US 20200019968A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2020/0019968 A1

PHAM et al. (43) Pub. Date: Jan. 16, 2020

(54) SYSTEM AND METHOD FOR AUTHENTICATING TRANSACTIONS FROM A MOBILE DEVICE

(71) Applicant: **Capital One Services, LLC**, McLean, VA (US)

(72) Inventors: **Vincent PHAM**, Champaign, IL (US); **Kenneth TAYLOR**, Champaign, IL (US); **Austin WALTERS**, Savoy, IL (US); **Anh TRUONG**, Champaign, IL (US); **Jeremy GOODSITT**, Champaign, IL (US); **Fardin Abdi Taghi ABAD**, Champaign, IL (US)

(21) Appl. No.: **16/032,303**

(22) Filed: **Jul. 11, 2018**

Publication Classification

(51) **Int. Cl.**

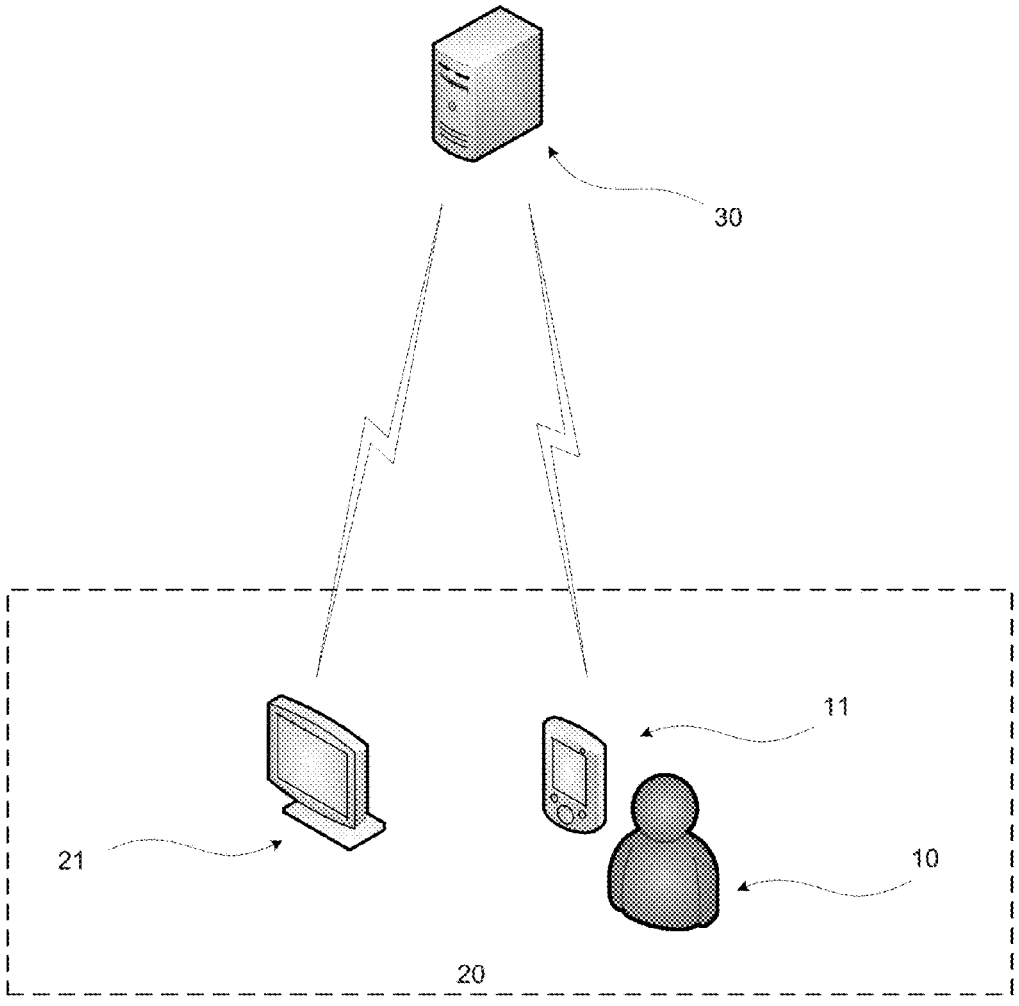
G06Q 20/40	(2006.01)
G06Q 20/20	(2006.01)
G06Q 20/32	(2006.01)
G06K 9/00	(2006.01)
G06K 9/22	(2006.01)
G06T 7/70	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/40145*** (2013.01); ***G06Q 20/206*** (2013.01); ***G06Q 20/322*** (2013.01); ***G06K 9/00087*** (2013.01); *G06F 17/30244* (2013.01); ***G06K 9/00926*** (2013.01); ***G06K 9/22*** (2013.01); ***G06T 7/70*** (2017.01); ***G06K 9/00288*** (2013.01)

(57) **ABSTRACT**

Systems and methods for authenticating transactions from a mobile device are described, including authenticating a user and a merchant location. A remote server receives an authentication request from a point-of-sale device, and requests that a user's mobile device use an associated camera to take a picture of the user at the merchant location. The remote server then processes the picture to determine the authenticity of the user and the location, and provides an authentication approval or denial to the point-of-sale device, instructing the point-of-sale device to execute, or not to execute, the transaction.



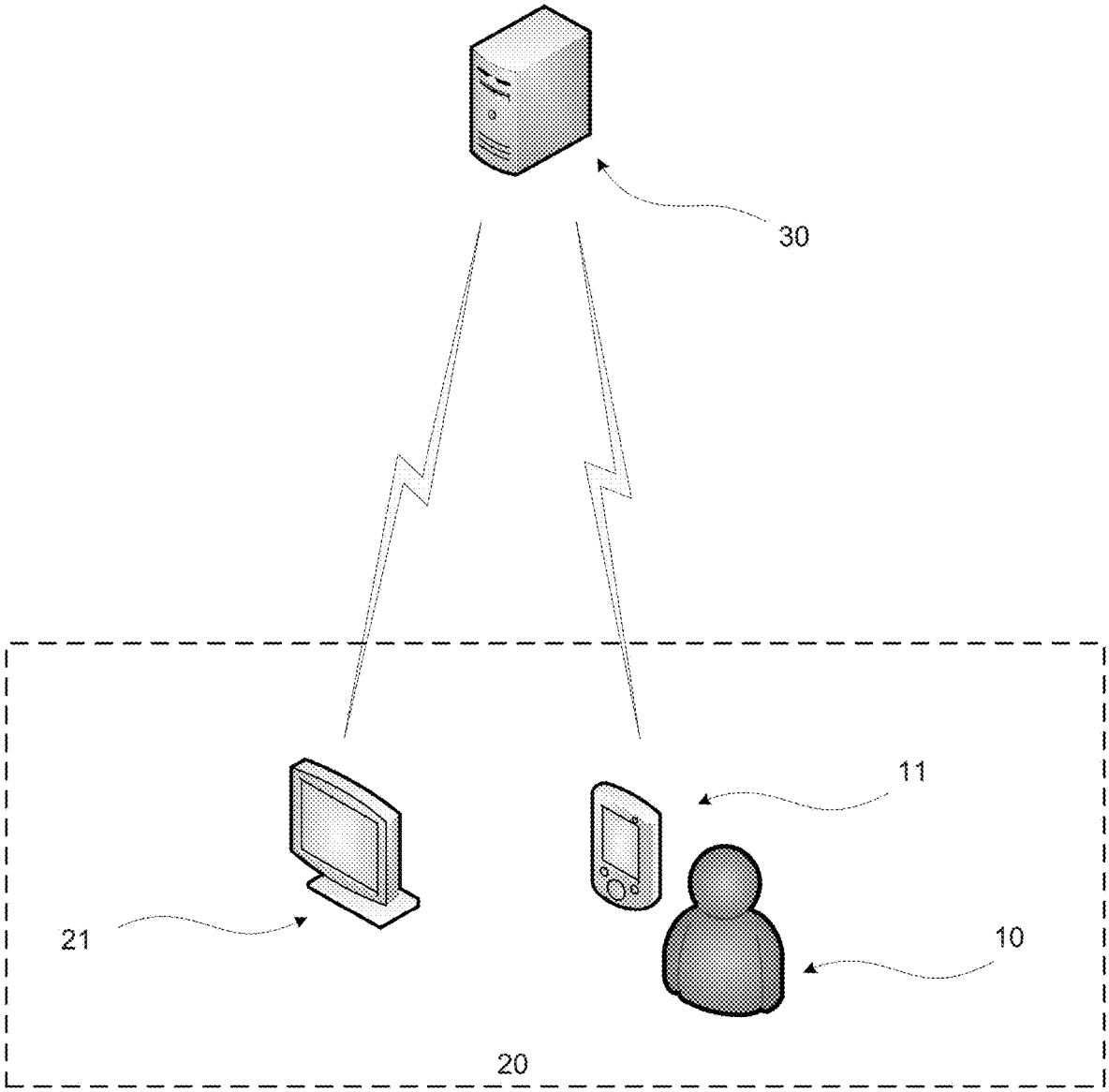


FIG. 1

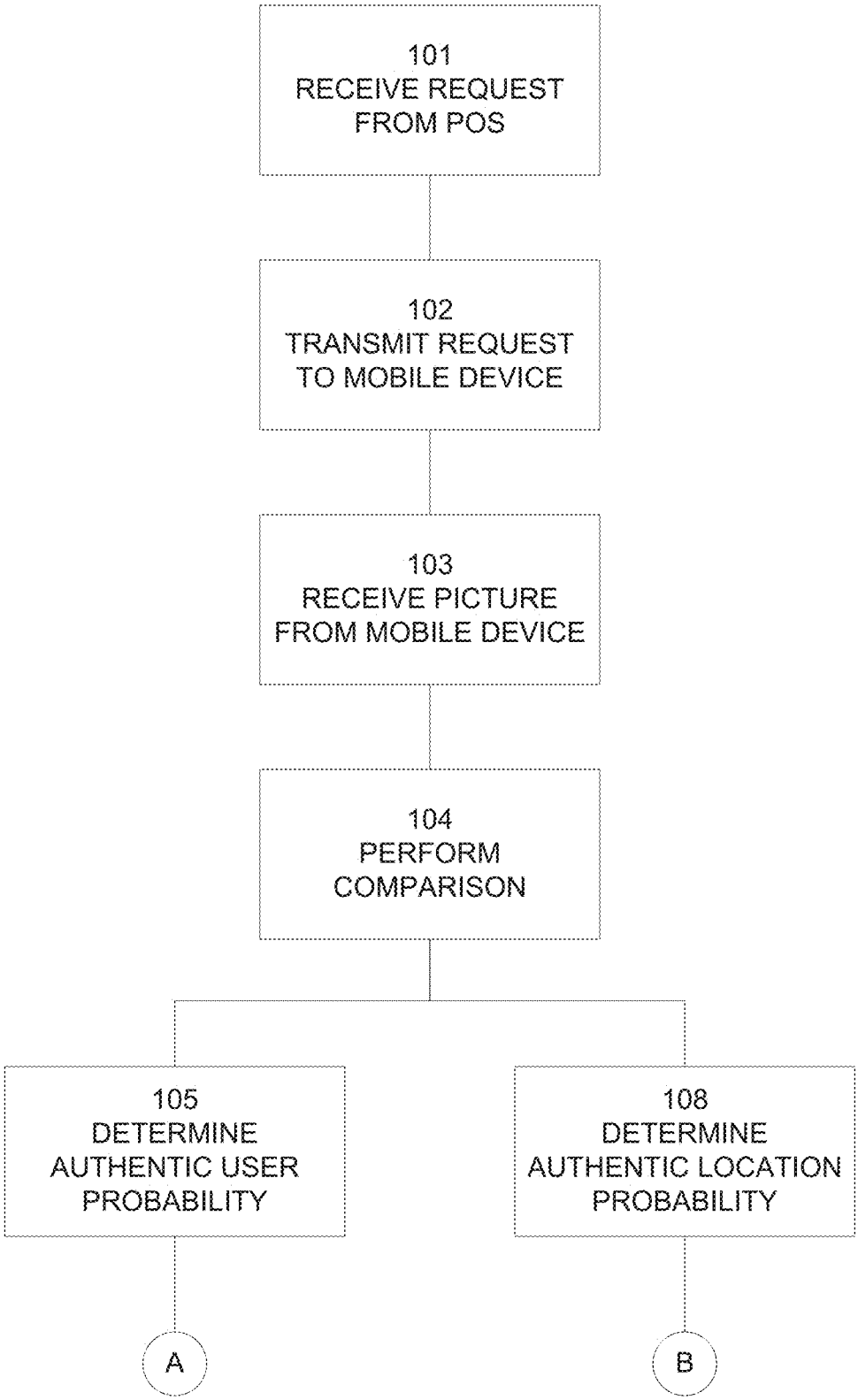

101
RECEIVE REQUEST
FROM POS
102
TRANSMIT REQUEST
TO MOBILE DEVICE
103
RECEIVE PICTURE
FROM MOBILE DEVICE
104
PERFORM
COMPARISON
105
DETERMINE
AUTHENTIC USER
PROBABILITY
108
DETERMINE
AUTHENTIC LOCATION
PROBABILITY
A
B

FIG. 2

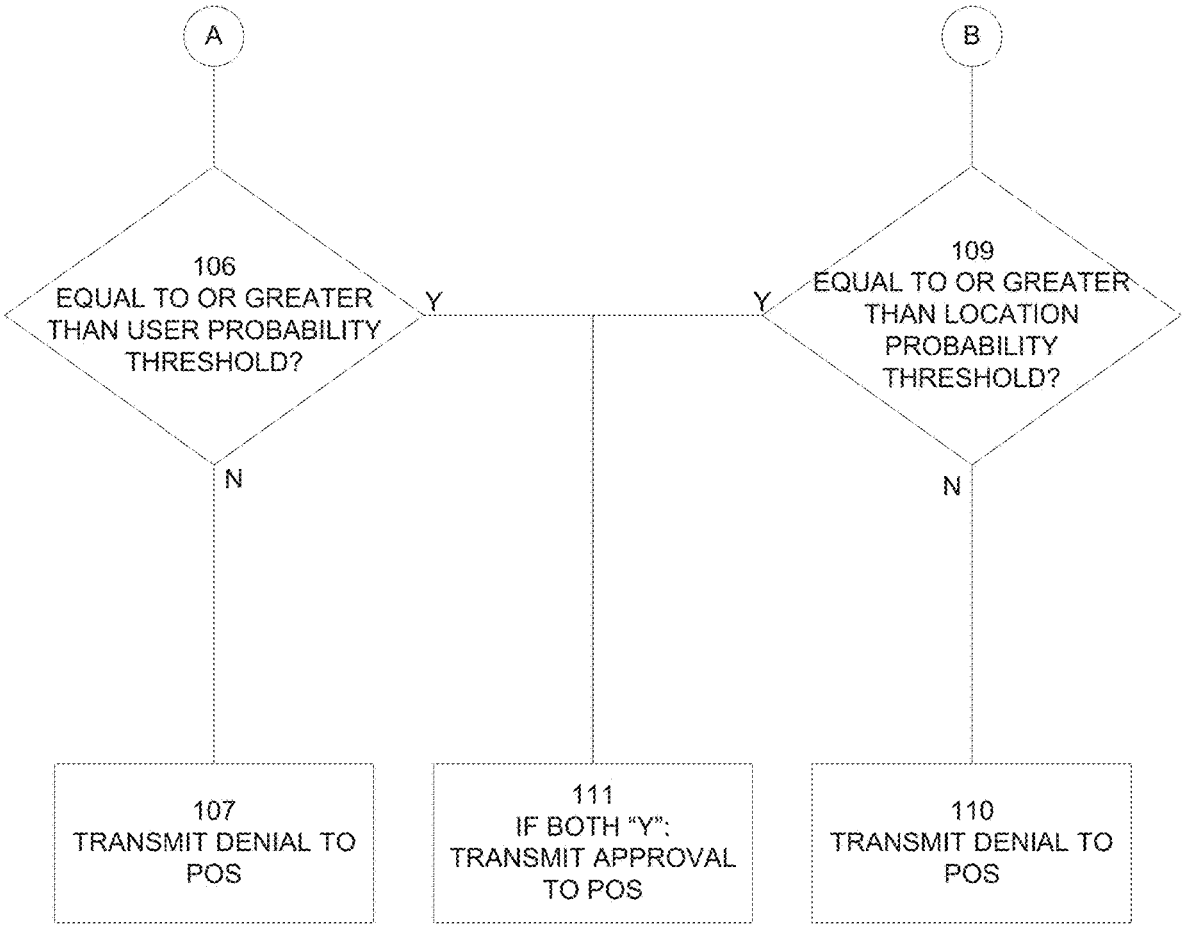

A
B
106
EQUAL TO OR GREATER THAN USER PROBABILITY THRESHOLD?
Y
Y
109
EQUAL TO OR GREATER THAN LOCATION PROBABILITY THRESHOLD?
N
N
107
TRANSMIT DENIAL TO POS
111
IF BOTH "Y": TRANSMIT APPROVAL TO POS
110
TRANSMIT DENIAL TO POS

FIG. 3

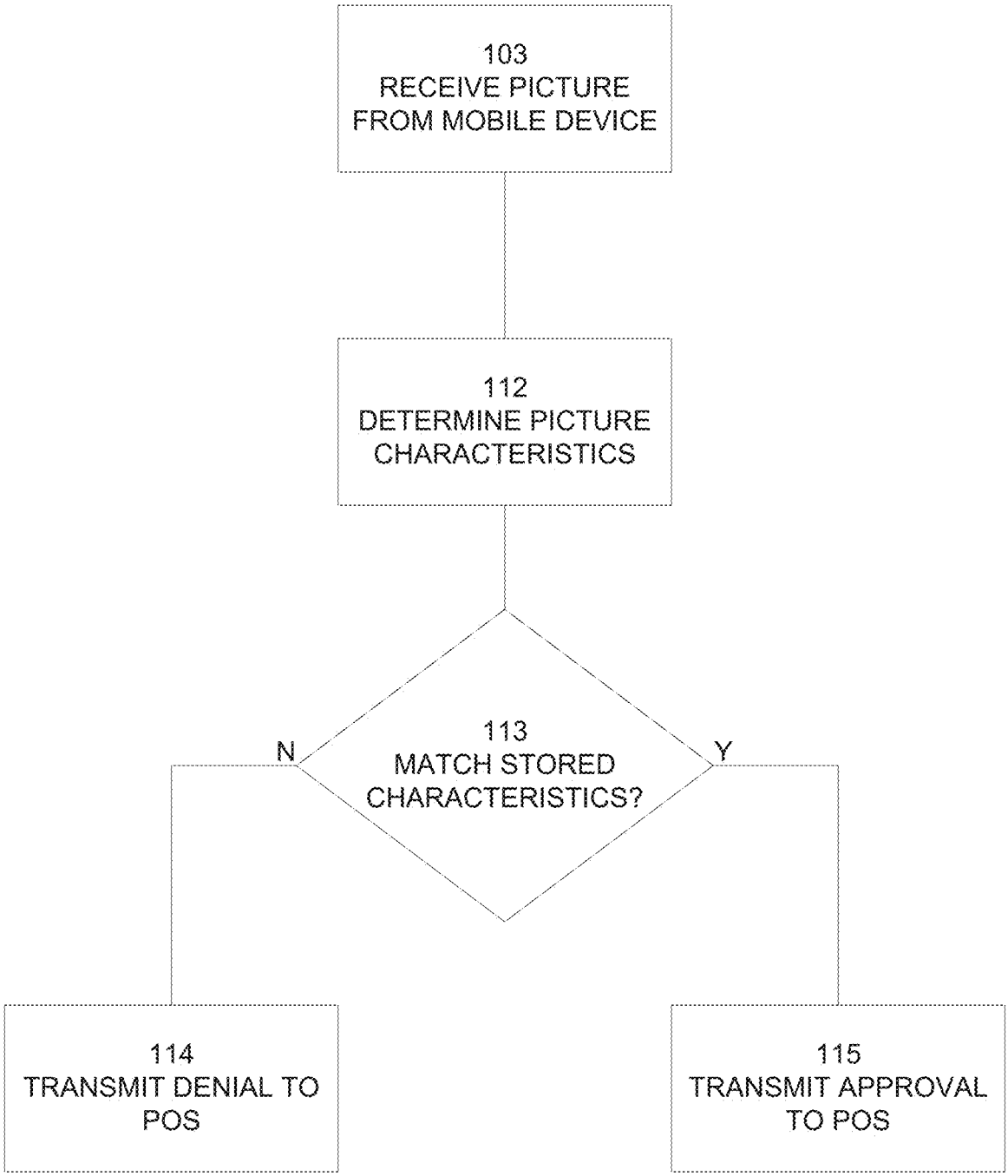

103
RECEIVE PICTURE FROM MOBILE DEVICE
112
DETERMINE PICTURE CHARACTERISTICS
113
MATCH STORED CHARACTERISTICS?
N
Y
114
TRANSMIT DENIAL TO POS
115
TRANSMIT APPROVAL TO POS

FIG. 4

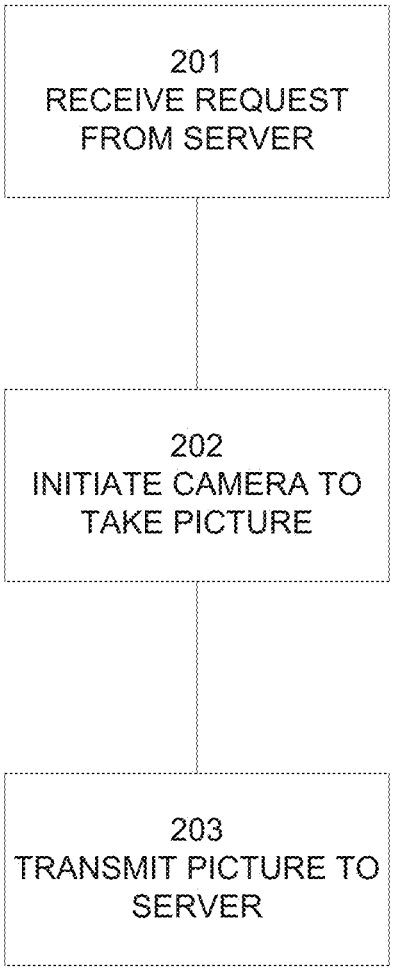

201
RECEIVE REQUEST FROM SERVER
202
INITIATE CAMERA TO TAKE PICTURE
203
TRANSMIT PICTURE TO SERVER

FIG. 5

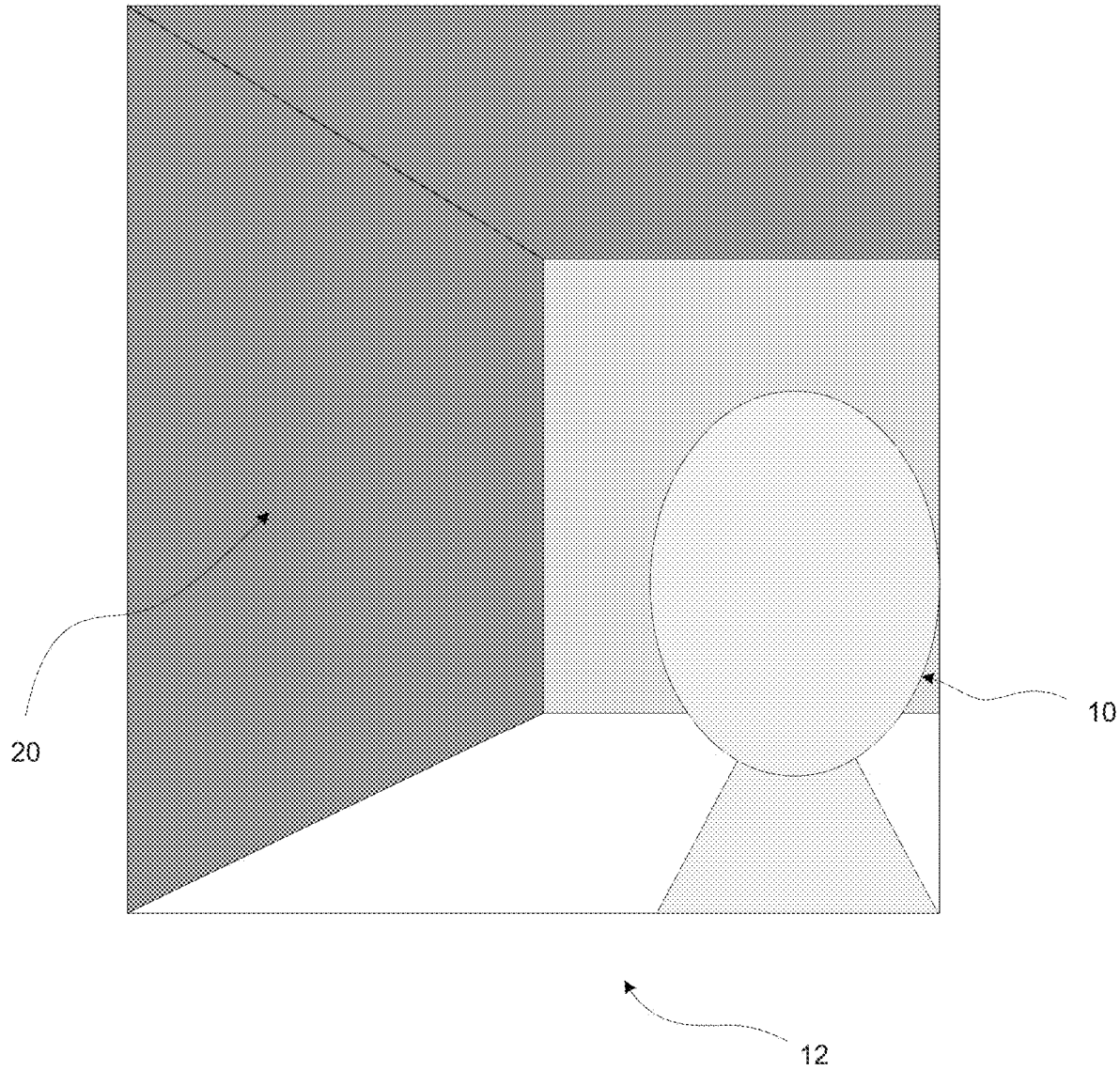


FIG. 6

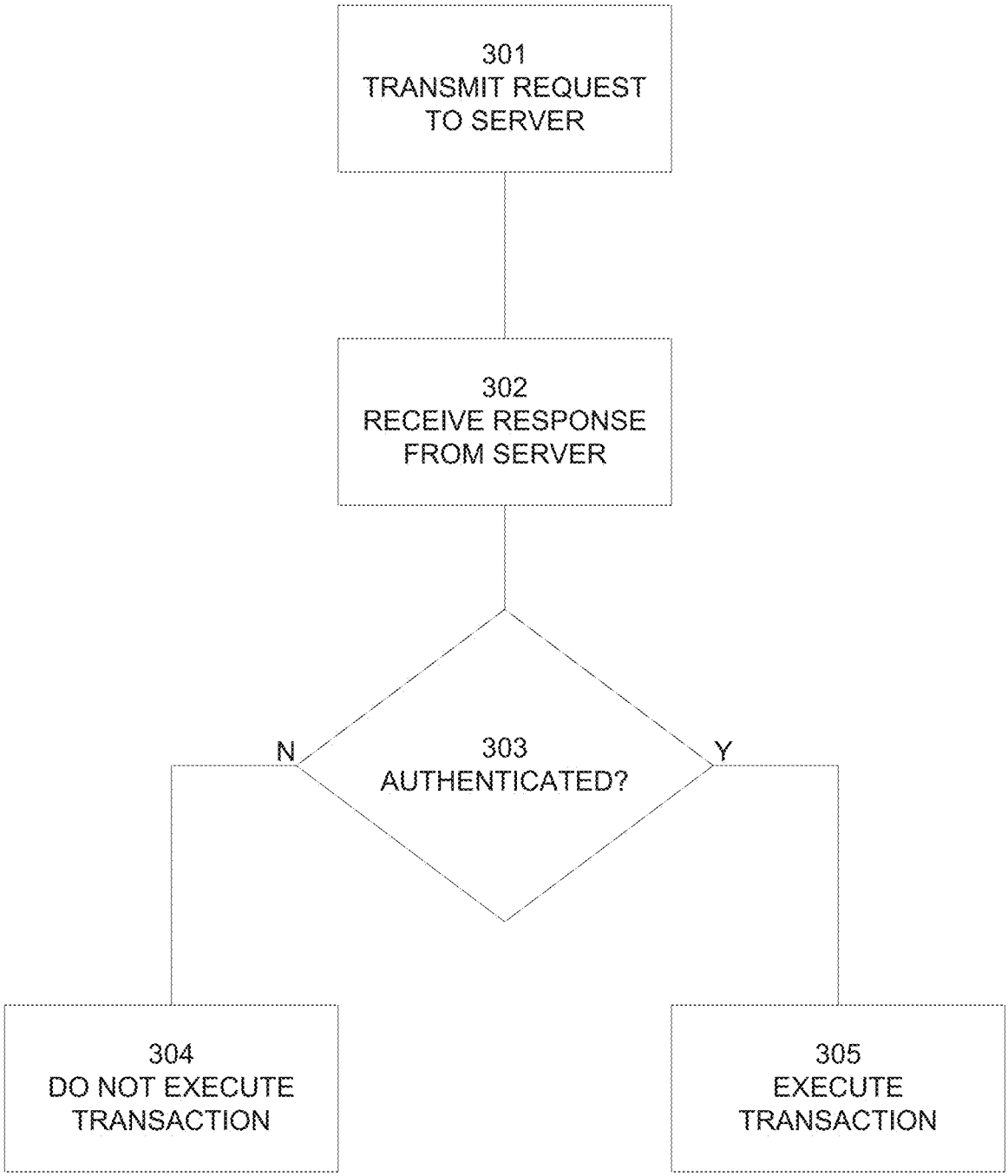

301
TRANSMIT REQUEST
TO SERVER
302
RECEIVE RESPONSE
FROM SERVER
303
AUTHENTICATED?
N
Y
304
DO NOT EXECUTE
TRANSACTION
305
EXECUTE
TRANSACTION

FIG. 7

SYSTEM AND METHOD FOR AUTHENTICATING TRANSACTIONS FROM A MOBILE DEVICE

FIELD OF THE INVENTION

[0001] The present invention relates to the authentication of transactions using a mobile device.

BACKGROUND

[0002] As mobile devices have become common among consumers, the corresponding popularity of executing transactions using those mobile devices has provided an increased opportunity for fraud, and an increased need to properly authenticate the participants to the transaction. Where those participants are identified by, or represented by, e.g., mobile devices or point-of-sale ("POS") devices, the need for authentication further extends to those devices. Systems for executing transactions using a mobile device to identify the user or consumer run the risk of executing the transaction for a false user, using a false device, or at a false merchant location.

[0003] If a false user is conducting the transaction using the mobile device, that false user may have obtained the mobile device through theft or fraud, and may have bypassed the user identification strategies of the mobile device. For example, the false user may have illegitimately identified the user's personal passwords, or forged a fingerprint capable of circumventing a fingerprint identification functionality of the mobile device. The variety of mobile devices available to consumers means that such mobile devices have varying levels of security functionality, leaving many users with limited ways to authenticate a transaction.

[0004] Further, authenticating the user alone does not achieve a sufficient level of security to protect the transaction. A false mobile device may be used for the transaction, for example, as a "spoofed" device mimicking the device of another consumer. A false merchant may be using a faked POS device to imitate a true merchant.

[0005] There is a need for systems and methods for authenticating transaction participants, using technology common to mobile devices.

SUMMARY

[0006] To address these problems, the following systems and methods authenticate components of a transaction: one party, the user; and the counterparty or merchant associated with a location such as a store or point of sale. Authenticating the location of the transaction, while also authenticating the user, provides necessary additional security for transactions that may otherwise be fraudulently executed. The user's mobile device may further be authenticated. The systems and methods of the present invention provide a greater level of security to transactions using mobile devices. Further, by utilizing a remote server, the additional security features are not limited to any particular mobile device; if the mobile device has access to a camera and to the remote server, it can use these security features.

[0007] In an exemplary embodiment, authenticating components of a transaction may include receiving, by an authentication server, via a network, an authentication request from a device associated with a location, the authentication request including information identifying a user participating in the transaction; transmitting, by the authentication server, via the network, a picture request to a mobile device associated with the user; receiving, by the authentication server, via the network, a picture taken by the mobile device in response to the picture request, wherein the picture includes an image of at least a portion of the user and at least a portion of the location; analyzing, by the authentication server, the image to determine the probability that the image includes the user, including comparing the image to images of the user stored in an identification database; analyzing, by the authentication server, the image to determine the probability that the image includes the location, including comparing the image to images of the location stored in the identification database; and, if the probability that the image includes the user is above a user probability threshold, and the probability that the image includes the location is above a location probability threshold, transmitting, by the authentication server, via the network, an authentication approval response to the device associated with the location.

[0008] The authentication may include comparing, by the authentication server, characteristics of the picture with information stored in the identification database, the information being associated with the mobile device, to determine the probability that the picture was taken by the mobile device associated with the user. The characteristics of the picture compared with information stored in the identification database may include at least one of the following: (a) pixel count; (b) resolution.

[0009] The picture may be taken by the mobile device in response to the picture request without additional commands from the user.

[0010] Analyzing the image to determine the probability that the image includes the user may include comparing the angle at which the picture was taken, with the angle of images of the user stored in an identification database.

[0011] The authentication may include automatically transmitting, from the mobile device, via the network, the images of the user to be stored in the identification database.

[0012] The authentication may include storing, in the identification database, images from previous picture requests associated with the user. The authentication may further include using the images from previous picture requests associated with the user to train the authentication server to determine the probability that an image includes the user.

[0013] The authentication may include storing, in the identification database, images from previous picture requests associated with the location. The authentication may further include using the images from previous picture requests associated with the location to train the authentication server to determine the probability that an image includes the location.

[0014] The step of analyzing the image to determine the probability that the image includes the user may be performed, and then the user's image may be removed from the image, and the step of analyzing the image to determine the probability that the image includes the location may then performed.

[0015] In an exemplary embodiment, a system for authenticating components of a transaction includes an identification database containing user identification information including reference images of a user, information identifying a mobile device associated with the user, and location identification information including reference images of a location; and an authentication server, in communication

with the identification database, including an authentication processor programmed to receive an authentication request from a device associated with the location, the authentication request including information identifying the user participating in the transaction; transmit a picture request to the mobile device; receive a picture taken by the mobile device in response to the picture request, wherein the picture includes an image of the at least a portion of the user and at least a portion of the location; analyze the image to determine the probability that the image includes the user, including comparing the image to images of the user stored in the identification database; analyze the image to determine the probability that the image includes the location, including comparing the image to images of the location stored in the identification database; and if the probability that the image includes the user is above a user probability threshold, and the probability that the image includes the location is above a location probability threshold, transmitting an authentication approval response to the device associated with the location.

[0016] The authentication server may be programmed to compare characteristics of the picture with information stored in the identification database, the information being associated with the mobile device, to determine the probability that the picture was taken by the mobile device associated with the user.

[0017] The authentication server may be programmed to compare the angle at which the picture was taken, with the angle of images of the user stored in an identification database.

[0018] The authentication server may be programmed to store, in the identification database, images from a previous picture request associated with the user; and use the stored images in later analysis to determine the probability that a later-taken image includes the user.

[0019] The authentication server may be programmed to store, in the identification database, images from a previous picture request associated with the location; and use the stored images in later analysis to determine the probability that a later-taken image includes the location.

[0020] The authentication server may be programmed to receive the results of a fingerprint identification taking place at the mobile device.

[0021] The authentication system may include the device associated with the location, and the device associated with the location may be programmed to execute the transaction only if the authentication server provides an authentication approval response.

[0022] The authentication server may be programmed to transmit an alert to the user if the probability that the image incudes the user is below the user probability threshold; and transmit an alert to the location if the probability that the image incudes the location is below the user probability threshold.

[0023] In an exemplary embodiment, authenticating components of a transaction may include receiving, by a mobile device associated with a user, via a network, a picture request from an authentication server; initiating a camera associated with the mobile device to take a picture, wherein the picture includes an image of at least a portion of the user and at least a portion of a real-time location of the user; and transmitting, by the mobile device, via the network, the picture to the authentication server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] FIG. **1** is an illustration of an authentication system, in accordance with an example embodiment of the present invention.

[0025] FIG. **2** is a flowchart illustrating a method for determining the probability of an authentic user and merchant location, in accordance with an example embodiment of the present invention.

[0026] FIG. **3** is a flowchart illustrating a method for determining the authenticity of a user and merchant location, in accordance with an example embodiment of the present invention.

[0027] FIG. **4** is a flowchart illustrating a further method for determining the authenticity of a user mobile device, in accordance with an example embodiment of the present invention.

[0028] FIG. **5** is a flowchart illustrating a method for obtaining input for determining the authenticity of a user, a user mobile device, or a merchant location, in accordance with an example embodiment of the present invention.

[0029] FIG. **6** is an illustration of an exemplary picture to be used in the authentication system, in accordance with an example embodiment of the present invention.

[0030] FIG. **7** is a flowchart illustrating a method for requesting a determination of the authenticity of a user, a user mobile device, or a merchant location, and responding thereto, in accordance with an example embodiment of the present invention.

DETAILED DESCRIPTION

[0031] The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. The embodiments described should be recognized as capable of implementation separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the invention. The description of embodiments should facilitate understanding of the invention to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the invention.

[0032] In a transaction between a user and a merchant, the user may be represented electronically by a mobile device, and the merchant may be represented electronically by a point-of-sale ("POS") device. The following systems and methods operate to authenticate the user, the merchant, or their respective devices.

[0033] The overall system is illustrated broadly in FIG. **1**. The user **10**, carrying mobile device **11**, seeks to execute a transaction with a merchant (not pictured) at the merchant's location **20**, such as a store, office, booth, or any other physical place of business where repeated transactions are executed.

[0034] Mobile device **11** may be any known mobile device, such as a smartphone, personal digital assistant, tablet computer, wearable device (such as a smartwatch), digital camera, or other computing device capable of communicating with a remote server **30** or capable of local

communication with a local device for communicating with a remote server **30**. The mobile device **11** includes a camera, and the ability to connect to a remote server on a network, such as via the Internet. At least some portion of the systems and methods described as being carried out by the mobile device may be divided among mobile devices carried by the user. For example, if the user is carrying one device communicating with a remote server (such as a smartphone), and a separate device for taking pictures (such as a wearable computing device), the two mobile devices of the user may coordinate to carry out the invention.

[0035] The merchant's location **20** includes POS device **21**. POS device **21** may be a computing device, capable of connecting to a remote server on a network, such as via the Internet.

[0036] To authenticate the requested transaction, the user's mobile device **11** and the merchant's POS device **21** communicate with a remote authentication server **30**. Server **30** includes an identification database for storing information associated with a user or merchant. For example, the identification database may store account information, contact information (e.g., telephone numbers, email addresses, IP addresses associated with mobile devices or POS devices), pictures and other information used to authenticate a user, a user's mobile device, or a merchant location in which the user and merchant are attempting to execute a transaction. Server **30** further includes processing capabilities for writing into the identification database, reading from the identification database, and comparing information received from the mobile device **11** and POS device **21** to the information stored in the identification database. The information stored in the identification database may also be stored across multiple databases, as long as the server **30** is able to access the information as needed.

[0037] In an exemplary embodiment, as illustrated in FIGS. **2** and **3**, when the user and/or the merchant initiates a transaction, at step **101** the POS device **21** transmits an authentication request to the authentication server **30**. The request may include information purporting to identify the participants in the transaction, such as the user, the user's mobile device, the merchant, or the POS. The identification information may take the form of readily identifiable information, e.g., names or addresses, or may take the form of coded or indexed reference information, e.g., usernames or customer numbers. The request may further include information describing the transaction, such as the nature of a product or service provided by the merchant or the value of goods being exchanged.

[0038] Upon receiving the request from the POS device **21**, the server **30** extracts the user identification information to associate the request with a user. The server **30** then identifies contact information for the user's mobile device **11**, such as a telephone number, email address, or IP address. At step **102**, the server initiates a communication to the mobile device **11**, the communication including a request for a picture.

[0039] Upon receiving the request from the server **30**, the mobile device **11** may initiate the exemplary embodiment illustrated in FIG. **5**. At step **201**, the mobile device **11** receives the request from the server, and parses the request to determine that the server **30** is requesting a picture. The mobile device **11** then initiates a connected camera to take a picture. The camera may be built into the mobile device **11**, or may be connected (either by wire, or wirelessly) to the mobile device.

[0040] In an exemplary embodiment, the request from the server **30** initiates a message to be displayed on the mobile device **11**, informing the user that a picture is necessary to carry out the transaction. The user may then operate the mobile device **11** to take a picture including at least some part of the user, and at least some part of the location. Once the picture is taken, the mobile device **11** may be used to transmit the picture back to the server **30**. The picture may include additional information identifying the user **10**, the mobile device **11**, and the transaction for which these authentication procedures are supporting.

[0041] The request from the server **30** may also include an alternative for the user **10** to provide some indication that the transaction should not be executed. For example, if the user did not initiate the transaction, then the request for the picture will serve as an alert the user that the transaction has been initiated, and the user may be provided with an icon or button for declining the transaction. This may take the form of a command to the server **30** to deny authentication of the transaction.

[0042] In an alternative exemplary embodiment, the request from the server **30** may ask for the picture to be taken without displaying an alert on the mobile device **11**, or without input from the user. In this manner, if the mobile device **11** has been stolen and is being used illegitimately to carry out the transaction, the illegitimate user will not be made aware of the security measures being enacted, limiting the ability of the illegitimate user to thwart these measures.

[0043] Returning to the exemplary embodiment illustrated in FIGS. **2** and **3**, the server **30** receives the picture from the mobile device at step **103**. The server **30** then carries out recognition processes, at steps **104-106** to compare the picture to information stored in the identification database and determine the probability that the user, or the merchant location, is authentic.

[0044] To identify the user **10**, the server **30** may use facial recognition programming to compare the image of the user **10** captured in the instant picture, to pictures of the user stored on the identification database. The identification database may store a collection of pictures of the user **10**, to be used in identifying the user **10** in the authentication process. For example, the user **10** may be required to take, or upload, one or more pictures of the user **10**, possibly from various angles, at a time prior to the transaction, such as when the user's identity can be confirmed in other ways. The server **30** may also request that the mobile device **11** transmit any pictures of the user **10** that are stored locally on the mobile device **11**, or stored on another server that the mobile device **11** may access. Further, the server **30** may store in the identification database any pictures of the user **10** that are used for authenticating a transaction, to assist in future authentication processes.

[0045] The server processes the picture to compare the image of the user to the images of the user previously stored in the identification database. For example, the server may use machine learning (e.g., a convolutional neural network) to process the previously-stored pictures of the user and compare them to the picture of the user taken during the instant authentication process. The server **30** may compare certain features depicted in the instant image (e.g., hair color, skin tone, size ratio of facial features) to the previ-

ously-stored pictures. Recognizing that each user may have a unique, and repeated, way to hold their mobile devices, the server **30** may compare the angle of the picture to the angle of other pictures taken during previous authentication processes.

[0046] As a result of this comparison, at step **105**, the server determines an authentic user probability, i.e., the probability that the pictured user is authentic. The authentic user probability may be determined based on any metric known to image recognition processing or convolutional neural network models. The authentic user probability may be impacted by several factors. For example, the number of stored pictures of the user in the identification database may impact the authentic user probability. The greater the number of pictures of the user stored in the identification database, the more readily the server will be able to identify the user, so that an identification of the user may be considered more probable if it is based on a large number of pictures. At step **106**, the server compares the user probability to a user probability threshold. If the determined user probability is below the user probability threshold, then, at step **107**, the server transmits an authentication denial to the POS device **21**, instructing the POS device **21** not to execute the transaction. The server **30** may also send a notification to the user or merchant that a fraudulent transaction has been attempted. If the determined user probability is equal to or greater than the user probability threshold, then the server **30** checks whether the determined location probability is equal to or greater than the location probability threshold. If both the determined user probability and the determined location probability are equal to or greater than their respective thresholds, then, at step **111**, the server **30** transmits an authentication approval to the POS device **21**, instructing the POS device **21** to execute the transaction. The server **30** may also send a notification to the user or merchant that the transaction has been authenticated. The threshold may be defined or adjusted as desired. For example, a high threshold will result in a higher level of security, but will increase the risk that a valid transaction being denied and will use more processing resources, while a low threshold will lessen the level of security, but will reduce the inconvenience of a denied valid transaction and will allow for faster processing.

[0047] To identify the location **20**, the server **30** may use visual imagery recognition programming to compare the image of the location **20** captured in the instant picture, to pictures of the location stored on the identification database. The identification database may store a collection of pictures of the location **20**, to be used in identifying the location **20** in the authentication process. For example, the merchant may be required to take, or upload, one or more pictures of the location **20**, possibly from angles that are expected to by commonly used by users in the authentication processes, at a time prior to the transaction, such as when the location's authenticity can be confirmed in other ways. The server **30** may store in the identification database any pictures of the location **20** that are used for authenticating a transaction (whether by the instant user or by other users), to assist in future authentication processes.

[0048] In particular, the stored pictures of the location may be focused on particular POS devices **21** within a merchant location **20**. For example, if a merchant location has five POS devices, the pictures taken by a user's mobile device **11** may include different parts of the location, depending on which POS device **21** is executing the transaction. Therefore, each POS device **21** may have its own associated pictures.

[0049] The server processes the picture to compare the image of the location to the images of the location previously stored in the identification database, associated with the relevant POS device **21**. For example, the server may use machine learning (e.g., a convolutional neural network) to process the previously-stored pictures of the location and compare them to the picture of the location taken during the instant authentication process. The server **30** may compare certain features depicted in the instant image (e.g., color or materials of the walls, ceiling, or floor, identifying damage, the size ratio of visible structures) to the previously-stored pictures. The server **30** may compare the angle of the picture to the angle of other pictures taken during previous authentication processes, that were associated with that particular POS device **21**.

[0050] As a result of this comparison, at step **108**, the server determines an authentic location probability, i.e., the probability that the pictured location is authentic. The authentic location probability may be determined based on any metric known to image recognition processing or convolutional neural network models. The authentic location probability may be impacted by several factors. For example, the number of stored pictures of the location in the identification database may impact the authentic location probability. The greater the number of pictures of the location stored in the identification database, the more readily the server will be able to identify the location, so that an identification of the location may be considered more probable if it is based on a large number of pictures. At step **109**, the server compares the location probability to a location probability threshold. If the determined location probability is below the location probability threshold, then, at step **110**, the server transmits an authentication denial to the POS device **21**, instructing the POS device **21** not to execute the transaction. The server **30** may also send a notification to the user or merchant that a fraudulent transaction has been attempted. If the determined location probability is equal to or greater than the location probability threshold, then the server **30** checks whether the determined user probability is equal to or greater than the location probability threshold. If both the determined user probability and the determined location probability are equal to or greater than their respective thresholds, then, at step **111**, the server **30** transmits an authentication approval to the POS device **21**, instructing the POS device **21** to execute the transaction. The server **30** may also send a notification to the user or merchant that the transaction has been authenticated. The threshold may be defined or adjusted as desired. For example, a high threshold will result in a higher level of security, but will increase the risk that a valid transaction being denied and will use more processing resources, while a low threshold will lessen the level of security, but will reduce the inconvenience of a denied valid transaction and will allow for faster processing.

[0051] Identifying a location may present a more difficult processing task than identifying a user. For example, as various users may appear in different positions in a picture, different portions of the location will appear in different pictures, and different portions will be obscured by the image of the user. It may be advantageous to set a lower location probability threshold, for example, in comparison to

the user probability threshold. It may further be advantageous to set a limit on the minimum number of stored pictures that must be determined to match the location before the location can be considered properly identified.

[0052] In an exemplary embodiment, steps **105** and **106** for authenticating the user may be carried out first, before steps **108** and **109** for authenticating the location. The server **30** may process the picture to recognize and authenticate the image of the user **10**. Once the user **10** has been authenticated, the server may again process the picture by removing the image of the user, and then exclusively processing the image of the location.

[0053] The server may be able to identify the user or location based on one stored picture, but the ability of the server to properly identify the user or location may increase with the number of stored pictures. The server may also undergo regular training to improve its recognition. For example, the server may be implementing a particular machine learning model in its recognition processes, and that model may be updated as additional pictures or other information yield improvements. In a particular example, the server may be trained regularly, e.g., once per day, at a time when the server typically experiences low service requirements, e.g., early morning. The model may also be developed and updated on a separate server, and loaded to the server **30**.

[0054] In certain embodiments, for example, in the use of a convolutional neural network, the embeddings of the pictures may be stored in the identification server, instead of the entire picture. The embeddings are a small vector of numbers that represents the picture. This will help to reduce storage space and calculation time.

[0055] An exemplary embodiment of the picture **12** is illustrated in FIG. **6**. The user **10** is depicted in the foreground of picture **12**, with at least a portion of the location **20** captured in the background. The illustration of FIG. **6** is exemplary; the picture **12** should include at least some part of the user sufficient to identify that user, and at least some part of the background location sufficient to identify the location. In the exemplary illustration of FIG. **6**, the image of the user **10** may be compared to the images in the pictures of the user stored in the identification database, and the image of the background location **20** may be compared to the images in the pictures of the background location **20** stored in the identification database, or, more specifically, with those pictures associated with the POS device **21** that being used in the transaction.

[0056] In addition to authenticating the user **10**, and the location **20**, the picture taken by the mobile device **11** may be used to authenticate the mobile device **11**, for an additional layer of security. In the exemplary embodiment illustrated in FIG. **4**, the server **30** receives the picture form the mobile device **11**, just as in FIGS. **2** and **3**. The picture may have certain characteristics useful in identifying the mobile device **11**. For example, the picture may have a certain size, ratio, pixel quality, or pixel count. At step **112**, these characteristics may be determined by the server in analyzing the picture, or may be included in metadata transmitted with the picture. The server **30** may have characteristics of the mobile device **11** stored in the identification database, allowing the server **30**, at step **113**, to match the characteristics of the picture to determine whether the mobile device **11** that took the picture is the mobile device associated with the user **10**. If the information matches, the server **30** may transmit an authentication approval to the POS device **21**, instructing the POS device **21** not to execute the transaction. If the information does not match, the server **30** may transmit an authentication denial to POS device **21**, instructing the POS device **21** to execute the transaction. In either case, the server **30** may also send a notification to the user or merchant including the results of the comparison.

[0057] In an exemplary embodiment, the process of the POS device **21** is illustrated in FIG. **7**. After transmitting an authentication request to the server **30** in step **301**, the POS device **21** waits for the response from the server **30**, which may include an authentication approval or an authentication denial. At step **302**, the POS device **21** receives the response from the server **30**, and determines, at step **303**, whether the response is an approval or a denial. If the server **30** provided an authentication denial, then at step **304** the POS device **21** does not execute the transaction. If the server **30** provided an authentication approval, then at step **305** the POS device **21** executes the transaction.

[0058] The present disclosure is not to be limited in terms of the particular embodiments described in this application, which are intended as illustrations of various aspects. Many modifications and variations can be made without departing from its spirit and scope, as may be apparent. Functionally equivalent methods and apparatuses within the scope of the disclosure, in addition to those enumerated herein, may be apparent from the foregoing representative descriptions. Such modifications and variations are intended to fall within the scope of the appended representative claims. The present disclosure is to be limited only by the terms of the appended representative claims, along with the full scope of equivalents to which such representative claims are entitled. It is also to be understood that the terminology used herein is for the purpose of describing particular embodiments only, and is not intended to be limiting.

1. A method for authenticating components of a transaction, comprising:

receiving, by an authentication server, via a network, an authentication request from a device associated with a location, the authentication request including information identifying a user participating in the transaction, wherein the authentication request is responsive to the initiation of the transaction between a mobile device associated with the user and the device associated with the location, wherein the mobile device is associated with a camera and is configured to communicate with the authentication server and the device associated with the location;

transmitting, by the authentication server, via the network, a picture request to the mobile device;

receiving, by the authentication server, via the network, a picture taken by the associated camera of the mobile device in response to the picture request;

analyzing, by the authentication server, the picture to determine the probability that the picture includes an image of at least a portion of the user, including comparing the picture to images of the user stored in an identification database;

analyzing, by the authentication server, the picture to determine the probability that the picture includes an image of at least a portion of the location other than the device associated with the location, including comparing the picture to images of the location stored in the identification database; and

if the probability that the picture includes an image of the user is above a user probability threshold, and the probability that the picture includes an image of the location is above a location probability threshold, transmitting, by the authentication server, via the network, an authentication approval response to the device associated with the location.

2. The method of claim **1**, further comprising:

comparing, by the authentication server, characteristics of the picture with information stored in the identification database, the information being associated with the mobile device, to determine the probability that the picture was taken by the mobile device associated with the user.

3. The method of claim **2**, wherein the characteristics of the picture compared with information stored in the identification database include at least one of the following: (a) pixel count; (b) resolution.

4. The method of claim **1**, wherein the picture request causes the mobile device to take the picture without additional commands from the user.

5. The method of claim **1**, wherein the step of analyzing the image to determine the probability that the picture includes the user further comprises:

comparing the angle at which the picture was taken, with the angle of images of the user stored in an identification database.

6. The method of claim **1**, further comprising:

automatically transmitting, from the mobile device, via the network, the images of the user to be stored in the identification database.

7. The method of claim **1**, further comprising:

storing, in the identification database, images from previous picture requests associated with the user.

8. The method of claim **7**, further comprising:

using the images from previous picture requests associated with the user to train the authentication server to determine the probability that an image includes the user.

9. The method of claim **1**, further comprising:

storing, in the identification database, images from previous picture requests associated with the location.

10. The method of claim **9**, further comprising:

using the pictures from previous picture requests associated with the location to train the authentication server to determine the probability that a picture includes an image of the location.

11. The method of claim **1**, wherein the step of analyzing the picture to determine the probability that the picture includes an image of at least a portion of the user is performed, and then the user's image is removed from the picture, and the step of analyzing the picture to determine the probability that the picture includes an image of at least a portion of the location is performed.

12. A system for authenticating components of a transaction, comprising:

an identification database containing user identification information including reference images of a user, information identifying a mobile device associated with the user, and location identification information including reference images of a location; and

an authentication server, in communication with the identification database, including an authentication processor programmed to:

receive an authentication request from a device associated with the location, the authentication request including information identifying the user participating in the transaction, wherein the authentication request is responsive to the initiation of the transaction between the mobile device and the device associated with the location, wherein the mobile device is associated with a camera and is configured to communicate with the authentication server and the device associated with the location;

transmit a picture request to the mobile device;

receive a picture taken by the associated camera of the mobile device in response to the picture request;

analyze the picture to determine the probability that the picture includes an image of at least a portion of the user, including comparing the picture to images of the user stored in the identification database;

analyze the picture to determine the probability that the picture includes an image of at least a portion of the location other than the device associated with the location, including comparing the picture to images of the location stored in the identification database; and

if the probability that the picture includes an image of the user is above a user probability threshold, and the probability that the image includes an image of the location is above a location probability threshold, transmitting an authentication approval response to the device associated with the location.

13. The system of claim **12**, the authentication server further programmed to:

compare characteristics of the picture with information stored in the identification database, the information being associated with the mobile device, to determine the probability that the picture was taken by the mobile device associated with the user.

14. The system of claim **12**, the authentication server further programmed to:

compare the angle at which the picture was taken with the angle of images of the user stored in an identification database.

15. The system of claim **12**, the authentication server further programmed to:

store, in the identification database, images from a previous picture request associated with the user; and

use the stored images in later analysis to determine the probability that a later-taken image includes the user.

16. The system of claim **12**, the authentication server further programmed to:

store, in the identification database, images from a previous picture request associated with the location; and

use the stored images in later analysis to determine the probability that a later-taken image includes the location.

17. The system of claim **12**, the authentication server further programmed to:

receive the results of a fingerprint identification taking place at the mobile device.

18. The system of claim **12**, further comprising the device associated with the location, wherein the device associated with the location is programmed to execute the transaction only if the authentication server provides an authentication approval response.

19. The system of claim **12**, the authentication server further programmed to:

transmit an alert to the user if the probability that the image incudes the user is below the user probability threshold; and

transmit an alert to the location if the probability that the image incudes the location is below the user probability threshold.

20. A method for authenticating components of a transaction, comprising:

receiving, by a mobile device associated with a user, via a network, a picture request from an authentication server;

initiating a camera associated with the mobile device to take a picture, wherein the picture includes an image of at least a portion of the user and at least a portion of a real-time location of the user; and

transmitting, by the mobile device, via the network, the picture to the authentication server.

21. The method of claim **1**, wherein the analyzing of the picture to determine the probability that the picture includes an image of at least a portion of the location is based on at least one of (i) a color of a wall, ceiling, or floor of the location, (ii) damaged portions of a wall, ceiling, or floor of the location, and (iii) a size ratio of a visible structure within the location.

* * * * *