



(51) International Patent Classification:

G06Q 20/32 (2012.01) G06Q 20/20 (2012.01)  
G06Q 20/00 (2012.01) G06Q 20/38 (2012.01)  
G06Q 20/40 (2012.01)

(21) International Application Number:

PCT/US2017/017558

(22) International Filing Date:

10 February 2017 (10.02.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/293,418 10 February 2016 (10.02.2016) US

(71) Applicant: AINTU INC. [US/US]; 111 N. Market Street, Suite 300, San Jose, California 95113 (US).

(72) Inventor: VAYSMAN, Arthur; 2196 Heather Brook Court, San Jose, California 95138 (US).

(74) Agent: MOODLEY, Vani; HM LAW GROUP LLP, 19925 Stevens Creek Blvd, Suite 100, Cupertino, California 95014 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available):

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

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

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

Published:

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

(54) Title: SYSTEM AND METHOD FOR CONTACTLESS PAYMENTS

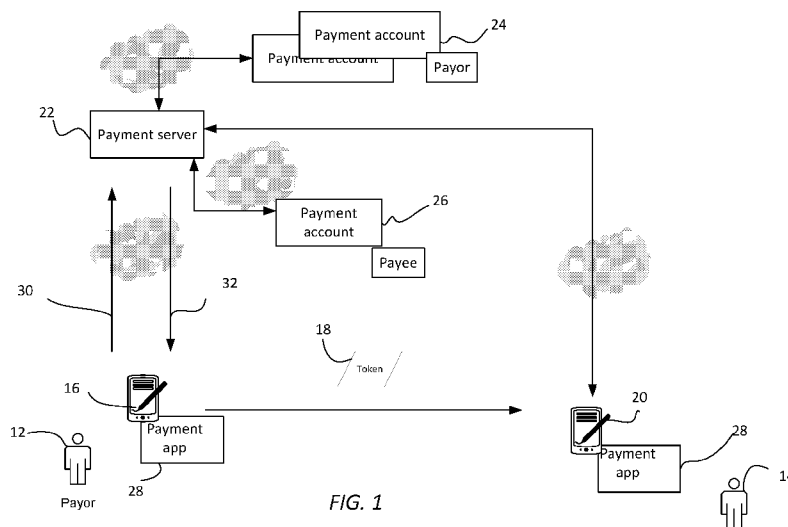


FIG. 1

(57) Abstract: A method for contactless payment is disclosed. The method comprises, at a point of sale, initiating payment by transmitting a token from a first device to a second device using a speaker associated with a first device, and a microphone associated with the second device; transmitting the token from the second device to a payment server; authenticating the token by the payment server; and upon successful authentication of the token, determining with a payment server whether the authorize of the payment.

WO 2017/139703 A1

1

2

### 3 System and Method for Contactless Payments

#### 4 FIELD

5 Embodiments of the present invention relate to methods and systems for  
6 effecting payment for goods and services.

#### 7 BACKGROUND OF THE INVENTION

8 There is a growing trend towards a cashless society where payments for  
9 goods and services takes place without the exchange of cash. Instead,  
10 payment occurs by initiating a transfer from one bank account to another via  
11 electronic means. For the most part cashless payments are effected by means  
12 of credit or debit cards that bear a magnetic stripe encoded with information  
13 that can be read by a card reader at the point-of-sale in order to complete a  
14 payment transaction. Increasingly, there is a trend towards contactless  
15 payment systems as exemplified by Apple Pay where a Near-Field  
16 Communication (NFC) device communicates with a mobile phone to facilitate  
17 payment. However, in the latter system specialized equipment is required in  
18 the form of NFC readers for the system to operate.

19

#### 20 SUMMARY

21 Embodiments of the present invention disclose a method and system for  
22 effecting contactless payments, without the need to install specialized  
23 equipment at a point-of-sale.

24

25 Advantageously, a payor using a mobile phone may transmit an encoded  
26 message wirelessly to a receiving device of a payee. Advantageously, the  
27 encoded message is transmitted using a speaker of the mobile phone, and  
28 received using a microphone of the receiving payee device.

29

30 The code may be masked by other audio included in the transmission, for  
31 example music that may be appealing to a human. Thus, a human may  
32 interpret the transmission as a catchy jingle when in reality the transmission  
33 includes a one-time payment token that may be used by the receiving device  
34 in order to complete a payment transaction.

35

36 Significantly, the transmission may occur in a noisy environment, such as at  
37 a busy checkout counter, without any data loss or errors.

38

39 Moreover, apart from the devices used to transmit and receive the code, which  
40 may be in the form of a mobile phone, no specialized equipment is required  
41 to complete a payment transaction.

42

43 BRIEF DESCRIPTION OF THE FIGURES

44 **FIG. 1** shows a network environment for practicing embodiments of the  
45 present invention.

46

47 **FIG. 2** illustrates the operations performed as part of the registration process,  
48 in accordance with one embodiment of the invention.

49

50 **FIG. 3** shows a token sandwiched between two parts of a melody, in  
51 accordance with one embodiment of the invention.

52

53 **FIG. 4** illustrates a process for encoding a token in a sound file, in accordance  
54 with one embodiment of the invention.

55

56 **FIG. 5** illustrates the operations to generate a payment request, in  
57 accordance with one embodiment of the invention.

58

59 **FIG. 6** illustrates the operations to process a payment request, in accordance  
60 with one embodiment of the invention.

61

62 **FIG. 7** illustrates hardware for implementing a payment server, in accordance  
63 with one embodiment of the invention.

64

65 DETAILED DESCRIPTION OF THE INVENTION

66 In the following description, for purposes of explanation, numerous specific  
67 details are set forth in order to provide a thorough understanding of the  
68 invention. It will be apparent, however, to one skilled in the art that the  
69 invention can be practiced without these specific details. In other instances,  
70 structures and devices are shown in block or flow diagram form only in order  
71 to avoid obscuring the invention.

72

73 Reference in this specification to "one embodiment" or "an embodiment"  
74 means that a particular feature, structure, or characteristic described in  
75 connection with the embodiment is included in at least one embodiment of  
76 the invention. The appearance of the phrase "in one embodiment" in various  
77 places in the specification are not necessarily all referring to the same  
78 embodiment, nor are separate or alternative embodiments mutually exclusive  
79 of other embodiments. Moreover, various features are described which may  
80 be exhibited by some embodiments and not by others.

81

82 Similarly, various requirements are described which may be requirements for  
83 some embodiments but not other embodiments.

84

85 Moreover, although the following description contains many specifics for the  
86 purposes of illustration, anyone skilled in the art will appreciate that many

87 variations and/or alterations to the details are within the scope of the present  
88 invention. Similarly, although many of the features of the present invention  
89 are described in terms of each other, or in conjunction with each other, one  
90 skilled in the art will appreciate that many of these features can be provided  
91 independently of other features. Accordingly, this description of the invention  
92 is set forth without any loss of generality to, and without imposing limitations  
93 upon, the invention.

94

95 Broadly, embodiments of the present invention disclose techniques for  
96 contactless payments. Referring to **FIG. 1** of the drawings, a payor **12** wishes  
97 to make payment to a payee **14**. In this scenario, the payor **12** uses a mobile  
98 device **16** such as a smartphone to initiate the payment to the payee **14**. As  
99 will be explained, the payment is effected by transmission of the payment  
100 token **18** to a receiving device **20** of the payee **14**. Devices **16**, **20** may  
101 comprise smart phones, tablet PCs, and the like.

102

103 In one embodiment, both payor **12** and payee **14** are registered with a  
104 payment server **22**. The payment server **22** may be deployed as a cloud-  
105 based server and is configured to facilitate payments between a payor and  
106 payee, as will be described.

107

108 In one embodiment, in order to enable payments, payor **12**, and the payee  
109 **14** are required to be registered with the payment server **22**. Thus, the  
110 payment server **22** may be configured to engage in a registration process  
111 with each of payor **12**, and payee **14**. At the end of the registration process,  
112 each of payor **12**, and payee **14** will have user accounts registered with the  
113 payment server **22**, and login credentials whereby said user accounts may  
114 be accessed.

115

116 **FIG. 2** illustrates the operations performed as part of the registration  
117 process, in accordance with one embodiment of the invention. Referring to  
118 **FIG. 2**, at block **200**, the user (payor or payee) uses an interface provided  
119 by the payment server **22** create a user ID and login credentials. This step  
120 may be facilitated using a web browser communicatively coupled to the  
121 payment server **22**. At block **202**, the user configures bank accounts to be  
122 used in conjunction with the payment service. In this step, for example, the  
123 user may provide information associated with one or more bank accounts to  
124 facilitate, for example, ACH transfers into and out of said bank accounts. In  
125 one embodiment, for security purposes, small token amounts may be  
126 deposited into each bank account identified by a user, and the user may be  
127 required to validate the bank account by specifying the amount of the deposit  
128 to the payment server **22**. If the amount deposited, and the amount of the  
129 deposit entered by the user do not match, then the particular bank account



130 will not be registered/configured. On the other hand, if the amount deposited,  
131 and the amount of the deposit entered by the user do match, then the bank  
132 account will be registered/configured.

133

134 At block **204**, the user downloads and provisions a client payment app **28**.  
135 For example, the payor **12** may download the client payment app **28** to the  
136 mobile device **16**, whereas the payee **14** may download the client payment  
137 app **28** to the device **20**. As will be explained, the client payment app **28**  
138 provides functionality to facilitate payments between a payor and a payee. In  
139 some embodiments, if the payee **14** is a merchant than the version of the  
140 client payment app **28** installed in the device **20** may include additional  
141 and/or different functionality from the client payment of **28** installed on the  
142 device of the consumer payor **12**.

143

144 A block **206**, the user performs a login to the payment server **22** using the  
145 client payment app **28**. As part of the login process, the device IDs associated  
146 with the devices **16**, **20** are transmitted to the payment server **22**. In  
147 response, the payment server **22** is configured to bind the particular device  
148 IDs to the user ID of the user as part of the step **208**, wherein the device ID  
149 is registered to the user.

150

151 Referring to **FIG. 1** of the drawings, it will be seen that the payor **12** has two  
152 payment accounts **24** registered with the payment server **22**, whereas the  
153 payee has one payment account **26** registered with the payment server **22**.

154

155 To begin the payment process, in one embodiment the payor **12** initiates a  
156 payment token request **30** to the payment server **20**. The payment token  
157 request **30** is generated by the payment app **28**.

158

159 In one embodiment, the payment server **22** is configured to receive the  
160 payment token request and to generate a one-time payment token in  
161 response thereto. The payment token may be a unique number from a  
162 number space that is large enough to prevent fraudsters from replicating the  
163 payment token. In one embodiment, the number space a large enough to  
164 accommodate a number that includes **18** trailing zeros. Additionally, the  
165 numbers from the number space may be randomly selected as one-time  
166 tokens. In other words, the one-time tokens are not serially generated, which  
167 reduces the possibility of a fraudster predicting a token.

168

169 The one-time payment token generated by the payment server **22** is  
170 transmitted to the client device **16**, as indicated by the arrow **32**. In one  
171 embodiment, upon receiving the one-time token from the payment server  
172 **22**, the payment app **28** of the payor **12** transmits the token (indicated by

173 reference **18**) to the payee **14**. More accurately, the one-time payment token  
174 **18** is transmitted to the mobile device **20** of the payee **14** that is provisioned  
175 with the payment app **28**. In one embodiment, transmission of the payment  
176 token may be based on a novel encoding scheme for transmitting digital data  
177 over a short-range audio link. Advantageously, for the transmission  
178 commodity microphone and speaker hardware associated with a handheld  
179 mobile device may be used. Moreover, even under noisy conditions the digital  
180 data may transmitted and decoded.

181

182 The above scenario for obtaining a token to defendant on connectivity being  
183 available to the payment server **22**. Therefore, this scenario is referred to as  
184 an online scenario. However, in an off-line scenario in which there is no  
185 connectivity to the payments of a **22**, the transmitting payment app **28** may  
186 generate a token by itself independently of the payment server **22**, for  
187 transmission to the receiving payment app **28**, in the manner described. The  
188 token generated by the payment app **28** may include a user ID, the payment  
189 amount, the transaction location, a time stamp for the transaction, and one  
190 or more additional tokens. The information of the token advantageously,  
191 uniquely identifies the user making the payment, the device through which  
192 the payment is made, and the payment transaction thereby minimizing the  
193 possibility of fraud. To further minimize the possible to fraud, the payment  
194 app 28 may be configured to require the payor to unlock the payment

195 functionality of the app by inputting a personal identification number. This is  
196 in addition to the user having unlocked his/her device for use in general.

197

198 In some embodiments, the token generated by the payment app **28** may also  
199 include typical information required in order to enable a credit card type  
200 transaction. This information may include a credit card number, and  
201 expiration date, and a verification code. Alternatively, the token generated  
202 by the payment app **28** may include sufficient admission to identify a bank  
203 account associated with the payor to allow the payment server **22** to process  
204 a payment authorization request associated with said bank account.

205

206 In one embodiment, the encoding scheme may be designed to spread signal  
207 energy over a wide frequency range to provide immunity against frequency-  
208 dependent channel fades. Simultaneously, the scheme may allow for  
209 complexity detection of incoming transmissions, as well as precise  
210 synchronization to the digital data stream encoded in the transmission.

211

212 In another embodiment, the encoding scheme may be designed to make  
213 maximum use of the limited dynamic range of the transmit speaker hardware  
214 by using square wave rather than sinusoidal signals.

215

216 To implement the encoding scheme, the usual elements of any  
217 communication system may be used such as a source encoder or compression  
218 engine, an error correction code, a checksum sequence, a digital to analog  
219 converter, transducer hardware to create sound waves from a voltage  
220 waveform on the transmitter side, and a sensor e.g. a microphone to detect  
221 air pressure variations from sound waves, an analog to digital converter, logic  
222 to detect and decode incoming data transmissions and to check the integrity  
223 of the transmission using the checksum.

224

225 The transmitted waveform may comprise a concatenation of two or more of  
226 the following distinct signals: a "start melody", "detection beacon",  
227 "preamble", "silence gaps", "data" and "end melody".

228

229 Each of these signals are intended to serve one distinct purpose: e.g. the  
230 start and end "melodies" are designed to bookend the rest of the transmission  
231 to make the overall audio pleasing or at least comfortable to the human ear.  
232 It may also have the effect of masking the transmission to potential  
233 eavesdropping devices.

234

235 In one embodiment, two or more separate signals may be generated to aid  
236 detection and synchronization. In conventional communications systems, a  
237 preamble sequence which has sharply peaked autocorrelation properties is

238 used to accurately identify the start of incoming transmissions. However,  
239 detecting such a sequence requires the use of a linear filter matched to the  
240 preamble sequence which usually takes the form of an FIR filter with a long  
241 impulse response. This can be an expensive operation in terms of power, CPU  
242 and memory especially for receivers that need to continuously monitor for  
243 incoming transmissions. A device using the inventive encoding scheme may  
244 employ an additional signal that is easy to detect, but does not have a sharp  
245 correlation function to first detect a transmission and only then invoke the  
246 expensive filter that searches for the preamble.

247

248 The waveform used to modulate data may have a constant envelope or at  
249 least a small peak to average ratio (e.g. the peak to average power ratio may  
250 be 0.5). One example of such a signal is a "square chirp (SC)"; just like the  
251 common chirp signal, the SC is a quasi-periodic signal with a frequency that  
252 increases at a constant rate in time over a specified band. However, unlike  
253 the common (sinusoidal) chirp, the SC consists of square waves, which  
254 surprisingly makes better use of the peak transmit power capability of the  
255 speaker hardware. The use of square wave signals in SC does lead to higher  
256 frequency harmonics, but under peak power rather than battery constraints,  
257 thus the waste of power represented by these harmonics is irrelevant. In one  
258 embodiment, interference with other devices is not an important

259 consideration because of the short range and short duration of the  
260 transmission.

261

262 In one embodiment, a one-time token **18** may be encoded for transmission  
263 by a carrier wave using a frequency modulation scheme such as Frequency-  
264 Shift Keying (FSK). Thus, the token **18** may be transmitted using discreet  
265 frequency changes of a carrier wave that is broadcast from the device **16** to  
266 the device **20**. Unfortunately, said discreet frequency changes when heard  
267 by the human ear can be very unpleasant. Accordingly, in one embodiment,  
268 the code representing the token is sandwiched between two portions of the  
269 melody/tune, which are also encoded through frequency modulation for  
270 transmission by the carrier wave. This is shown in **FIG. 3** of the drawings,  
271 where token **18** is sandwiched between a first part **300** of a melody and a  
272 second part **302** of said melody.

273

274 Referring now to **FIG. 4** of the drawings, in one embodiment, in order to  
275 generate a signal with a one-time token **18** sandwiched between two parts  
276 of the melody, the token **18** is input into an encoder **400**. The encoder **400**  
277 is configured to implement encoding techniques, such as the FSK encoding  
278 technique described above. The encoder **400** encodes the one-time token **18**  
279 together with a melody or tune to produce a sound file **402** which includes  
280 two melody portions and a code representing the one-time token **18**

281 sandwiched there between in similar fashion to what has been described  
282 above with reference to **FIG. 3**. The encoding and the generation of the sound  
283 file **402** is performed by the device **16**.

284

285 In one embodiment, for transmission of the one-time token **18**, the device  
286 **16** plays the sound file **402** at block **404**. The sound file **402** is received by  
287 the device **20** at block **406** through a microphone associated with the device  
288 **20**. Within the device **20**, once the one-time token **18** of the sound file **402**  
289 has been received, decoding thereof begins. This process happens  
290 concurrently as the melody portions **300**, **302** are played. In one  
291 embodiment, the melody portions **300**, **302** may be of a sufficient length to  
292 enable the device **20** to completely decode the one-time token **18** so that  
293 when the melody portions **300**, **302** end, the one-time token **18** is  
294 completely decoded. Thus, a perception of a fast decode is achieved.  
295 Moreover, playing of the melody portions masks the unpleasant sound  
296 associated with the transmission of the one-time code **18**.

297

298 In one embodiment, the payment of **28** may allow the payor **12** to specify  
299 the payment account. In this case, the transmission to the device **20** may  
300 include the amount of the payment in addition to the one-time payment token  
301 **18**. In some cases, the payment app **28** may be configured to transmit the



302 payment amount to the payment server **22** is part of the payment  
303 authorization request **30**.

304

305 As noted above, the device **20** receives and decodes the transmission from  
306 the device **16** in order to recover the one-time payment token **18**. Referring  
307 now to **FIG. 5** of the drawings, operations performed by the device **20** in  
308 conjunction with the client payment app **28**, in accordance with one  
309 embodiment of the invention, is shown. As will be seen, at block **500** a  
310 payment request is generated. The payment request includes the one-time  
311 payment token **18**. Optionally, the payment request may also include a  
312 payment amount associated with the transaction. For example, if the payee  
313 **14** is a merchant or retailer then according to one use case, the payor **12**  
314 does not insert the payment amount, rather the merchant does this as part  
315 of a checkout process. In this case the payment request will then include the  
316 payment amount inserted by the merchant. At block **502**, the device **20**  
317 transmits the payment request to the payment server **22**.

318

319 Turning now to **FIG. 6** of the drawings, the operations performed by the  
320 payment server **22**, in accordance with one embodiment, to effect payment  
321 between the payor **12** in the payee **14**, is shown. Referring to **FIG. 6**, at  
322 block **600** the payment server **22** receives the payment request from the  
323 device **20**. At block **602**, the payment server **22** authenticates the payee **14**.

324 In one embodiment, authentication succeeds if the device ID included in the  
325 transmission from the device **20** matches the device ID of a registered device  
326 of the payee **14**. If the payee **14** is authenticated, then at block **604** the one-  
327 time token included in the payment request is validated. In one embodiment,  
328 the one-time token passes validation only if it matches an open one-time  
329 token generated by the payment server **22**. In one embodiment, an open  
330 one-time token may include any token generated by the payment server **22**  
331 in response to the pavement authorization request within a certain time, for  
332 example say was in the last five minutes, and which is not yet been  
333 transmitted back to the payment server **22** is part of a payment request.

334

335 At block **606**, if the one-time token **18** is validated, then the payment server  
336 generates and sends a payment authorize message to the payee **12**. In one  
337 embodiment, this message may include information specifying that the payor  
338 **14** is requesting the transaction amount to be paid. In one embodiment, the  
339 payee **12** transmits a payment authorize confirmation message back to the  
340 payment server **22**. Once this message is received, the block **608** executes  
341 in order to transfer the payment amount to the payee **14**. Transferring the  
342 payment amount may be achieved in various ways, in accordance with  
343 different embodiments. In one embodiment, the payment server **22** initiates  
344 a funds request from a payment account associated with the payor **12**. In the  
345 case of the payor **12** having multiple payment accounts, and the payor **12**

346 may be requested to specify the particular payment account as a source of  
347 payment funds. The funds request may be initiated via an ACH request. The  
348 payment server **22** in effect acts as a broker to transfer the payment amount  
349 from the payor's payment account to the payee's payment account. In this  
350 case, the payment server **22** implements functionality similar to PayPal, and  
351 other such payment providers. In some cases, the payment accounts of both  
352 the payor and the payee may actually be virtual payment accounts.

353

354 **FIG. 7** shows an example of hardware **700** that may be used to implement  
355 the payment server **22** in accordance with one embodiment. The hardware  
356 **700** may include at least one processor **702** coupled to a memory **704**. The  
357 processor **702** may represent one or more processors (e.g.,  
358 microprocessors), and the memory **704** may represent random access  
359 memory (RAM) devices comprising a main storage of the hardware, as well  
360 as any supplemental levels of memory e.g., cache memories, non-volatile or  
361 back-up memories (e.g. programmable or flash memories), read-only  
362 memories, etc. In addition, the memory **704** may be considered to include  
363 memory storage physically located elsewhere in the hardware, e.g. any cache  
364 memory in the processor **702**, as well as any storage capacity used as a  
365 virtual memory, e.g., as stored on a mass storage device.

366 [001] The hardware also typically receives a number of inputs and outputs  
367 for communicating information externally. For interface with a user or

368 operator, the hardware may include one or more user input output devices  
369 **706** (e.g., a keyboard, mouse, etc.) and a display **708**. For additional  
370 storage, the hardware **700** may also include one or more mass storage  
371 devices **710**, e.g., a Universal Serial Bus (USB) or other removable disk drive,  
372 a hard disk drive, a Direct Access Storage Device (DASD), an optical drive  
373 (e.g. a Compact Disk (CD) drive, a Digital Versatile Disk (DVD) drive, etc.)  
374 and/or a USB drive, among others. Furthermore, the hardware may include  
375 an interface with one or more networks **712** (e.g., a local area network (LAN),  
376 a wide area network (WAN), a wireless network, and/or the Internet among  
377 others) to permit the communication of information with other computers  
378 coupled to the networks. It should be appreciated that the hardware typically  
379 includes suitable analog and/or digital interfaces between the processor **712**  
380 and each of the components, as is well known in the art.

381 **[002]** The hardware **700** operates under the control of an operating  
382 system **714**, and executes application software **716** which includes various  
383 computer software applications, components, programs, objects, modules,  
384 etc. to perform the techniques described above.

385 **[003]** In general, the routines executed to implement the embodiments of  
386 the invention, may be implemented as part of an operating system or a  
387 specific application, component, program, object, module or sequence of  
388 instructions referred to as "computer programs." The computer programs  
389 typically comprise one or more instructions set at various times in various

390 memory and storage devices in a computer, and that, when read and  
391 executed by one or more processors in a computer, cause the computer to  
392 perform operations necessary to execute elements involving the various  
393 aspects of the invention. Moreover, while the invention has been described  
394 in the context of fully functioning computers and computer systems, those  
395 skilled in the art will appreciate that the various embodiments of the invention  
396 are capable of being distributed as a program product in a variety of forms,  
397 and that the invention applies equally regardless of the particular type of  
398 machine or computer-readable media used to actually effect the distribution.  
399 Examples of computer-readable media include but are not limited to  
400 recordable type media such as volatile and non-volatile memory devices, USB  
401 and other removable media, hard disk drives, optical disks (e.g., Compact  
402 Disk Read-Only Memory (CD ROMS), Digital Versatile Disks, (DVDs), etc.),  
403 flash drives among others.

## CLAIMS:

1. A method for contactless payment, comprising:
  - at a point of sale, initiating payment by transmitting a token from a first device to a second device using a speaker associated with a first device, and a microphone associated with the second device;
  - transmitting the token from the second device to a payment server;
  - authenticating the token by the payment server; and
  - upon successful authentication of the token, determining with a payment server whether the authorize of the payment.
  
2. The method of claim 1, further comprising registering the first device, and the second device as authorized devices for payment processing with the authentication server.
  
3. The method of claim 1, wherein in an online mode the first device engages in a transaction with the payment server in order to obtain the token prior to transmission.
  
4. The method of claim 3, wherein the token comprises a payment amount and identification information to uniquely identify aspects of the payment transaction.

5. The method of claim 4, wherein the identification information comprises information selected from the group consisting of a consumer ID, a payment amount, a transaction location, a time stamp, and a token.
6. The method of claim 1, wherein in an off-line mode, the first device generates a token independently of the payment server.
7. The method of claim 1, wherein the token is encrypted by the first device prior to transmission.
8. The method of claim 1, wherein the token is encoded with a melody prior to transmission.
9. The method of claim 1, wherein the second device plays a melody while decoding the token.
10. The method of claim 1, wherein the second device transmits the token to the payment server in encrypted form.
11. The method of claim 1, wherein a payment application provisioned in the first device authenticates a user prior to transmission of the token.
12. The method of claim 11, wherein authentication of the user is through a personal identification number input by the user.

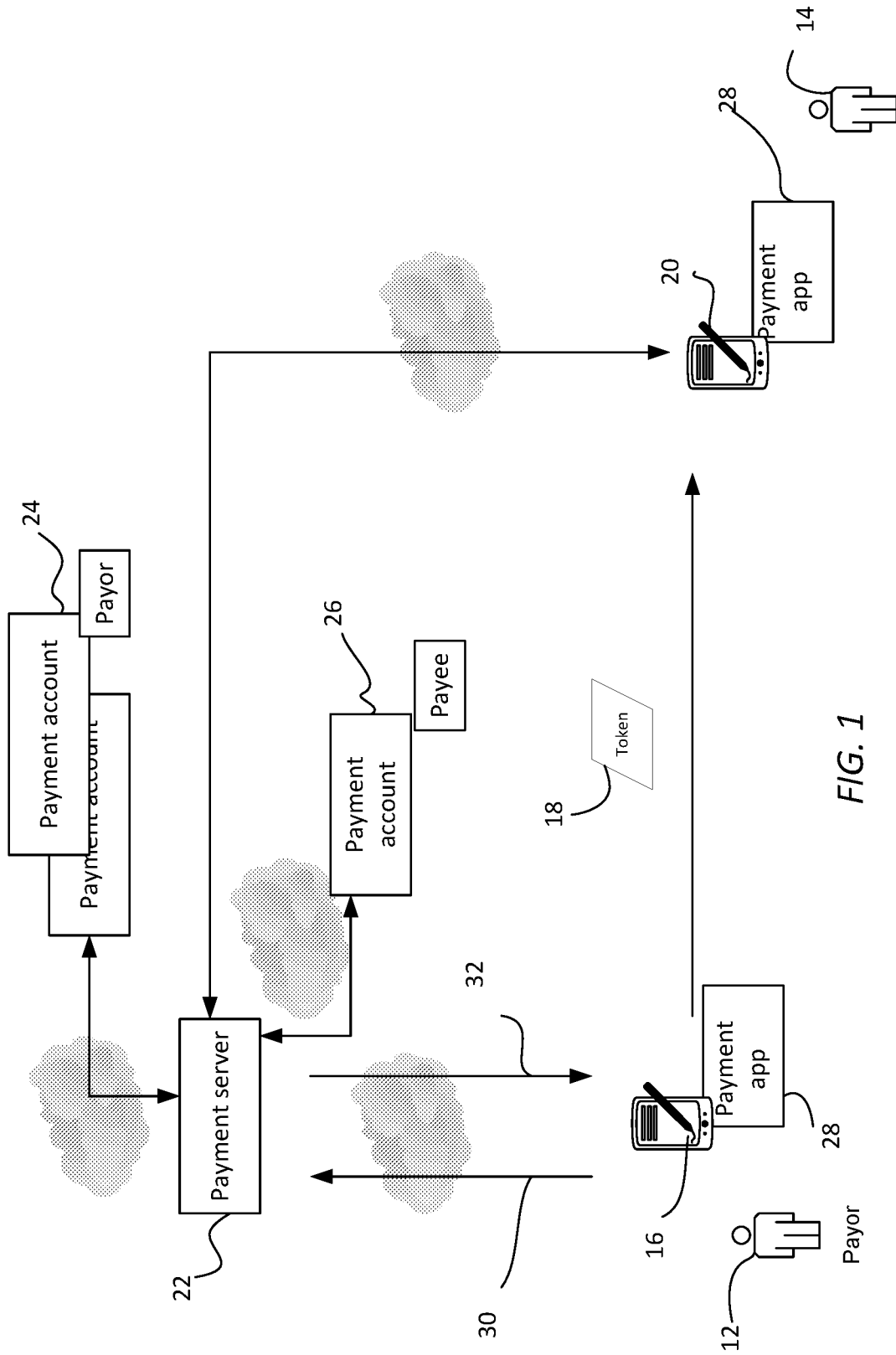


FIG. 1



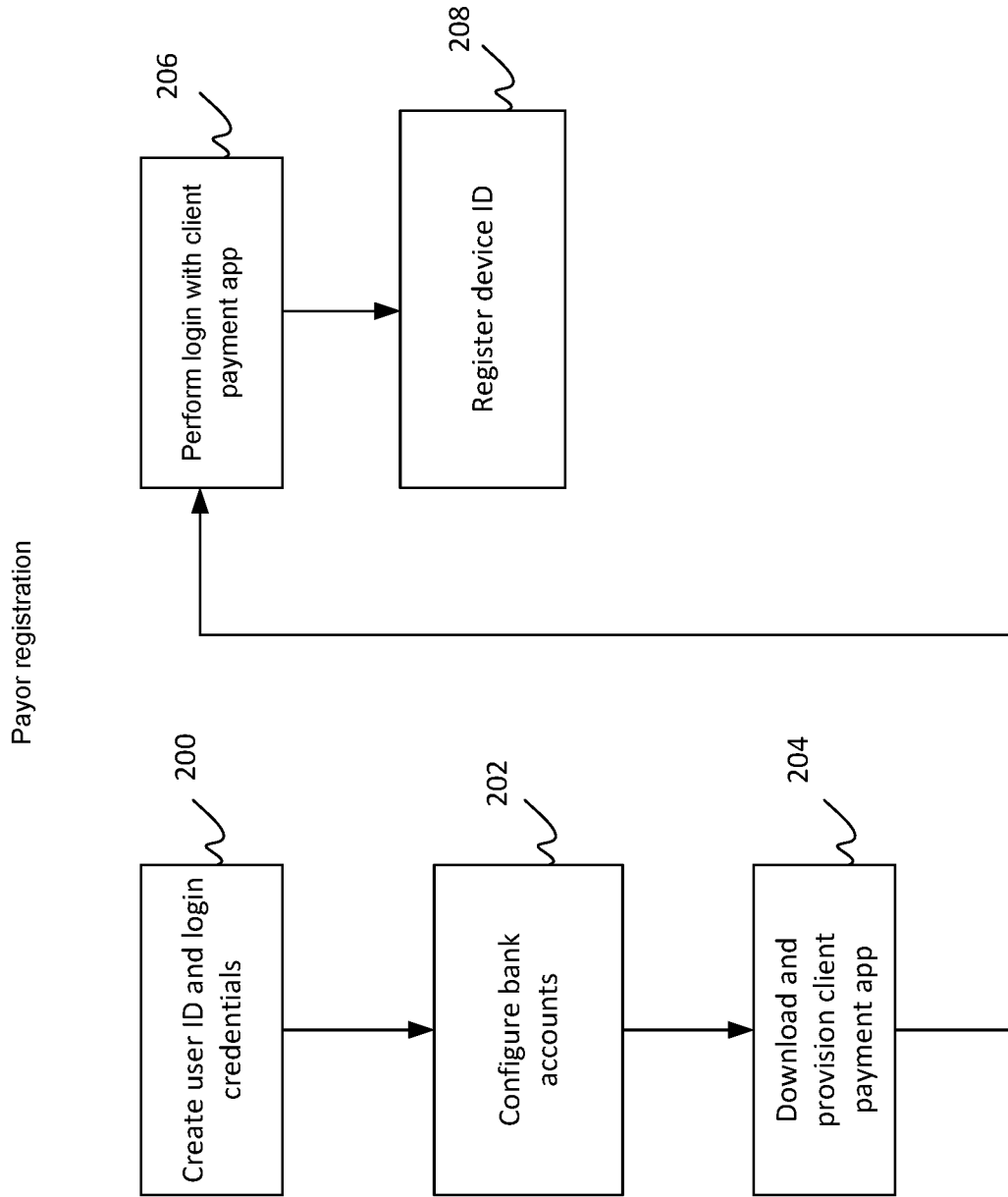


FIG. 2

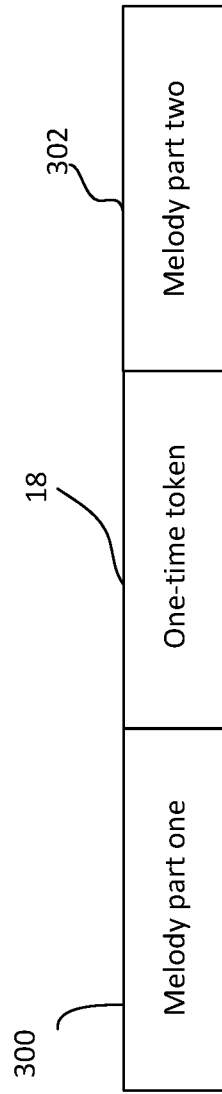


FIG. 3

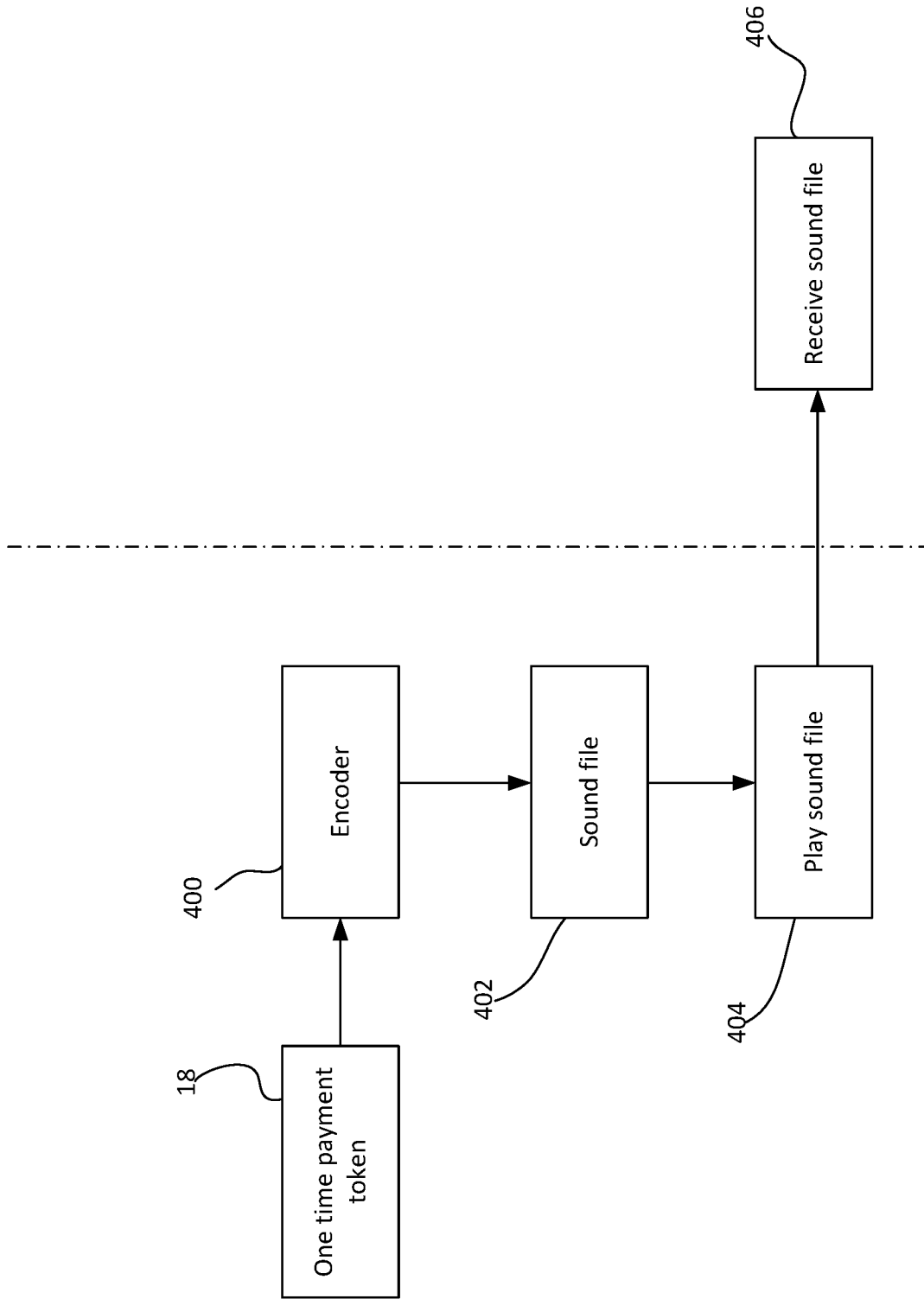


FIG. 4

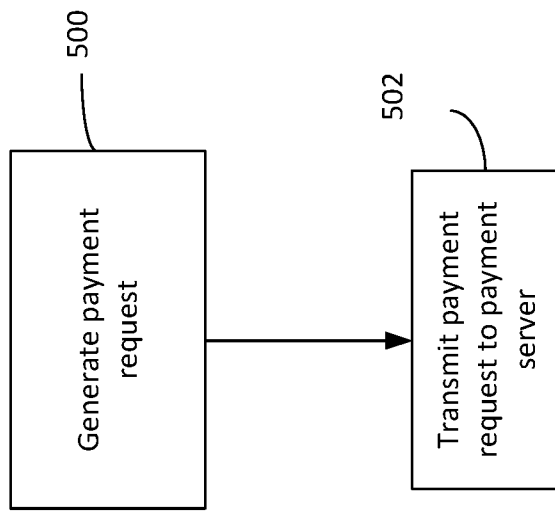


FIG. 5

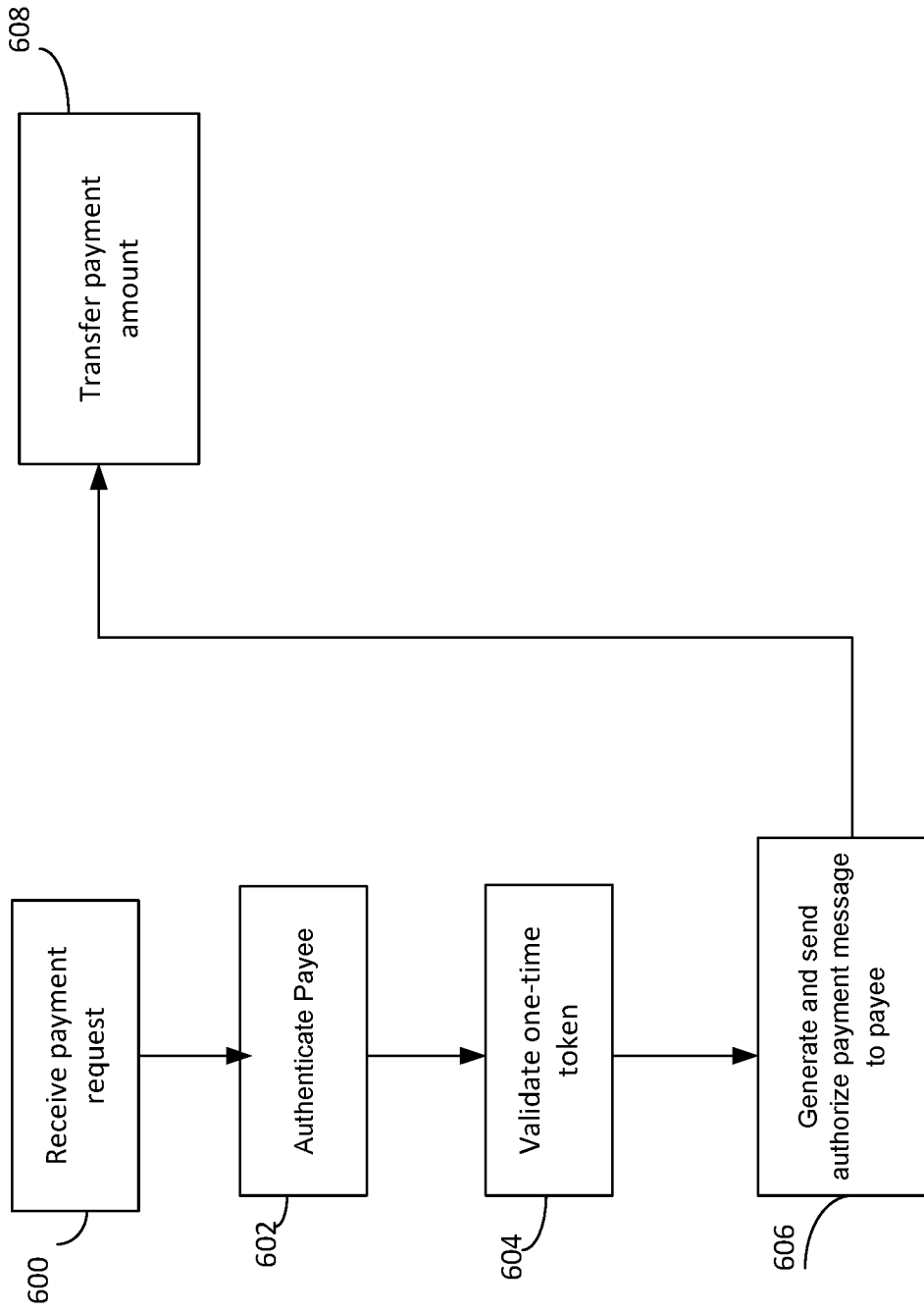


FIG. 6

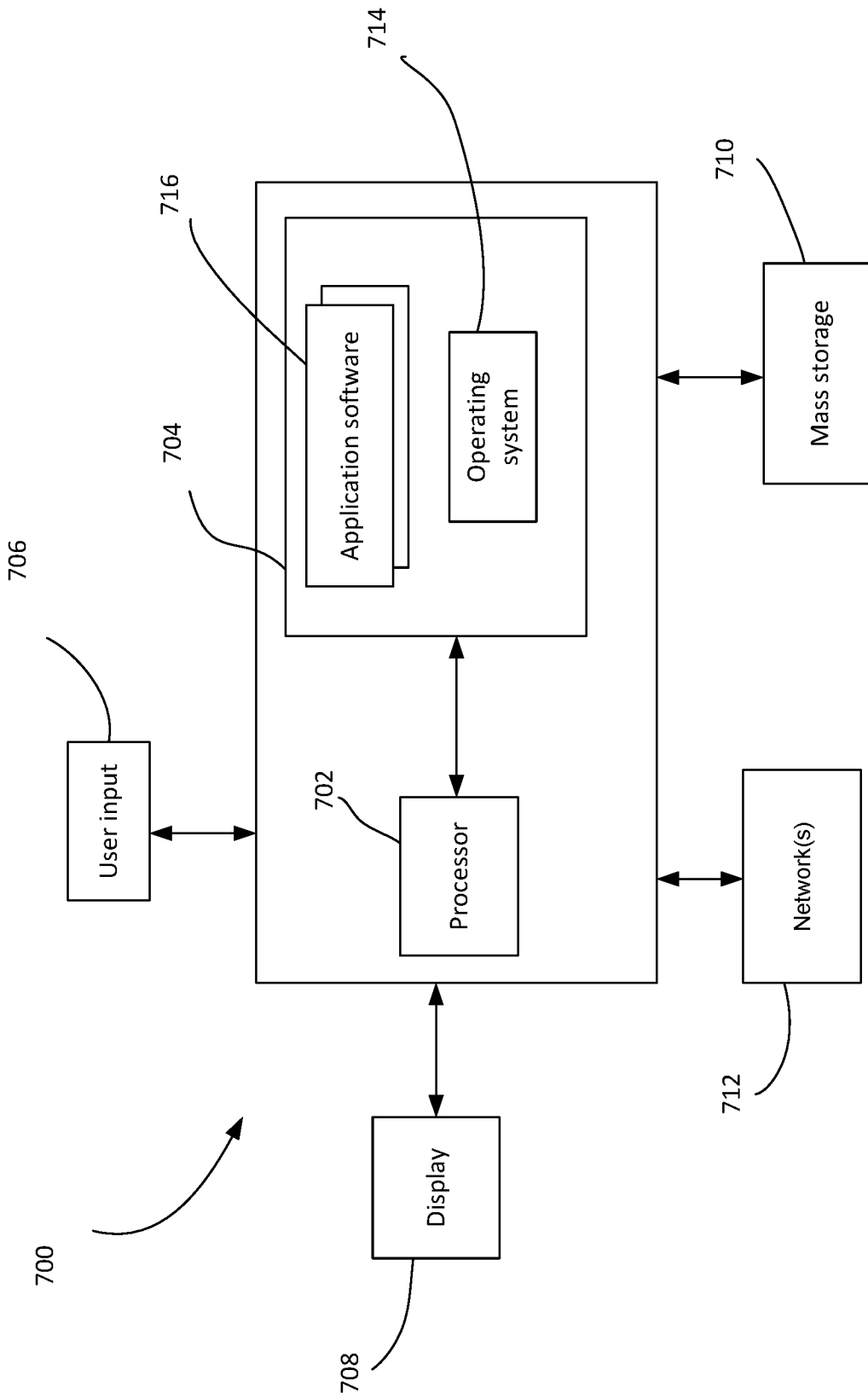


FIG. 7

**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/US2017/017558

A. CLASSIFICATION OF SUBJECT MATTER  
IPC(8) - G06Q 20/32; G06Q 20/00; G06Q 20/40; G06Q 20/20; G06Q 20/38 (2017.01)  
CPC - G06Q 20/3272; G06Q 20/32; G06Q 20/20; G06Q 20/40; G06Q 20/3223 (2017.02)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
USPC - 705/44; 705/39; 705/16; 705/41 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---	US 2011/0258121 A1 (KAUNISKANGAS et al) 20 October 2011 (20.10.2011) entire document	1-8, 10-12 ---
Y		9
Y	WO 2015/176019 A1 (AINTU INC.) 19 November 2015 (19.11.2015) entire document	9
A	US 2014/0101043 A1 (BANK OF AMERICA CORPORATION) 10 April 2014 (10.04.2014) entire document	1-12
A	US 2014/0244514 A1 (DIGIMARC CORPORATION) 28 August 2014 (28.08.2014) entire document	1-12
A	US 9,082,413 B2 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 14 July 2015 (14.07.2015) entire document	1-12
A	WO 2014/059520 A1 (RIAVERA CORP.) 24 April 2014 (24.04.2014) entire document	1-12

Further documents are listed in the continuation of Box C.  See patent family annex.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed  
 "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
12 April 2017

Date of mailing of the international search report  
**05 MAY 2017**

Name and mailing address of the ISA/US  
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents  
P.O. Box 1450, Alexandria, VA 22313-1450  
Facsimile No. 571-273-8300

Authorized officer  
Blaine R. Copenheaver  
PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774