System And Method For Identifying A Payment Account To Process A Financial Transaction

Technical Field

[0001] The present invention relates generally to a system and a method for identifying a payment account to process a financial transaction.

Background

[0002] Mobile payments and wallet platforms are already in widespread use, and digital wallets have accelerated economic activity to unprecedented levels in recent years. Around the same time, technologies for face recognition and identification have dramatically improved; machine performances are already comparable to human level. Leveraging face or facial image as an authentication key has been pushed forward in the past few years and in certain regions of the world it found widespread use. However, pervasive use of “face” or “facial image” has also met strong opposition from privacy advocates, government and even sections of consumers. Early attempts for biometric based payment (e.g., using facial data) didn’t always highlight user’s real-time consent to access his/her payment account (e.g., a consent could be granted by the user once and then used for extended periods of time), lifetime of a data match (facial data match) or consent, opacity around source of reference images and entities who have access to data. In some markets this created a lot of confusion and suspicion around biometric based payments or other such biometric based authorizations.

[0003] There is thus a need for identifying a payment account of a user to process a financial transaction to address the above concerns and challenges. Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

Summary

[0004] In a first aspect, the present disclosure provides a method for identifying a payment account to process a financial transaction comprising: determining if a location of a payer device matches a location of a payee device; determining if an image of a payer taken at the location of the payee device matches a registered image of the payer in a database in communication with

a server; and identifying a payment account of the payer associated with the registered image of the payer to process the financial transaction in response to the determinations.

[0005] In a second aspect, the present disclosure provides a system for identifying a payment account to process a financial transaction, the system comprising: at least one processor; and at least one memory including computer program code; the at least one memory and the computer program code configured to, with at least one processor, cause the server at least to: determine if a location of a payer device matches a location of a payee device; determine if an image of a payer taken at the location of the payee device matches a registered image of the payer stored in a database in communication with a server; and identify a payment account of the payer associated with the registered image of the payer to process the financial transaction in response to the determinations.

[0006] Additional benefits and advantages of the disclosed embodiments will become apparent from the specification and drawings. The benefits and/or advantages may be individually obtained by the various embodiments and features of the specification and drawings, which need not all be provided in order to obtain one or more of such benefits and/or advantages.

Brief Description of the Drawings

[0007] Embodiments and implementations are provided by way of example only, and will be better understood and readily apparent to one of ordinary skill in the art from the following written description, read in conjunction with the drawings, in which:

[0008] Figure 1 shows a block diagram illustrating a system for identifying a payment account to process a financial transaction according to an embodiment of the present disclosure.

[0009] Figure 2 shows a flow chart illustrating a method for identifying a payment account to process a financial transaction according to an embodiment of the present disclosure.

[0010] Figure 3 shows a flow chart illustrating a lookup and matching process according to an embodiment of the present disclosure.

[0011] Figure 4 shows a flow chart illustrating a backend lookup process according to an embodiment of the present disclosure.

[0012] Figure 5 shows an example image of a payer taken at a location of a payee device and used for identifying the payer.

[0013] Figures 6 and 7 depict an exemplary server for identifying a payment account to process a financial transaction according to an embodiment of the present disclosure.

Detailed Description

Terms Description

[0014] Payment account – a payment account is a financial or transaction account that is used to fund and perform a transaction, such as a checking account, savings account, credit account, virtual payment account, etc. A financial or transaction account may be associated with a consumer, which may be any suitable type of entity such as a person, a family, a company, a corporation, a governmental entity, etc. A payment account may also be associated with a payment card, such as credit card, debit card, prepaid card, charge card, membership card, royalty card, promotional card, frequent flyer card, identification card, gift card, and/or may also relate to a digital wallet (which is also known as an e-wallet). A digital wallet is typically used to store various forms of electronic money to aid in completing e-commerce transactions (or wallet-based transactions). For example, it is possible to link / register one or more payment account/card to a digital wallet to perform a wallet-based transaction. It will be understood that each type of these payment account can be used as a method of payment for the online payment system described herein. The payment account includes account information such as an account number, account owner, and the like.

[0015] Financial transaction – a financial transaction refers to a payment transaction between two entities in which money or other financial benefit is exchanged from one entity to the other. The payment transaction may be a transfer of funds via a payment card and/or payment account, for the purchase of goods or services, for the repayment of debt, or for any other exchange of financial benefit as will be apparent to persons having skill in the relevant art. Such payment transactions may be processed via an issuer, payment network, and acquirer. Typically, the process for processing such a payment transaction may include at least one of authorization, batching, clearing, settlement, and funding. Authorization may include furnishing of payment details by the consumer to a merchant, the submitting of transaction details (e.g., including the payment details) from the merchant to their acquirer, and the verification of payment details with the issuer of the consumer's payment account used to fund the transaction. Batching may refer to the storing of an authorized transaction in a batch with other authorized transactions for

distribution to an acquirer. Clearing may include the sending of batched transactions from the acquirer to a payment network for processing. Settlement may include the debiting of the issuer by the payment network for transactions involving beneficiaries of the issuer. In some instances, the issuer may pay the acquirer via the payment network. In other instances, the issuer may pay the acquirer directly. Funding may include payment to the merchant from the acquirer for the payment transactions that have been cleared and settled. It will be apparent to persons having skill in the relevant art that the order and/or categorization of the steps discussed above performed as part of payment transaction processing.

[0016] User – a user may be any suitable type of entity, which may include a person, consumer, passenger, family, company, corporation, governmental entity who register a user account under a biometric based payment server/system (hereinafter may refer to as a remote assistance server) for identifying a payment account to process a financial transaction. Such registration step is called on-boarding. A user account identifier will be assigned to each user account (i.e., the user). In one embodiment, the remote assistance server may be connected to a payment network server, and a user account is thus associated with one or more payment accounts of the user, each of which can be used to process a financial transaction, i.e., transfer and receive money or other financial benefit. In various embodiments, unless otherwise is specified, a user refers to a person (i.e., payer) whose data and information associated his/her user account will be utilized to make a payment to goods and/or service providers such as a merchant in a merchant store, a driver in a vehicle (i.e., payee). Additionally, a payee could also register himself/herself a user account for receiving the payment from the payer.

[0017] Image – an image refers to a facial image or any other biometric data which could be processed and used for identifying a person (e.g., a user) and differentiating him/her from another person. In various embodiments, for identifying a payment account of a consumer for making a payment to a payee, an image of the consumer is taken at the location of a payee's device and send to the remote assistance server to verify the identity of the user prior to processing a financial transaction.

[0018] Registered image - a registered image refers to an image of user stored in a database in communication with the remote assistance server in communication with the payment application or digital wallet. In various embodiment, such registered image(s) is taken or uploaded by the user during the user account registration process. Additionally, the user is free to add new image or change the current registered image(s) in his/her account. Alternatively or additionally, an image of the user taken at a location of a payee device may be stored as a registered image in the database for future identification of the user.

[0019] Payer device – a payer device typically is associated with a customer (or payer) who is a party to a transaction. The payer device may be a handheld or portable or mobile device or other types of electronic devices such as a personal computer, a land-line telephone or an interactive voice response (IVR) system and the like carried by the customer when a financial transaction is initiated. The mobile device may be a device, such as a mobile phone, a laptop computer, a personal digital computer (PDA), a mobile computer, a portable music player (such as an iPod™ and the like).

[0020] Payee device – a payee device typically is associated with a good and/or service provider who is also a party to the transaction. The payee device may be a point-of-sale (POS) terminal, an automatic teller machine (ATM), a personal computer, a computer server (hosting a website, for example), an IVR system, a land-line telephone, or any type of mobile device such as a mobile phone, a personal digital assistant (PDA), a laptop computer, a tablet computer and the like. In various embodiments below, the payee device comprises an image capturing device or sensor configured to capture an image of a customer (or payer) who is the opposite party of the transaction, and the payee device is configured to send the captured image to the remote assistance server to verify the identity of the user prior to processing a financial transaction. Examples of image capturing devices and sensors includes depth sensor, RGB (red green blue) camera, IR (infra-red) camera, etc. In an alternative implementation, the image capture device is not part of the payee device but they are in communication with the via connections which may be through wire, wireless (e.g., via NFC communication, Bluetooth, etc.) or over a network (e.g., the Internet).

[0021] Location – a location corresponds to geolocation data of a device. In various embodiment, such geolocation data of the device may be obtained from a communication network or server in communication with the device such as a code division multiple access (CDMA) network or a global system for mobile communication (GSM) network. Additionally or alternatively, the geolocation data of the device may be obtained from Global Positioning System (GPS) signals received from satellites. The geolocation data includes latitude and longitude coordinates in any suitable format, such as: (i) Degrees, minutes, and seconds (DMS), (ii) Degrees and decimal minutes (DMM), and (iii) Decimal degrees (DD). In various embodiments below, geolocation and time data received by devices associated with a customer (or payer) and a merchant who are parties to a transaction are sent to the remote assistance server to determine if the devices' locations are close to one another prior to processing the transaction.

[0022] Presence – a presence of a person (e.g., user, payer) refers to an actual, live, three-dimensional (3D) appearance of the person at the location of the payee device (e.g., at the merchant store and inside a driver's vehicle) detected by the image capturing device or sensor associated with the payee device as the person appears within the field of view of (e.g., in front of) the image capturing device or sensor. A live appearance of a person may be detected from an image based on the person's physical characteristic like (i) facial feature which includes relative position, size, shape and/or contour of eyes, nose, lip, cheekbones, jaw and chin, and also iris pattern, skin colour, hair colour, other similar features or a combination thereof, and (ii) body feature which includes height, body size, body ratio, length of limbs, hair colour, skin colour, apparel, belongings, other similar features or a combination thereof. Such detection of a live presence of a payer at payee's location can protect the transaction from spoofing attacks like screen replay, printed faces, masks or other techniques.

[0023] In one embodiment, where facial images or any other biometric data are processed and used for identifying a person (e.g., a user, payer) and differentiating him/her from another person, the physical characteristic for detecting the presence of the person at the location of the payee device is obtained from such facial images or biometric data. For example, a 3D facial contour of a passenger in his/her facial image captured by a driver's device (payee device) may be analyzed to identify if the passenger is actually present in the driver's vehicle, and the facial image is then used for further processing, for example to match a registered facial image of the passenger in the server, and identify a user account and/or a payment account of the passenger.

Exemplary Implementations

[0024] Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

[0025] It is to be noted that the discussions contained in the "Background" section and that above relating to prior art arrangements relate to discussions of devices which form public knowledge through their use. Such should not be interpreted as a representation by the present inventor(s) or the patent applicant that such devices in any way form part of the common general knowledge in the art.

[0026] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer

memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0027] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “calculating”, “determining”, “updating”, “generating”, “initializing”, “outputting”, “receiving”, “retrieving”, “identifying”, “dispersing”, “authenticating” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0028] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[0029] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[0030] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer

readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0031] As described above, during a typical cashless payment processing the requirement is to identify a payment account of a customer, Existing options for payment account identification have been credit cards, phone-based wallets (QR code activated) etc. In this present disclosure, a payment account can be identified through facial data of a person. While looking up a facial data and other biometric data is frictionless, additional steps are taken to guard user's consents, privacy, and ensure transparency at all levels.

[0032] Figure 1 shows a block diagram illustrating a system for identifying a payment account to process a financial transaction according to an embodiment of the present disclosure.

[0033] The system 100 comprises payer devices used by consumers (users) who are registered with a remote assistance server 112. For the sake of simplicity, only one payer device 102 is illustrated in Figure 1. Examples of the payer devices are tablets, laptops, desktop computers, smartphones, and the like. The payer device 102 connects to the remote assistance server 112 via connections. The connections may be wired, wireless (e.g., via NFC communication, Bluetooth, etc.) or over a network (e.g., the Internet). The payer device 102 can communicate with the remote assistance server 112 and provide commands to the remote assistance server 112 in the form of voice, text, and the like.

[0034] The system 100 further comprises payee devices used by merchants or service providers who offer goods and services. For the sake of simplicity, only one payee device 104 is illustrated in Figure 1. Examples of the payee devices are tablets, laptops, desktop computers, smartphones, point-of-sales terminals, and the like. The payee devices may be used to present transaction records or transaction identifiers associated with the transaction records. The payee device 104 in communication with an acquirer server 106. The acquirer server 106, in turn, is in communication with the payment network server 108. The payment network server 108, in turn, is in communication with an issuer server 110. In an implementation, the payee device 104 connects with the remote assistance server 112 via connections. The connections may be wired, wireless (e.g., via NFC communication, Bluetooth, etc.) or over a network (e.g., the Internet). Similarly, the payee devices can communicate with the remote assistance server 112 and provide

commands to the remote assistance server 112 in the form of voice, text, and the like. As described above, a payee device 104 comprises an image capturing device configured to capture an image of a customer (or payer) who is the opposite party of the transaction, and the payee device is configured to send the captured image to the remote assistance server 112 to verify the identity of the user prior to processing a financial transaction.

[0035] Use of the term 'server' herein can mean a single computing device or a plurality of interconnected computing devices which operate together to perform a particular function. That is, the server may be contained within a single hardware unit or be distributed among several or many different hardware units.

[0036] The acquirer server 106 generally is associated with an acquirer who may be an entity (e.g., a company or organization) which issues (e.g., establishes, manages, administers) a transaction credential or an account (e.g., a financial bank account) of the merchant. Examples of the acquirer include a bank and/or other financial institution. The acquirer server 106 may include one or more computing devices that are used to establish communication with another server by exchanging messages with and/or passing information to the other server (e.g., payment network server 108 and issuer server 110, or other third-party server (not shown)).

[0037] The payment network server 108 typically is associated with a payment facilitator. The payment facilitator may be an entity (e.g., a company or organization) who operates to process transactions, clear and settle funds for payments between two entities (e.g., two banks). The payment network server 108 may include one or more computing devices that are used for processing transactions.

[0038] The issuer server 110 generally is associated with an issuer and may include one or more computing devices that are used to perform a payment transaction. The issuer may be an entity (e.g. a company or organization) which issues (e.g. establishes, manages, administers) a transaction credential, a financial bank account and a payment account of a user (payer). An account may be associated with a plurality of payer devices 102. That is, a payer may use a plurality of payer devices 102 including, among other things, his mobile phone, his PDA and his laptop to utilise his account.

[0039] The payment network server 108 may be configured to communicate with, or may include, a database (or a transaction database) 109. The transaction database 109 stores data corresponding to a transaction (or transaction data). Examples of the data include Transaction identifier (ID), Merchant ID, Merchant Name, MCC / Industry Code, Industry Description,

Merchant Country, Merchant Address, Merchant Postal Code, Aggregate Merchant ID. For example, data (“Merchant name” or “Merchant ID”) relating to the merchant, time and date for which the goods/ services relating to the transaction will be delivered, and a corresponding delivery option that has been utilised. In other words, the transaction database 109 stores information that indicates the types of delivery option that a merchant offers.

[0040] The remote assistance server 112 which is a server that hosts software application programs to function as a biometric based payment server 100, the biometric based payment server configured to identify a payment account of a person using biometric data of the person such as facial image. The structural context of the remote assistance server 112 is discussed below in relation to Figures 6A and 6B.

[0041] According to the present disclosure, In the illustrative embodiment, the remote assistance server 112 provides an interface to enable communication with each of devices 102, 104 and servers 106, 108. The remote assistance server 112 provides an application programming interface (“API”) to facilitate such communication. Such APIs may be part of a user interface that may include graphical user interfaces (GUIs), Web-based interfaces, programmatic interfaces such as application programming interfaces (APIs) and/or sets of remote procedure calls (RPCs) corresponding to interface elements, messaging interfaces in which the interface elements correspond to messages of a communication protocol, and/or suitable combinations thereof. Examples of APIs include the REST API, and the like.

[0042] The remote assistance server 112 is configured to receive and send commands and data (e.g., details of transaction records and associated transaction identifiers) from and to the devices 102, 104.

[0043] In one arrangement, the biometric-based payment system implemented in the remote assistance server 112 is compatible with existing payment application, payment gateways, digital wallets and the like. In another arrangement, the biometric-based payment system implemented in the remote assistance server 112 is an additional function on a payment application or digital wallet.

[0044] The remote assistance server 112 may be operated by any entity (e.g., a company or organization) different from an acquirer and a payment network server provider and the like. The remote assistance server 112 is in communication with the payment network server 108. Alternatively or additionally, the remote assistance server 112 is in communication with the acquirer server 106, as shown in Figure 1.

[0045] In an alternative embodiment, the remote assistance server 112 may be operated by any entity which includes at least one of an acquirer, a payment server provide, and the like. If the acquirer operates the remote assistance server 112, then the acquirer may integrate the acquirer server 106 with the remote assistance server 112. In another implementation, if the payment network server provider operates the remote assistance server 112, then the payment network server provider may integrate the payment network server 108 with the remote assistance server 112.

[0046] According to the present disclosure, a user may register himself/herself and create a user account via the remote assistance server 112 or connected payment application or digital wallet to access a face lookup and face based payment service. The user is required to upload one or more facial images to the remote assistance server 112. The remote assistance server 112 may also index the facial images so that they could be used for lookup and matching the user. The remote assistance server 112 is in communication with a database 113. The database 113 stores data relating to registered users of such biometric based payment service. Examples of the data include user name, user address, user account identifier, password, given name, identity card number, account numbers, contact number, facial images, biometric data, application settings. Optionally, the user may configure to have a list of user's preferred merchants/types of business, or a list of merchants or type of business authorized to access his/her data to perform facial lookup and payment transactions. Additionally, the database 113 may store transaction data of transactions completed through the remote assistance server 112. Such data stored in the database 113 may be accessible by respective users through their devices, e.g., payer device 102 and payee device 104.

[0047] The remote assistance server 112 may send a request for a consent to payer device 102 during registration process or any time thereafter to have his/her facial images registered for face lookup service via an application or connected payment or digital wallet applications and used for identifying a payment account to process financial transactions and make payments to a payee. The user explicitly agrees by sending a response to the request to provide his/her consent, for example, by toggle a setting, tapping a "confirm" button and inserting password or authentication key through the payer device 102. In one additional implementation, such facial images registration and provision of the user's consent have to be carried out prior to processing any financial transactions or and the consent precede any face-based payment.

[0048] According to the present disclosure, the system 100 (for example the remote assistance server 112) is configured to determine if a location of the payer device 102 matches a location of

the payee device 104; determine if an image of a user (i.e., customer/payer) taken at the location of the payee device matches his/her registered image(s) of the user, for example, associated with a user account of the user under a payment application or digital wallet, stored in the database 113 in communication with the remote assistance server 112; and identify a payment account of the user associated with his/her registered of the payer, for example, linked to the user account of the user under the payment application or digital wallet, to process the financial transaction in response to the determinations.

[0049] The payer device 102 and the payee device 104 may be further configured to receive location data corresponding to a location of the devices 102, 104. The payer device 102 and the payee device 104 may be configured to communicate with a third-party server (not shown) managed by another service provider to receive the geolocation data. The remote assistance server is further configured to receive or retrieve the location data of the payer device 102 and the payee device 104 and determine if a distance between the location of the payer device 102 and the location of the payee device 104 is within a threshold distance (e.g., within 20 meters) based on the location data.

[0050] The system 100 (for example the remote assistance server 112 of the system 100) may be further configured to receive a list of merchants or types of business (i.e., payees) authorized to perform a determination of an image of the payer at a payee device and/or perform a financial transaction with the user, and determine if the merchant associated with the payee device 104 is one of the list of payees or relates to one of the list of types of business in order to determine if the image of the user taken at the location of the payee device matches the registered image of the user. For example, if it is determined that the merchant associated with the payee device 104 is not one of the user's list of payee or relates to one of the list of types of business authorized to access user data (e.g., his/her registered images in his/her account) or perform transactions, the determination on whether the image of the payer taken at the location of the payee device matches the registered image of the payer will then not be carried out such that the financial transaction cannot be further processed. Advantageously, this promotes user's privacy as only merchants who are authorized by the user can uses his/her data (e.g., facial image and location data) to verify his/her location and real-time consent at the location of a payee (e.g., at the merchant store and inside a driver's vehicle), as well as prevent misuse of biometric data of the user to carry out transactions with merchants that have not been authorized by the user.

[0051] Figure 2 shows a flow chart illustrating a method 200 for identifying a payment account to process a financial transaction according to an embodiment of the present disclosure. In step 202, a step of determining if a location of a payer device matches a location of a payee device is

carried out. In step 204, a step of determining if an image of a payer taken at the location of the payee device matches a registered image of the payer in a database in communication with a server is carried out. In step 206, a step of identifying a payment account of the payer associated with the registered image of the payer to process a financial transaction.

[0052] Figure 3 shows a flow chart 300 illustrating a lookup and matching process according to an embodiment of the present disclosure. A kiosk (i.e., payee device) is present at a store counter and is equipped with various types of sensors such as a camera. The kiosk screen as shown in block 302 may display kiosk sale information 304 relating to goods and services that a customer wishes to purchase and a touch button 306 “Take Selfie for Payment” that will activate a camera upon tapping and take an image of the customer to make the payment. Such kiosk can be part of POS terminal or separated from POS terminal. Assuming the customer is a user who has registered with the face look-up service, the user agrees and taps on the kiosk screen 302 to use the face look-up service to make the payment. Although the following process is illustrated using a kiosk at a store counter, it is appreciated by a skilled person that the same process can apply to other payee device and location such as a mobile device of a driver in a car.

[0053] Subsequently, in step 308, a selfie picture (i.e., facial image) of the user (i.e., payer) is taken by the kiosk camera. Additionally, after the selfie picture is taken, it is then checked whether a live three-dimensional (3D) facial feature of the user can be detected from the image so as to ensure user’s liveness and presence in front of the kiosk camera through processing of a software on the kiosk and/or service backend. This protects the system from spoofing attacks like screen replay, printed faces, masks or other techniques. In one implementation, the kiosk with sensors collects data of the user in the merchant store and feed to service backend (i.e., server) with anti-spoofing deep neural networks to detect any spoofing events.

[0054] Then, in step 310, the selfie picture is sent to service backend (i.e., server) to perform a face lookup against registered users via multi-step ensemble. This face lookup is performed by comparing the selfie picture taken by the kiosk against registered images of registered users. In this case, a match between the picture taken by the kiosk and the registered images associated with the user account of the user is found and a notification is sent to a user’s device for a consent.

[0055] In various embodiments of the present disclosure, once a match is found, in step 312, it is determined if the personal device of the identified user is near to the kiosk or in the store (via location service). In an alternative implementation, when finding a match during the lookup process, registered images of users whose devices are at the same or near the location (via

location service) as the kiosk taking pictures are extracted and compared if any registered image matches the selfie picture taken at the kiosk.

[0056] In the notification sent to the user device, the user is explicitly asked whether the transaction should proceed with specific data and information stored for such face lookup service being shared to the merchant. In one implementation, transaction data such as the kiosk sale information and an identified user's payment account associated with the user account are included in the notification for the user to preview before he/she makes a decision. Users are able to revoke their consent at any point of time without providing a reason. During consent on their phone, users may have the option to see the picture that was captured by the kiosk, alongside reference images/sources.

[0057] In step 314, the user confirms the transaction by tapping on his/her device. In one implementation, the user is allowed to switch to another payment account associated with his/her user account for making the payment. In step 316, upon receiving the confirmation, the transaction is then processed, and the merchant will be notified about the transaction outcome.

[0058] Figure 4 shows a flow chart 400 illustrating a backend lookup process according to an embodiment of the present disclosure. In step 402, when an image of a user at a location of a payee device is captured, for example, after tapping the button "Take Selfie for Payment" on the screen of the kiosk at a merchant store or a mobile phone of a driver and taking a selfie, an image to face detection is carried out to detect a face or facial image (hereinafter referred to as "search input image"), for example, using a machine learning face detection algorithm trained to identify faces according to the location in which the system is implemented, for example, south east Asian faces in Singapore, as well as faces in indoor, outdoor, low light (night) conditions which occurs more typically for passengers and drivers. In steps 402 and 404, multiple parallel transfer learning based face vectorizations are carried out on the search input image, for example by resizing it to 224x224 pixels with RGB setting [224x224x3] and outputting a single 512 float vector array. Although two face vectorization algorithms with independent ways of output vector arrays from the search input image are leveraged in this embodiment, it should be appreciated by a skilled person that more or less than two face vectorization algorithms may be utilized in this step(s), depending on the implementations.

[0059] In step 408, a vector lookup such as a partitioned and indexed vector storage lookup is carried out to a search from a set of 50 million vectors under five second is carried out. In step 410, the vector loop for each of the vectorization algorithm outputs generate a set of high confidence candidates (i.e., likely matches / users with their registered images match substantially

with the search input image. For example, such matches may be determined based on a matching score indicating a degree of similarly between the registered images and the search input image, the matching score exceeding a certain threshold. Such threshold for collecting high confidence candidates may be determined based on previous matching results and accuracy. The set of high confidence candidates and their registered images may be sent to 1-1 match algorithm for face matching in subsequent steps.

[0060] In steps 412 and 414, candidate vectors are evaluated for direct one-to-one matching with their registered images and the search input image. Although two face matching algorithms with independent ways of looking at face images and performing the one-to-one matching are leveraged in this embodiment, it should be appreciated by a skilled person that more or less than two face matching algorithms may be utilized in this step(s), depending on the implementations.

[0061] In step 416, an ensemble model is run to predict a likelihood of a false positive (FP). There are two different ensemble approaches: (a) a simple and conservative approaches where all of the input algorithms (e.g., face match algorithm 1 in step 412 and face match algorithm 2 in step 412) need to result in a positive match, only then the overall outcome is directed as a valid fact match. An example code to carry out the ensemble approach is shown in code (a) below; and (b) a weighted ensemble where outputs of different algorithms are given different weights in determining the output. An example code to carry out the ensemble approach is shown in code (b) below.

Code (a):

```
is_face_match(input_image, candidate_image) = is_match_alg1(input_image,
candidate_image) AND is_match_alg2(input_image, candidate_image) AND ...
```

Code (b)

```
face_match_probability(input_image, candidate_image) = w1 *
match_prob_alg1(input_image, candidate_image) + w2 *
match_prob_alg2(input_image, candidate_image) + w3 * ...
```

[0062] In step 418, a final output of identified face such as a user account of the server identified from the search input image is generated. Such user account can then be used to identify a payment associated with it for making payment and processing the financial transaction.

[0063] Optionally, in step 418, a fraction of automated face match obtained in step 416 may be evaluated by a human operator to improve the quality and accuracy of the prediction result. In particular, the matches labelled by the ensemble model are checked if they were correct or wrong. Such evaluation may be carried out using more than one human operator to avoid biases, and the outcome is then averaged and compiled for machine learning training. In step 422, a set of previous search input images with known prediction results may be input to retrain the ensemble method to generate better and more accurate predictions on a daily basis. Different sets of previous search input may be used on different days. It is appreciated by a skilled person that the frequency of the retaining can be changed, for example, to twice a day or once a week depending on the implementation.

[0064] When running the set of previous search input images, the ensemble parameters and weights are modified and optimized such that the model, using the optimized parameters and weights, will then generate prediction results that match the known prediction results. As a result, the ensemble models will generate having more accurate output of identified face in step 418 over time.

[0065] Figure 5 shows an example image 502a, 504a of a payer taken at a location of a payee device and used for identifying the payer. Screen 502 may be a screen displayed by a kiosk (i.e., payee device) at a merchant store after a user (i.e., payer) taps a button “Take Selfie for Payment” on the screen of the kiosk as shown in Figure 3, or a screen display on a mobile phone (i.e., payee device) of a driver (i.e., payee). The user may position his/her face in front of a camera of the payee device to take a selfie picture of himself/herself, a preview of image presently recorded by the camera may be displayed on the screen, as illustrated in screen portion 502a. In an implementation, an instructional text or icon 502b may also be displayed on the screen 502a to provide instructions to the user or payee to take the selfie picture, and a touch button 502c on the screen 502a that is, upon pressing, configured to provide instructions to the payee device to record the selfie picture and send the recorded selfie picture to a server to identify the user.

[0066] In this example, the user Kyle Measner is identified and a welcome text along with his name 504b is displayed on the screen 502b. The recorded selfie picture may be displayed on the screen potion 504a. A touch button 504c may also be displayed on the screen 502a and configured to provide instructions to the payee device to retake another selfie picture or go back to the previous screen / interface as illustrated in screen 502.

[0067] Figures 6 and 7 depict an exemplary server, for example the remote assistance server 112 of Figure 1, for identifying a payment account to process a financial transaction according to

an embodiment of the present disclosure, upon which the biometric based payment system described above can be practiced.

[0068] As seen in Figure 6, the remote assistance server 112 includes: a computer module 601; input devices such as a keyboard 602, a mouse pointer device 603, a scanner 626, a camera 627, and a microphone 680; and output devices including a printer 615, a display device 614 and loudspeakers 617. An external Modulator-Demodulator (Modem) transceiver device 616 may be used by the computer module 601 for communicating to and from a communications network 620 via a connection 621. The communications network 620 may be a wide-area network (WAN), such as the Internet, a cellular telecommunications network, or a private WAN. Where the connection 621 is a telephone line, the modem 616 may be a traditional "dial-up" modem. Alternatively, where the connection 621 is a high capacity (e.g., cable) connection, the modem 216 may be a broadband modem. A wireless modem may also be used for wireless connection to the communications network 660.

[0069] The input and output devices may be used by an operator who is interacting with the remote assistance server 112. For example, the printer 615 may be used to print reports relating to the status of the remote assistance server 112.

[0070] The remote assistance server 112uses the communications network 620 to communicate with the payee device 104 and the payer device102 to receive commands and data. The remote assistance server 112 also uses the communications network 620 to communicate with the payee device 104, the payer device 102 to send notification messages or transaction data.

[0071] The computer module 601 typically includes at least one processor unit 605, and at least one memory unit 606. For example, the memory unit 606 may have semiconductor random access memory (RAM) and semiconductor read only memory (ROM). The computer module 601 also includes a number of input/output (I/O) interfaces including: an audio-video interface 607 that couples to the video display 614, loudspeakers 617 and microphone 680; an I/O interface 613 that couples to the keyboard 602, mouse 603, scanner 626, camera 627 and optionally a joystick or other human interface device (not illustrated); and an interface 608 for the external modem 616 and printer 615. In some implementations, the modem 616 may be incorporated within the computer module 601, for example within the interface 608. The computer module 601 also has a local network interface 611, which permits coupling of the computer system 112 via a connection 223 to a local-area communications network 622, known as a Local Area Network (LAN). As illustrated in Figure 6, the local communications network 622 may also couple to the wide network 620 via a connection 624, which would typically include a so-called "firewall" device

or device of similar functionality. The local network interface 611 may comprise an Ethernet circuit card, a Bluetooth® wireless arrangement or an IEEE 802.11 wireless arrangement; however, numerous other types of interfaces may be practiced for the interface 611.

[0072] The I/O interfaces 608 and 613 may afford either or both of serial and parallel connectivity, the former typically being implemented according to the Universal Serial Bus (USB) standards and having corresponding USB connectors (not illustrated). Storage devices 609 are provided and typically include a hard disk drive (HDD) 610. Other storage devices such as a floppy disk drive and a magnetic tape drive (not illustrated) may also be used. An optical disk drive 612 is typically provided to act as a non-volatile source of data. Portable memory devices, such optical disks (e.g., CD-ROM, DVD, Blu-ray Disc™), USB-RAM, portable, external hard drives, and floppy disks, for example, may be used as appropriate sources of data to the remote assistance server 112.

[0073] The components 605 to 613 of the computer module 601 typically communicate via an interconnected bus 604 and in a manner that results in a conventional mode of operation of a computer system known to those in the relevant art. For example, the processor 605 is coupled to the system bus 604 using a connection 618. Likewise, the memory 606 and optical disk drive 612 are coupled to the system bus 604 by connections 619. Examples of computers on which the described arrangements can be practised include IBM-PC's and compatibles, Sun Sparcstations, Apple Mac™ or like computer systems.

[0074] The methods of operating the remote assistance server 112, as shown in the processes of Figures 2-4 to be described, may be implemented as one or more software application programs 633 executable within the remote assistance server 112. In particular, the steps of the methods shown in Figures 2-4 are effected by instructions 231 (see Figure 7) in the software (i.e., computer program codes) 633 that are carried out within the remote assistance server 112. The software instructions 631 may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part and the corresponding code modules performs the operation of the remote assistance server 112 and a second part and the corresponding code modules manages the API and corresponding user interfaces in the payee device 104, the payer device 102, and on the display 614. In other words, the second part of the software manages the interaction between (a) the first part and (b) any one of the payee device 104, the payer device 102, and the operator of the server 112.

[0075] The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the remote assistance server 112 from the computer readable medium, and then executed by the computer system 112. A computer readable medium having such software or computer program recorded on the computer readable medium is a computer program product. The use of the computer program product in the remote assistance server 112 preferably effects an advantageous apparatus for identifying a payment account for processing a financial transaction, functioning as a biometric based payment system.

[0076] The software (i.e., computer program codes) 633 is typically stored in the HDD 610 or the memory 606. The software 633 is loaded into the computer system 112 from a computer readable medium (e.g., the memory 606), and executed by the processor 605. Thus, for example, the software 633 may be stored on an optically readable disk storage medium (e.g., CD-ROM) 625 that is read by the optical disk drive 612. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the assistance server 112 preferably effects an apparatus for identifying a payment account for processing a financial transaction, for functioning as a biometric based payment system.

[0077] In some instances, the application programs 633 may be supplied to the user encoded on one or more CD-ROMs 625 and read via the corresponding drive 612, or alternatively may be read by the user from the networks 620 or 622. Still further, the software can also be loaded into the remote assistance server 112 from other computer readable media. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the remote assistance server 112 for execution and/or processing by the processor 605. Examples of such storage media include floppy disks, magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, USB memory, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computer module 601. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computer module 601 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0078] The second part of the application programs 633 and the corresponding code modules mentioned above may be executed to implement one or more API of the remote assistance server

112 with associated graphical user interfaces (GUIs) to be rendered or otherwise represented upon the display 614 or the display of the payee device 104 and the payer device 102. Through manipulation of typically the keyboard 602 and the mouse 603, an operator of the server 110 and the application may manipulate the interface in a functionally adaptable manner to provide controlling commands and/or input to the applications associated with the GUI(s). Similarly, on the payee device 104 and the payer device 102, a user of those devices 102, 104 manipulate the input devices (e.g., touch screen, keyboard, mouse, etc.) of those devices 102, 104 in a functionally adaptable manner to provide controlling commands and/or input to the applications associated with the GUI(s). Other forms of functionally adaptable user interfaces may also be implemented, such as an audio interface utilizing speech prompts output via the loudspeakers 617 and user voice commands input via the microphone 680. These other forms of functionally adaptable user interfaces may also be implemented on the payee device 104 and the payer device 102.

[0079] Figure 7 is a detailed schematic block diagram of the processor 605 and a “memory” 634. The memory 634 represents a logical aggregation of all the memory modules (including the HDD 609 and semiconductor memory 606) that can be accessed by the computer module 601 in Figure 6.

[0080] When the computer module 601 is initially powered up, a power-on self-test (POST) program 650 executes. The POST program 650 is typically stored in a ROM 649 of the semiconductor memory 606 of Figure 6. A hardware device such as the ROM 649 storing software is sometimes referred to as firmware. The POST program 650 examines hardware within the computer module 601 to ensure proper functioning and typically checks the processor 605, the memory 634 (609, 606), and a basic input-output systems software (BIOS) module 651, also typically stored in the ROM 649, for correct operation. Once the POST program 650 has run successfully, the BIOS 651 activates the hard disk drive 610 of Figure 6. Activation of the hard disk drive 610 causes a bootstrap loader program 652 that is resident on the hard disk drive 610 to execute via the processor 605. This loads an operating system 653 into the RAM memory 606, upon which the operating system 653 commences operation. The operating system 653 is a system level application, executable by the processor 605, to fulfil various high level functions, including processor management, memory management, device management, storage management, software application interface, and generic user interface.

[0081] The operating system 653 manages the memory 634 (609, 606) to ensure that each process or application running on the computer module 601 has sufficient memory in which to execute without colliding with memory allocated to another process. Furthermore, the different

types of memory available in the server 110 of Figure 6 must be used properly so that each process can run effectively. Accordingly, the aggregated memory 634 is not intended to illustrate how particular segments of memory are allocated (unless otherwise stated), but rather to provide a general view of the memory accessible by the server 110 and how such is used.

[0082] As shown in Figure 7, the processor 605 includes a number of functional modules including a control unit 639, an arithmetic logic unit (ALU) 640, and a local or internal memory 648, sometimes called a cache memory. The cache memory 648 typically includes a number of storage registers 644 - 646 in a register section. One or more internal busses 641 functionally interconnect these functional modules. The processor 605 typically also has one or more interfaces 642 for communicating with external devices via the system bus 604, using a connection 618. The memory 634 is coupled to the bus 604 using a connection 619.

[0083] The application program 633 includes a sequence of instructions 631 that may include conditional branch and loop instructions. The program 633 may also include data 632 which is used in execution of the program 233. The instructions 631 and the data 632 are stored in memory locations 628, 629, 630 and 635, 636, 637, respectively. Depending upon the relative size of the instructions 631 and the memory locations 628-630, a particular instruction may be stored in a single memory location as depicted by the instruction shown in the memory location 630. Alternately, an instruction may be segmented into a number of parts each of which is stored in a separate memory location, as depicted by the instruction segments shown in the memory locations 628 and 629.

[0084] In general, the processor 605 is given a set of instructions which are executed therein. The processor 605 waits for a subsequent input, to which the processor 605 reacts to by executing another set of instructions. Each input may be provided from one or more of a number of sources, including data generated by one or more of the input devices 602, 603, data received from an external source across one of the networks 620, 602, data retrieved from one of the storage devices 606, 609 or data retrieved from a storage medium 625 inserted into the corresponding reader 612, all depicted in Figure 6. The execution of a set of the instructions may in some cases result in output of data. Execution may also involve storing data or variables to the memory 634.

[0085] The disclosed association management and payment initiation arrangements use input variables 654, which are stored in the memory 634 in corresponding memory locations 655, 656, 657. The association management and payment initiation arrangements produce output variables 661, which are stored in the memory 634 in corresponding memory

locations 662, 663, 664. Intermediate variables 258 may be stored in memory locations 659, 660, 666 and 667.

[0086] Referring to the processor 605 of Figure 7, the registers 644, 645, 646, the arithmetic logic unit (ALU) 640, and the control unit 639 work together to perform sequences of micro-operations needed to perform “fetch, decode, and execute” cycles for every instruction in the instruction set making up the program 633. Each fetch, decode, and execute cycle comprises: a fetch operation, which fetches or reads an instruction 631 from a memory location 628, 629, 630 ; a decode operation in which the control unit 639 determines which instruction has been fetched; and an execute operation in which the control unit 639 and/or the ALU 640 execute the instruction.

[0087] Thereafter, a further fetch, decode, and execute cycle for the next instruction may be executed. Similarly, a store cycle may be performed by which the control unit 639 stores or writes a value to a memory location 632.

[0088] Each step or sub-process in the processes of Figures 2-4 is associated with one or more segments of the program 633 and is performed by the register section 644, 645, 647, the ALU 640, and the control unit 639 in the processor 605 working together to perform the fetch, decode, and execute cycles for every instruction in the instruction set for the noted segments of the program 633.

[0089] It is to be understood that the structural context of the remote assistance server 112 is presented merely by way of example. Therefore, in some arrangements, one or more features of the remote assistance server 112 may be omitted. Also, in some arrangements, one or more features of the remote assistance server 112 may be combined together. Additionally, in some arrangements, one or more features of the transaction portal server 110 may be split into one or more component parts.

[0090] The foregoing describes only some embodiments of the present disclosure, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

Claims

1. A method for identifying a payment account to process a financial transaction comprising:

determining if a location of a payer device matches a location of a payee device;

determining if an image of a payer taken at the location of the payee device matches a registered image of the payer in a database in communication with a server; and

identifying a payment account of the payer associated with the registered image of the payer to process the financial transaction in response to the determinations.

2. The method according to claim 1, further comprising:

detecting a presence of the payer at the location of the payee device based on a physical feature of the payer in the image of the payer.

3. The method according to claim 2, wherein the step of determining if the image of the payer taken at the location of the payee device matches the registered image of the payer in the database in communication with the server comprises:

determining if the physical feature in the image of the payer taken at the location of the payee device matches the physical feature in the registered image of the payer in a database in communication with a server.

4. The method according to claim 1, wherein the step of determining if a location of the payer device matches the location of the payee device comprises:

extracting location data of the payer device and the payee device; and

determining if a distance between the location of the payer device and the location of the payee device is within a threshold distance based on the location data.

5. The method according to claim 1, further comprising:

receiving, prior to the financial transaction, a list of payees or types of business authorized to perform a determination of an image of the payer at a payee device;

determining if the payee is one of the list of payees or relates to one of the list of types of business, wherein the step of determining if the image of the payer taken at the location of the payee device matches the registered image of the payer is carried out in response to the determination of the payee being one of the list of payees or relates to one of the list of types of business.

6. The method according to claim 1, further comprising:

receiving, prior to the financial transaction, an authorization from the payer to perform a determination of an image of the payer at the terminal.

7. The method according to claim 1, further comprising:

sending, to the payer device, transaction data corresponding to the financial transaction and a request for a verification of the transaction data.

8. The method according to claim 1, in response to the determinations, further comprising:

sending, to the payer device, a request for a consent to send at least one of the image of the payer and information associated with account of the payer to the payee when processing the financial transaction.

9. The method according to claim 8, wherein the request comprises the image of the payer taken at the location of the terminal.

10. The method according to any one of claims 7 to 9, further comprising:

receiving, from the device of the payer, a response to the request, wherein the step of identifying the payment account of the payer associated with the registered image of the payer to process the financial transaction is carried out in response to the receipt of the response.

11. A system for identifying a payment account to process a financial transaction, the system comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with at least one processor, cause the server at least to:

determine if a location of a payer device matches a location of a payee device;

determine if an image of a payer taken at the location of the payee device matches a registered image of the payer stored in a database in communication with a server; and

identify a payment account of the payer associated with the registered image of the payer to process the financial transaction in response to the determinations.

12. The system according to claim 11, wherein the at least one memory and the computer program code is further configured with the at least one processor to:

detect a presence of the payer at the location of the payee device based on a physical feature of the payer.

13. The system according to claim 12, wherein the at least one memory and the computer program code is further configured with the at least one processor to:

determine if the physical feature in the image of the payer taken at the location of the payee device matches the physical feature in the registered image of the payer in a database in communication with a server.

14. The system according to claim 11, wherein the at least one memory and the computer program code is further configured with the at least one processor to:

receive location data of the payer device and the payee device; and

determine if a distance between the location of the payer device and the location of the payee device is within a threshold distance based on the location data.

15. The system according to claim 11 wherein the at least one memory and the computer program code is further configured with the at least one processor to:

receive, prior to the financial transaction, a list of payees or types of business authorized to perform a determination of an image of the payer at a payee device; and

determine if the payee is one of the list of payees or relates to one of the list of types of business wherein the at least one memory and the computer program code is further configured with the at least one processor to determine if the image of the payer taken at the location of the payee device matches the registered image of the payer in response to determining if the payee is the one of the list of payees or relates to the one of the list of types of business.

16. The system according to claim 11 wherein the at least one memory and the computer program code is further configured with the at least one processor to:

receive, prior to the financial transaction, an authorization from the payer to perform a determination of an image of the payer at the payee device.

17. The system according to claim 11 wherein the at least one memory and the computer program code is further configured with the at least one processor to:

send, to the payer device, transaction data corresponding to the financial transaction and a request for a verification of the transaction data.

18. The system according to claim 11 wherein the at least one memory and the computer program code is further configured with the at least one processor to:

send, to the payer device, a request for a consent to send at least one of the image of the payer and information associated with account of the payer to the payee when processing the financial transaction.

19. The system according to claim18, wherein the request comprises the image of the payer taken at the location of the payee device.

20. The system according to any one of claims 14-19, wherein the at least one memory and the computer program code is further configured with the at least one processor to:

receive, from the device of the payer, a response to the request, wherein the at least one memory and the computer program code is further configured with the at least one processor to identify the payment account of the payer associated with the registered image of the payer to process in response to the receipt of the response.