Request for authentication information
Authentication Device
104
Detect an authentication event

FIG. 1A

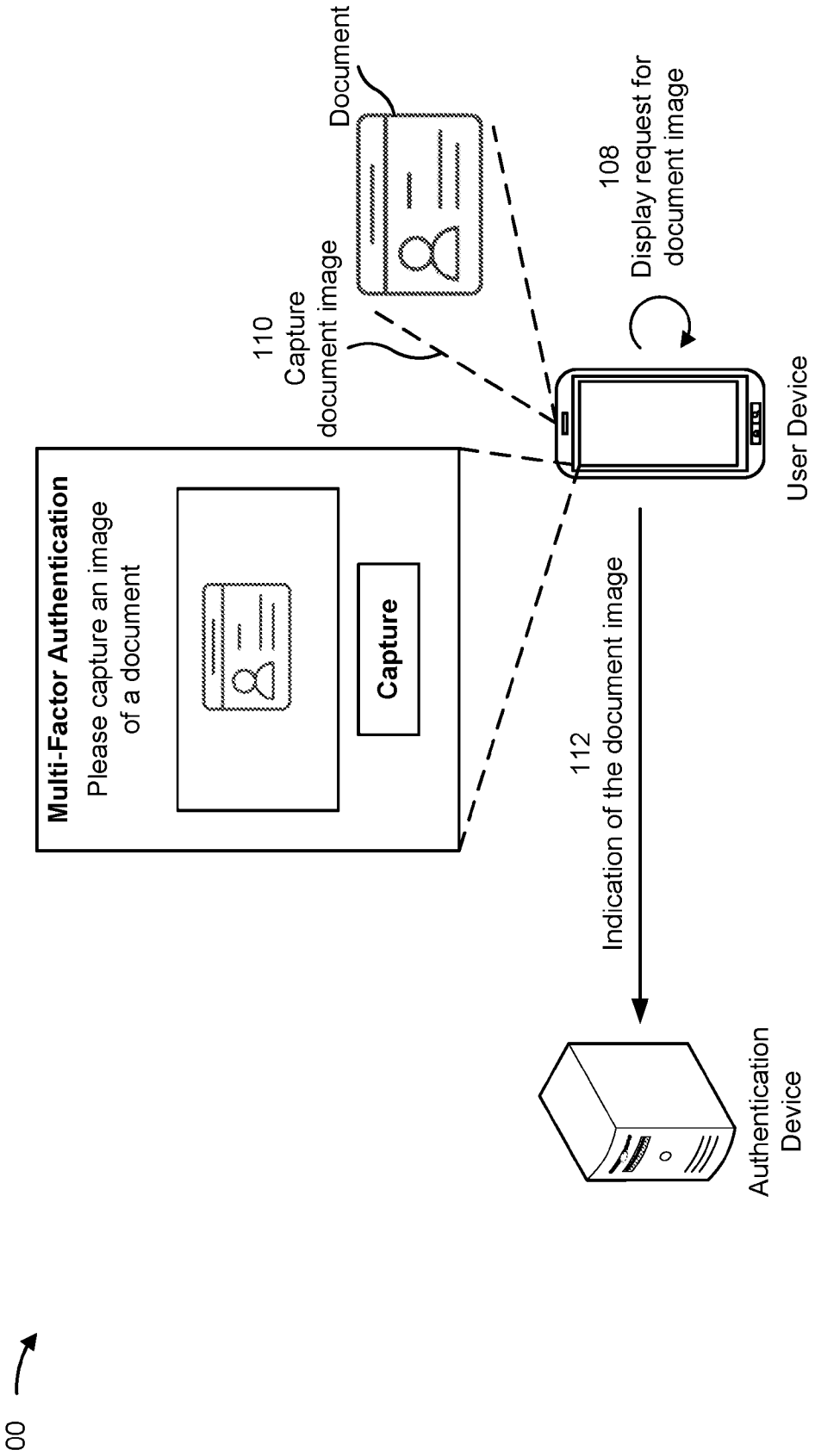
100
Multi-Factor Authentication
Please capture an image of a document
Capture
Document
110
Capture document image
108
Display request for document image
User Device
112
Indication of the document image
Authentication Device

FIG. 1B

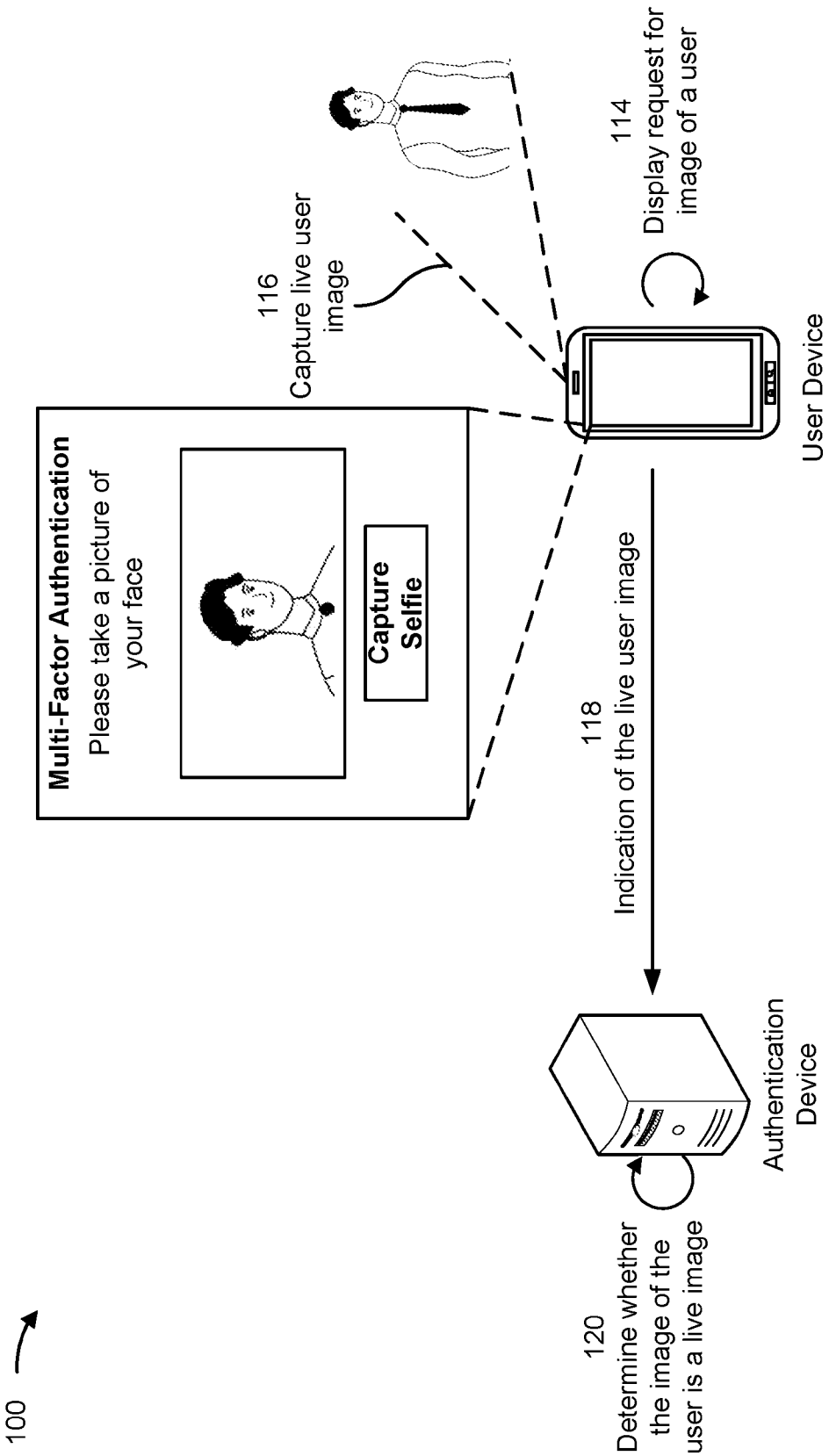
100
Multi-Factor Authentication
Please take a picture of your face
Capture Selfie
116
Capture live user image
114
Display request for image of a user
User Device
118
Indication of the live user image
Authentication Device
120
Determine whether the image of the user is a live image

FIG. 1C

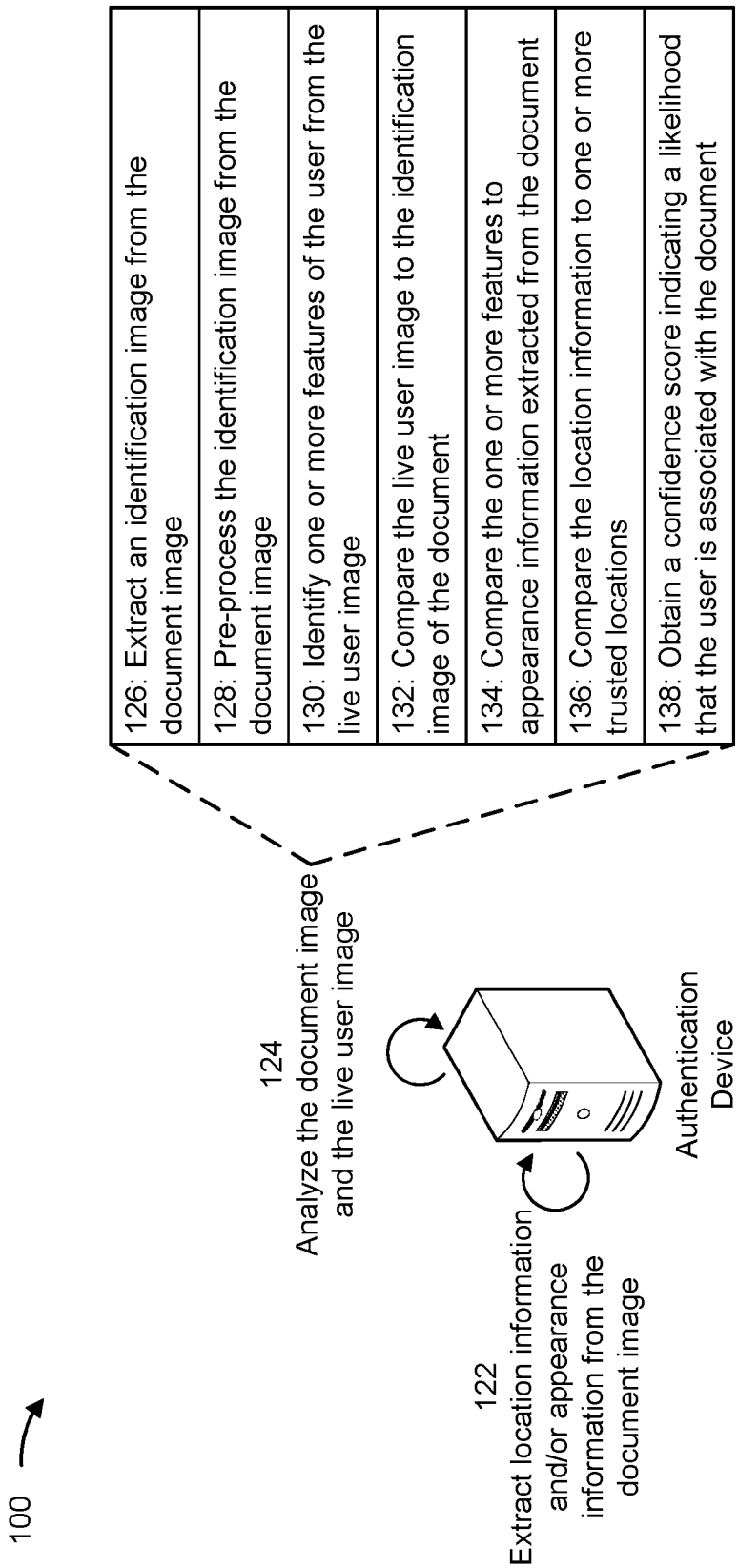
100
122
Extract location information and/or appearance information from the document image
124
Analyze the document image and the live user image
Authentication Device
126: Extract an identification image from the document image
128: Pre-process the identification image from the document image
130: Identify one or more features of the user from the live user image
132: Compare the live user image to the identification image of the document
134: Compare the one or more features to appearance information extracted from the document
136: Compare the location information to one or more trusted locations
138: Obtain a confidence score indicating a likelihood that the user is associated with the document

FIG. 1D

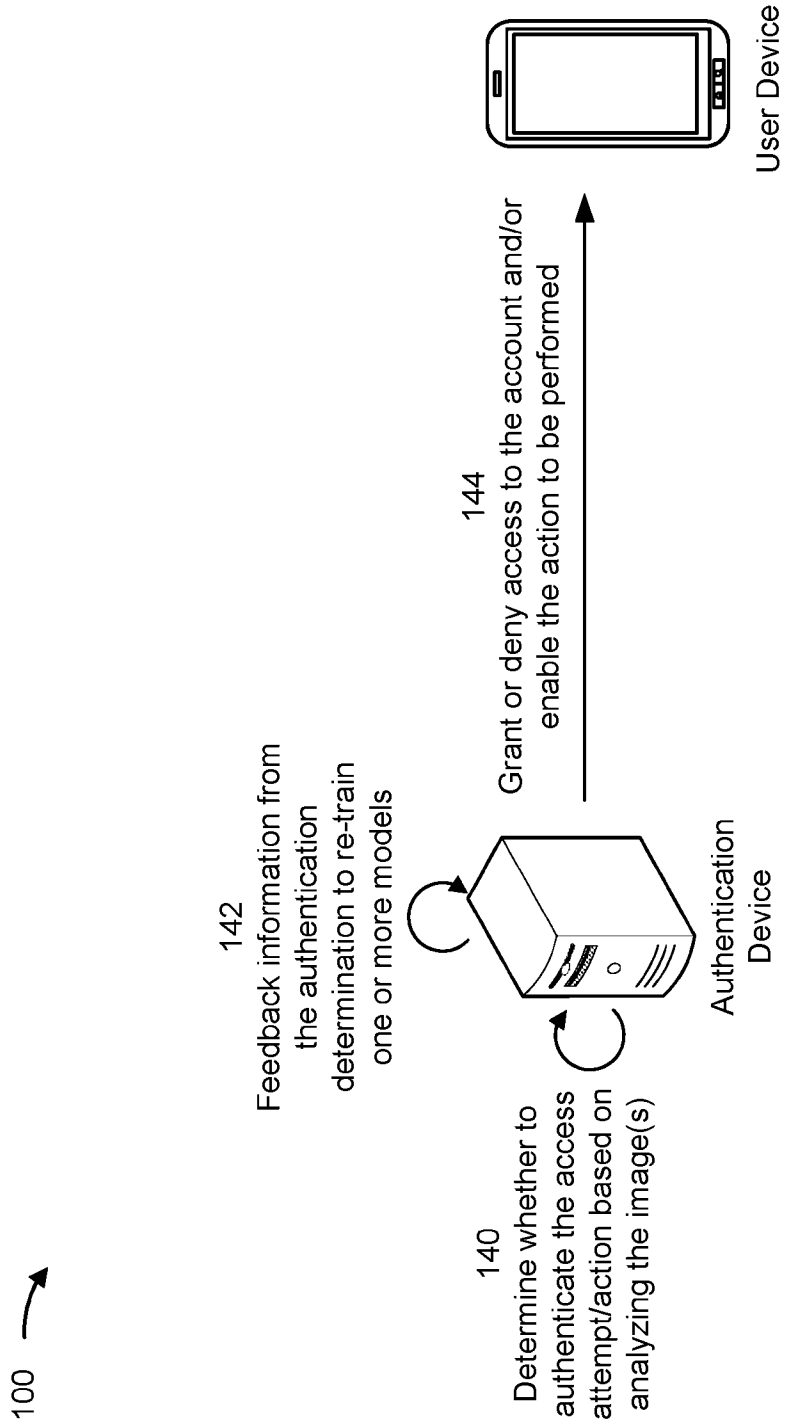
100
140
Determine whether to authenticate the access attempt/action based on analyzing the image(s)
142
Feedback information from the authentication determination to re-train one or more models
Authentication Device
144
Grant or deny access to the account and/or enable the action to be performed
User Device

FIG. 1E

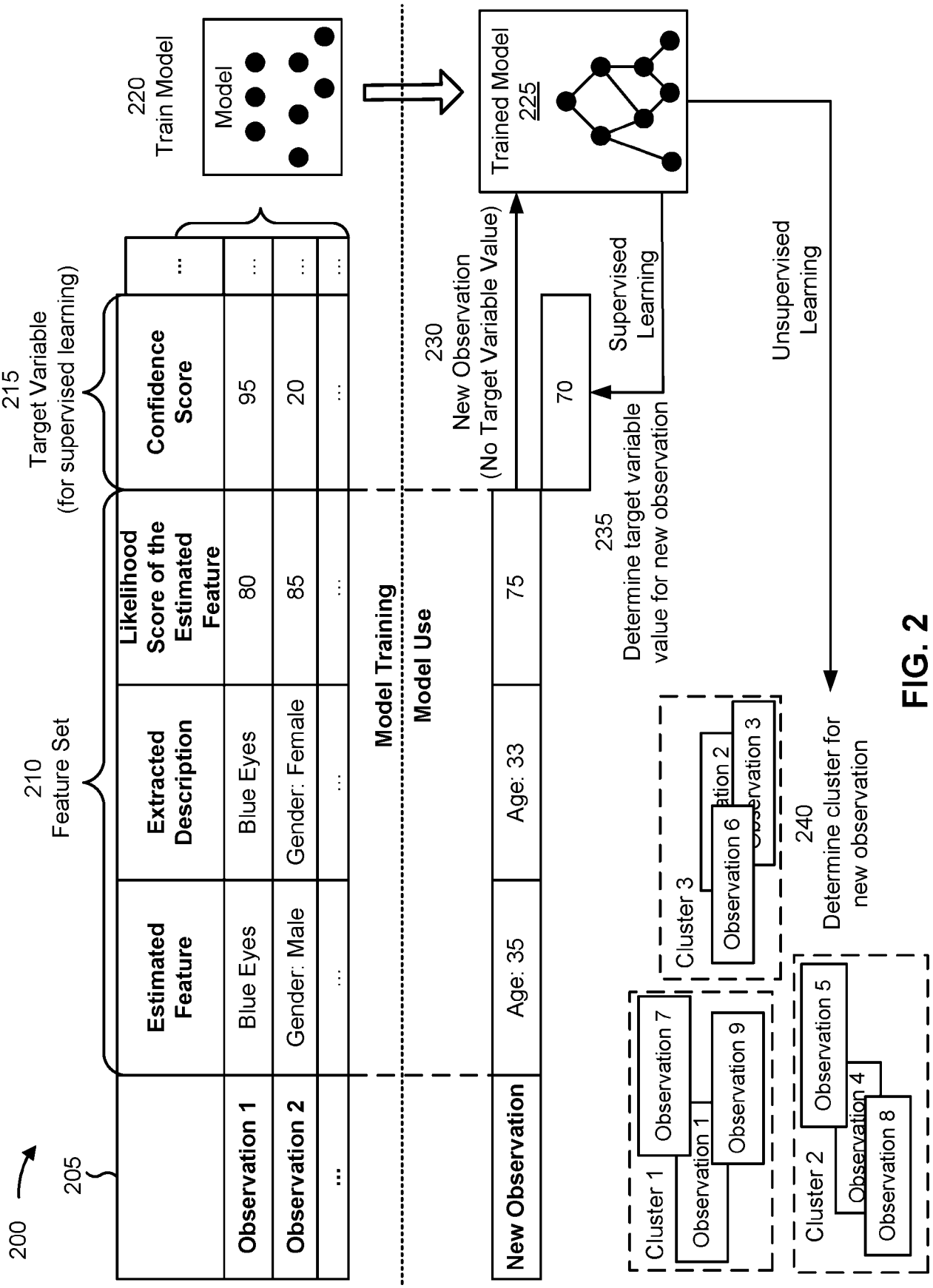
200
205
210
Feature Set
215
Target Variable
(for supervised learning)
Estimated Feature
Extracted Description
Likelihood Score of the Estimated Feature
Confidence Score
Observation 1
Blue Eyes
Blue Eyes
80
95
Observation 2
Gender: Male
Gender: Female
85
20
...
...
...
...
...
...
Model Training
Model Use
220
Train Model
Model
Trained Model
225
230
New Observation
(No Target Variable Value)
New Observation
Age: 35
Age: 33
75
70
235
Determine target variable value for new observation
Supervised Learning
Unsupervised Learning
240
Determine cluster for new observation
Cluster 1
Observation 1
Observation 7
Observation 9
Cluster 3
Observation 6
Observation 2
Observation 3
Cluster 2
Observation 5
Observation 4
Observation 8

FIG. 2

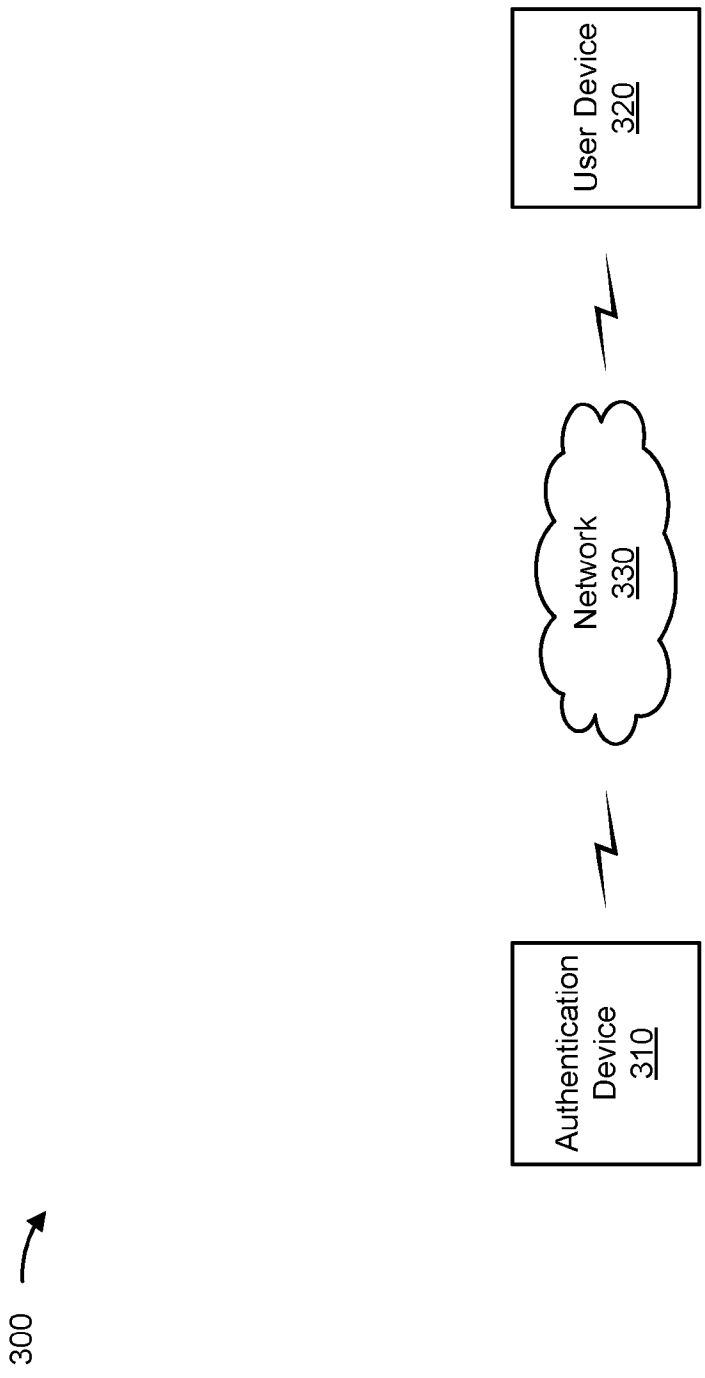

FIG. 3

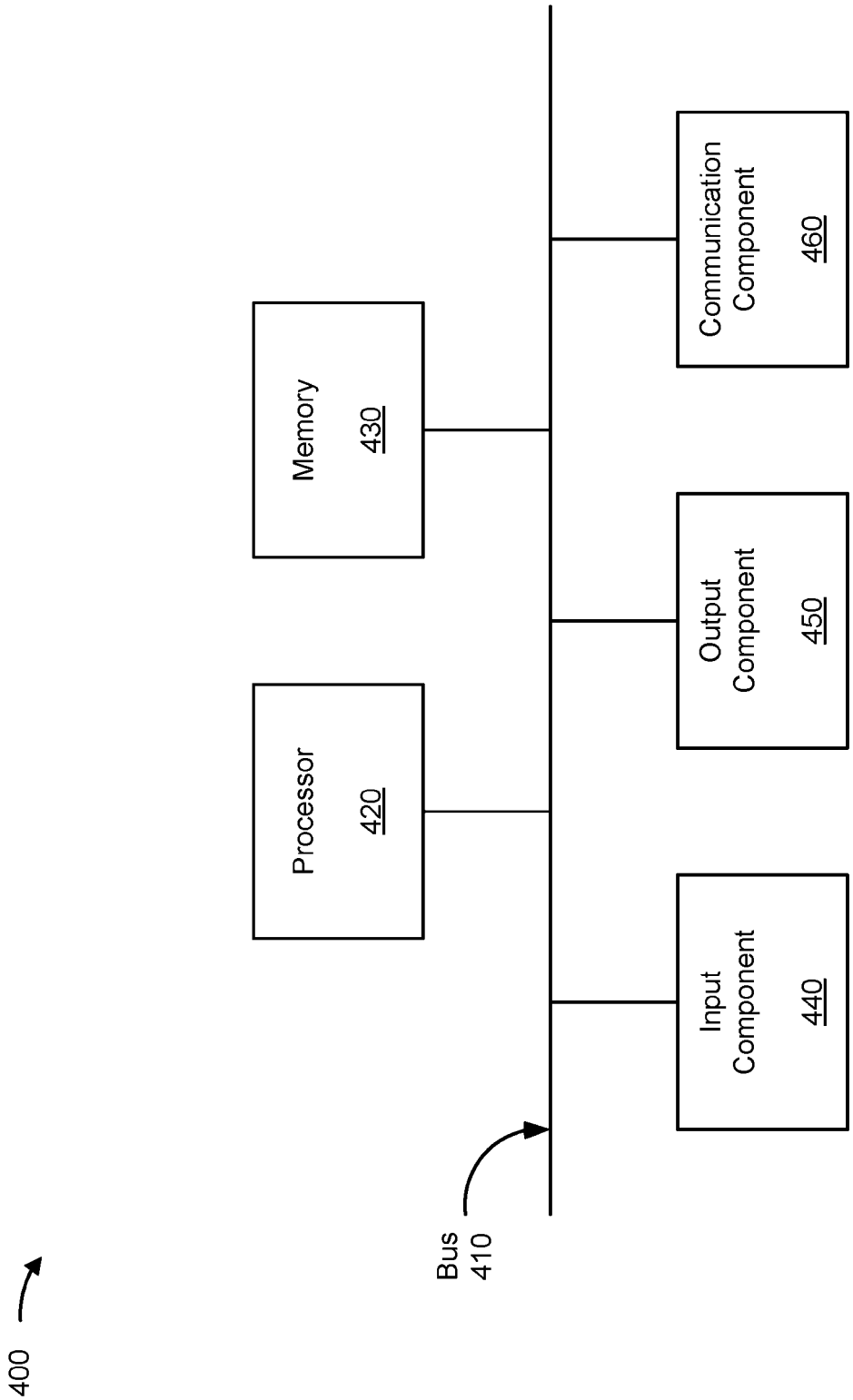
400
Bus
410
Processor
420
Memory
430
Input
Component
440
Output
Component
450
Communication
Component
460

FIG. 4

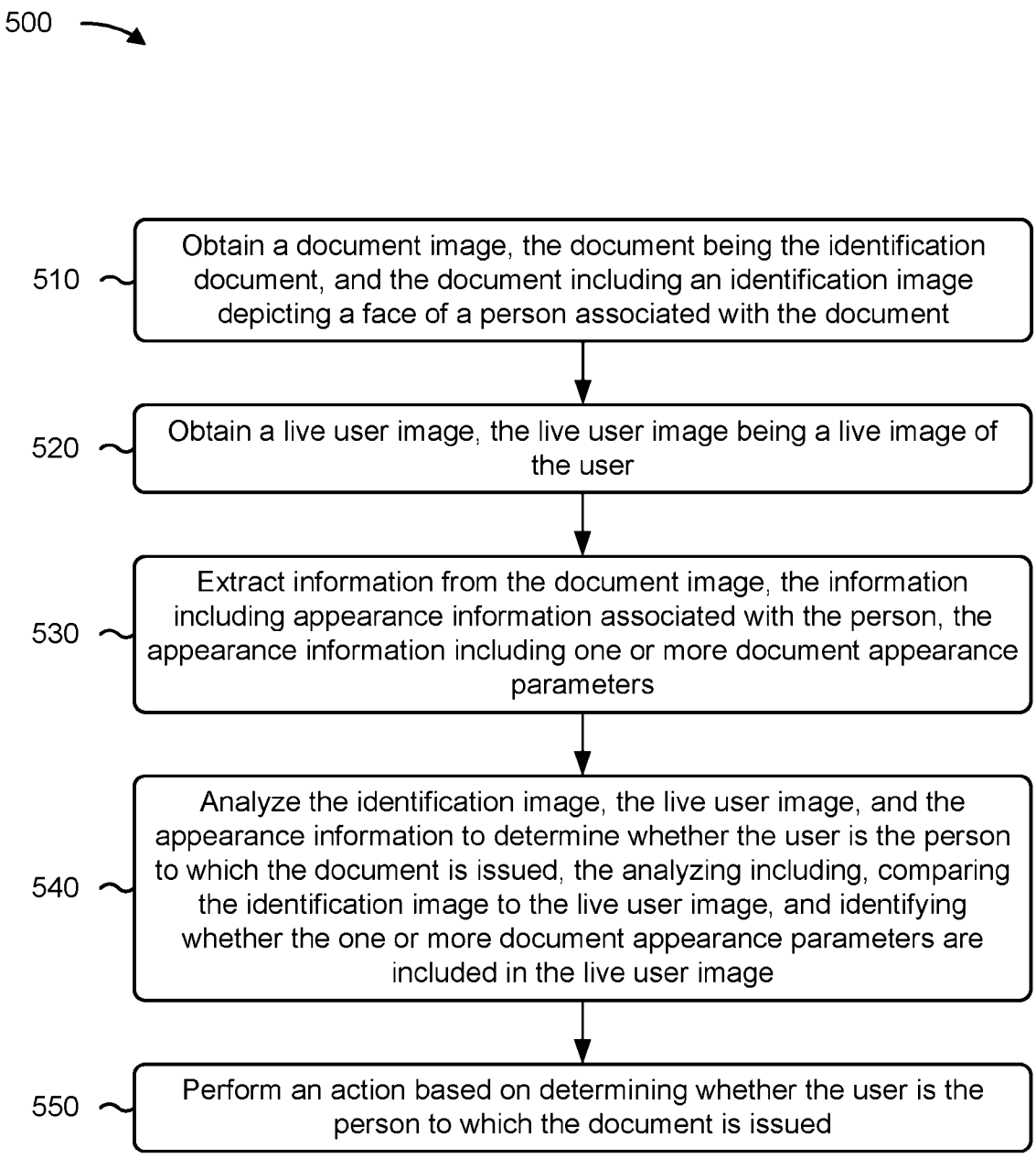
500
510
Obtain a document image, the document being the identification document, and the document including an identification image depicting a face of a person associated with the document
520
Obtain a live user image, the live user image being a live image of the user
530
Extract information from the document image, the information including appearance information associated with the person, the appearance information including one or more document appearance parameters
540
Analyze the identification image, the live user image, and the appearance information to determine whether the user is the person to which the document is issued, the analyzing including, comparing the identification image to the live user image, and identifying whether the one or more document appearance parameters are included in the live user image
550
Perform an action based on determining whether the user is the person to which the document is issued

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2024/028362

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/31 G06V40/16
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G06V

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	CA 3 047 248 A1 (CAPITAL ONE SERVICES LLC [US]) 13 November 2019 (2019-11-13) paragraph [0002] - paragraph [0004] paragraph [0030] - paragraph [0039] paragraph [0056] - paragraph [0061] -----	1-11, 13-18,20 12,19
Y	JP 2005 346447 A (GIJUTSU TRANSFER SERVICE KK) 15 December 2005 (2005-12-15) paragraph [0011] - paragraph [0013] -----	12
Y	KR 2022 0057254 A (SAMSUNG ELECTRONICS CO LTD [KR]) 9 May 2022 (2022-05-09) paragraph [0089] - paragraph [0091] -----	19

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2024	26/07/2024

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Krauß, Stefan

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2024/028362

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 3047248 A1	13-11-2019	CA 3047248 A1	13-11-2019
		EP 3608810 A1	12-02-2020
		US 10452897 B1	22-10-2019
		US 2020042773 A1	06-02-2020
		US 2021174069 A1	10-06-2021
		US 2023083852 A1	16-03-2023
		US 2024126855 A1	18-04-2024
JP 2005346447 A	15-12-2005	JP 2005346447 A	15-12-2005
		WO 2005119588 A1	15-12-2005
KR 20220057254 A	09-05-2022	KR 20220057254 A	09-05-2022
		WO 2022092582 A1	05-05-2022