US 20180165441A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2018/0165441 A1**

Everhart (43) **Pub. Date: Jun. 14, 2018**

(54) **SYSTEMS AND METHODS FOR MULTIFACTOR AUTHENTICATION**

(76) Inventor: **Glenn Cobourn Everhart**, Smyrna, DE (US)

(21) Appl. No.: **11/137,409**

(22) Filed: **May 26, 2005**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/419,107, filed on Apr. 21, 2003, now Pat. No. 7,899,753, which is a continuation-in-part of application No. 10/105,471, filed on Mar. 25, 2002, now abandoned.

(60) Provisional application No. 60/646,622, filed on Jan. 26, 2005, provisional application No. 60/661,488, filed on Mar. 15, 2005.

Publication Classification

(51) **Int. Cl.**
G06F 21/36 (2006.01)
G06Q 20/40 (2006.01)

(52) **U.S. Cl.**
CPC ***G06F 21/36*** (2013.01); ***G06Q 20/40*** (2013.01)

(57) **ABSTRACT**

The invention provides an authentication system and method. In particular, the invention provides a method for performing a financial authentication utilizing a token associated with a user, the method comprising the token generating a set of display characters that are viewable by the user, the token generating the display characters using logic; the user transforming a portion of the set of display characters using a transformation process, based on knowledge of the user, so as to form a display character sequence; the user outputting the display character sequence to an authentication entity; and the authentication entity authenticating the display character sequence using the logic and knowledge of the transformation.

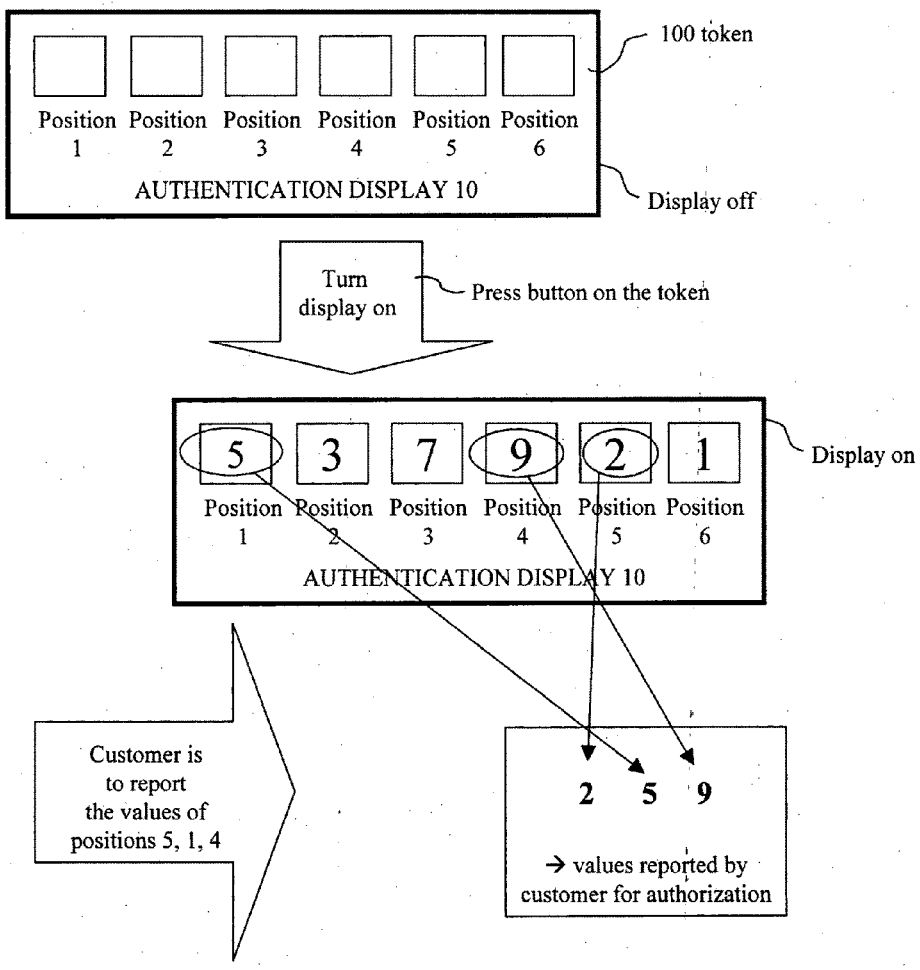


Fig. 1

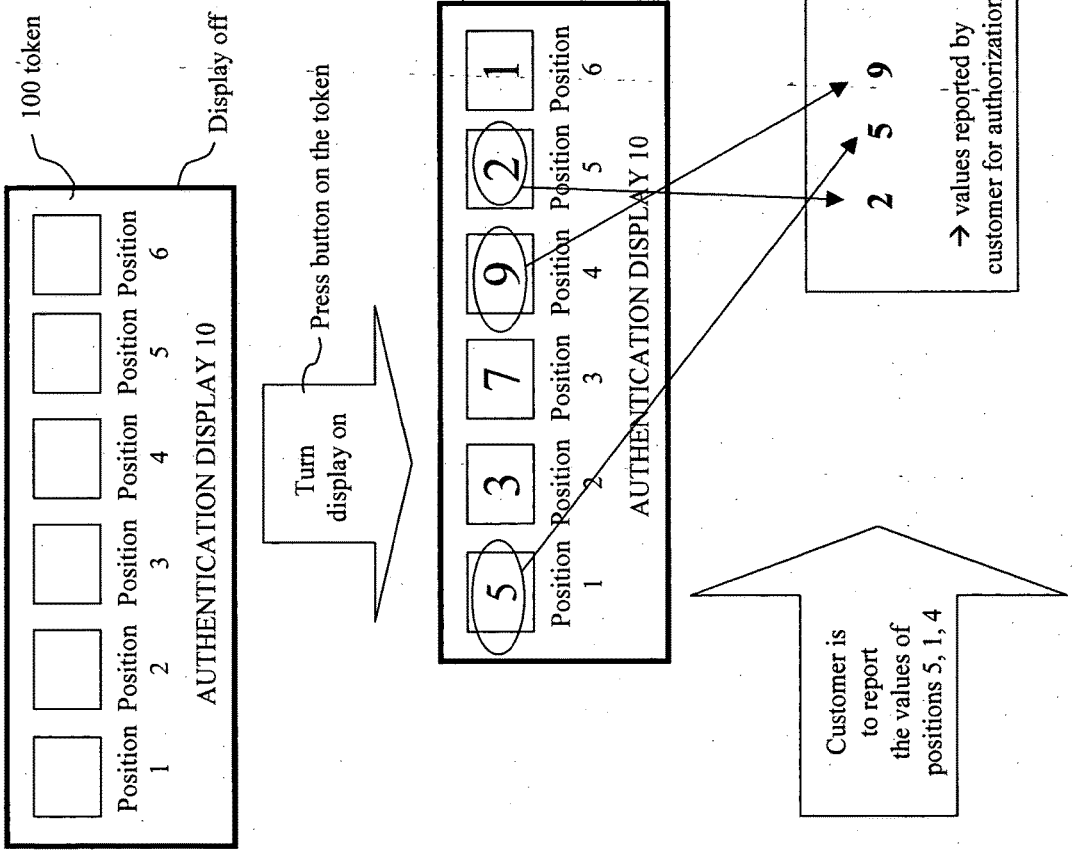

100 token
Display off
Position 1
Position 2
Position 3
Position 4
Position 5
Position 6
AUTHENTICATION DISPLAY 10
Press button on the token
Turn display on
Display on
5
3
7
9
2
1
AUTHENTICATION DISPLAY 10
2 5 9
→ values reported by customer for authorization
Customer is to report the values of positions 5, 1, 4

Fig. 2

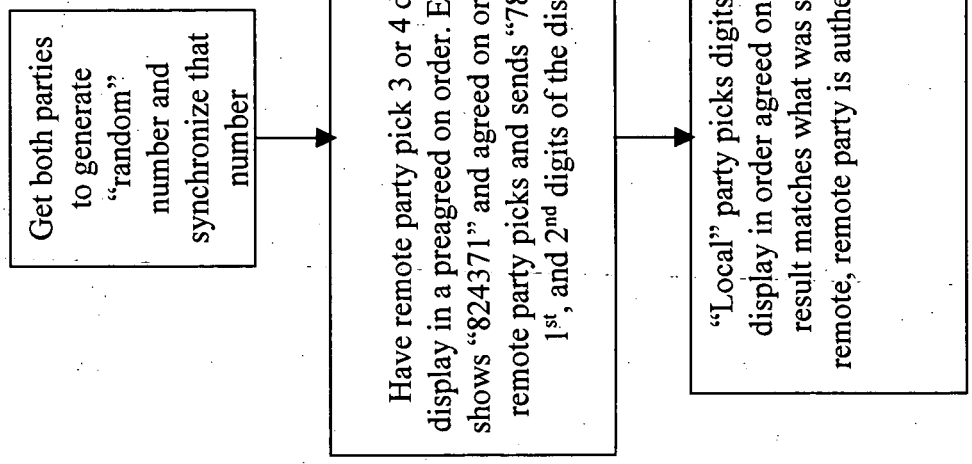

Get both parties to generate "random" number and synchronize that number
Have remote party pick 3 or 4 digits from display in a preagreed on order. E.g. if display shows "824371" and agreed on order is "512", remote party picks and sends "782" (the 5th, 1st, and 2nd digits of the display).
"Local" party picks digits from display in order agreed on. If the result matches what was sent by remote, remote party is authenticated.

Fig. 3

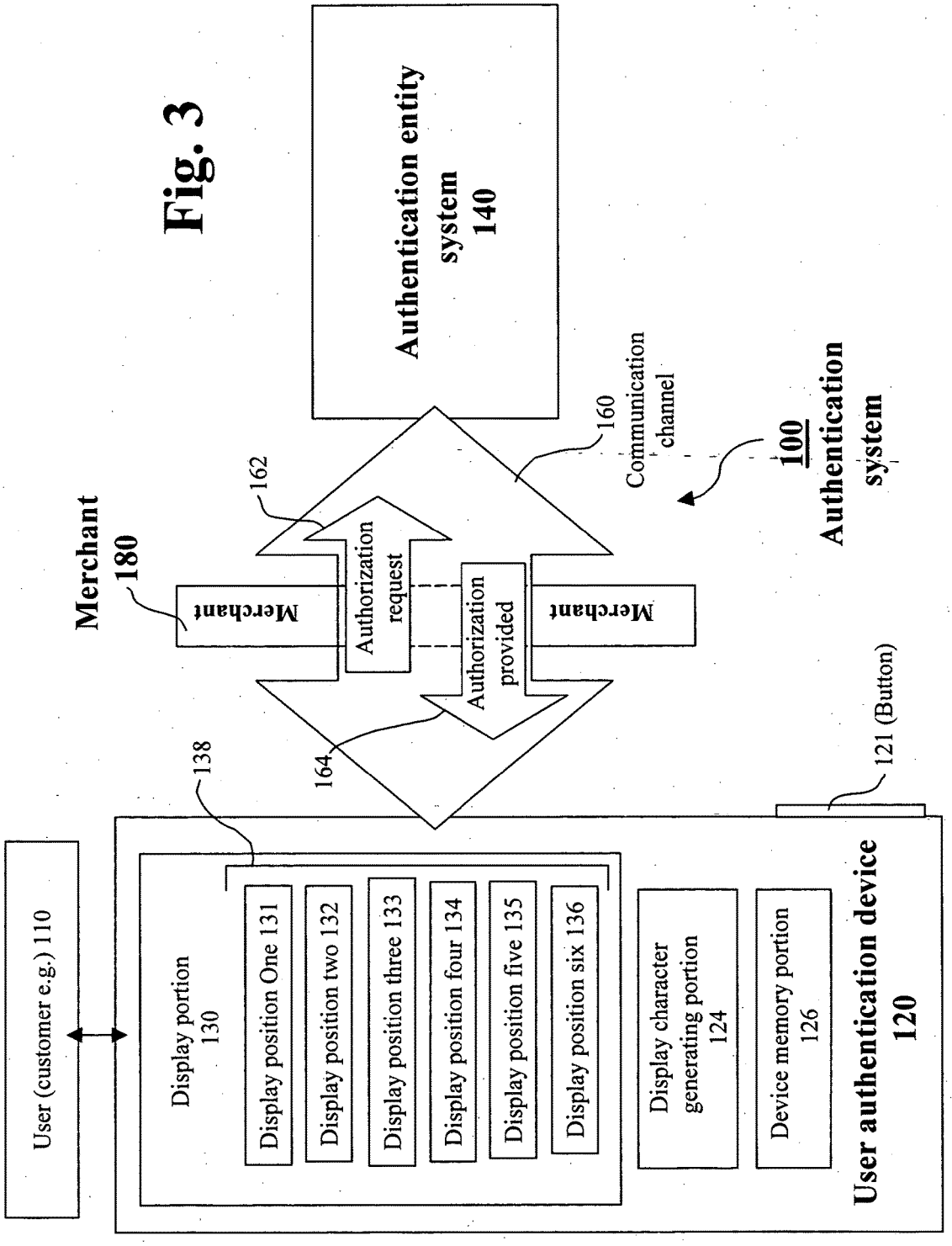
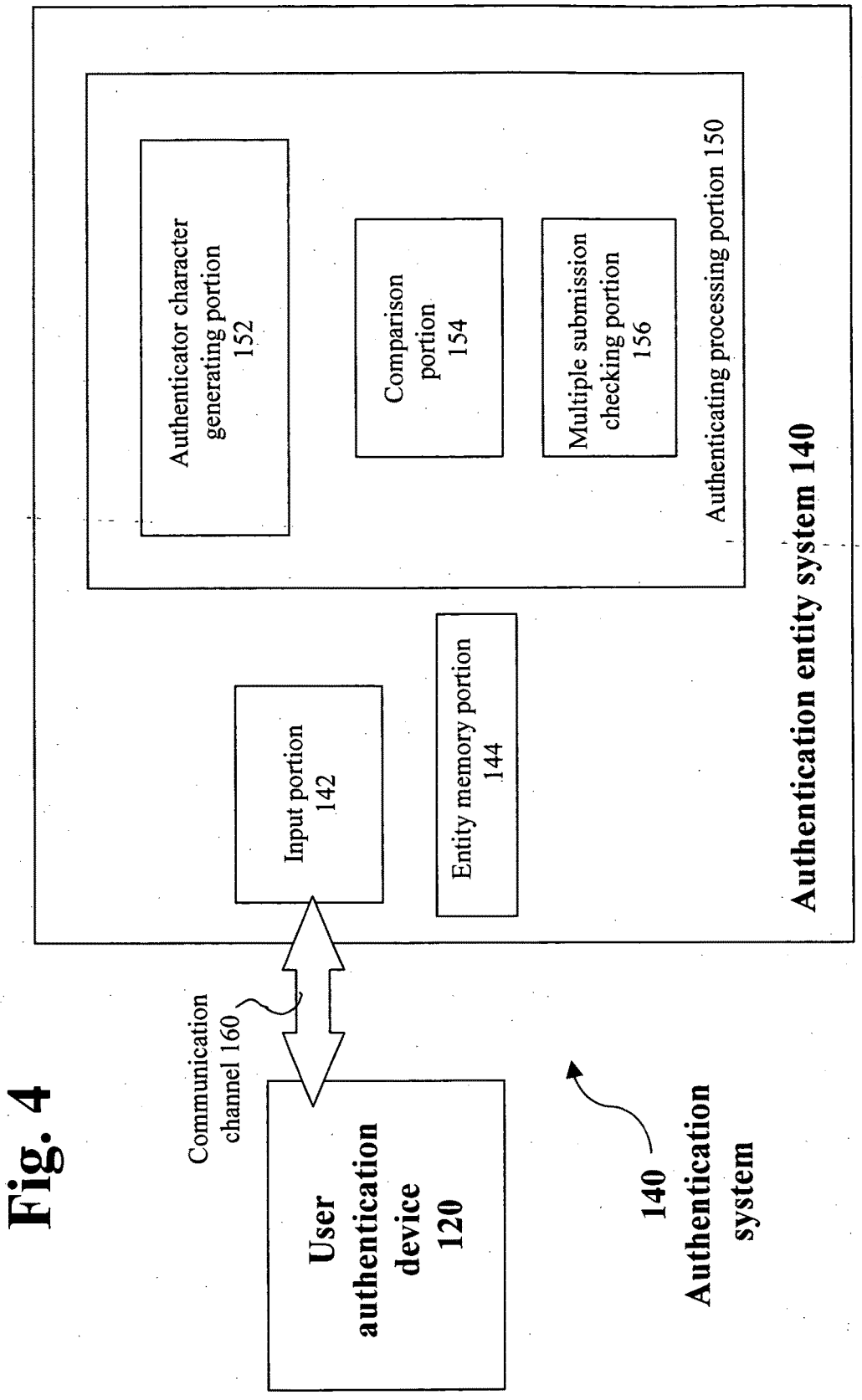

Authentication entity system 140
Merchant 180
Merchant
Merchant
Authorization request
Authorization provided
162
164
160
Communication channel
100 Authentication system
User (customer e.g.) 110
Display portion 130
Display position One 131
Display position two 132
Display position three 133
Display position four 134
Display position five 135
Display position six 136
Display character generating portion 124
Device memory portion 126
User authentication device 120
138
121 (Button)

Fig. 4


User authentication device 120
Communication channel 160
Input portion 142
Entity memory portion 144
Authentication entity system 140
Authenticating processing portion 150
Authenticator character generating portion 152
Comparison portion 154
Multiple submission checking portion 156
140 Authentication system

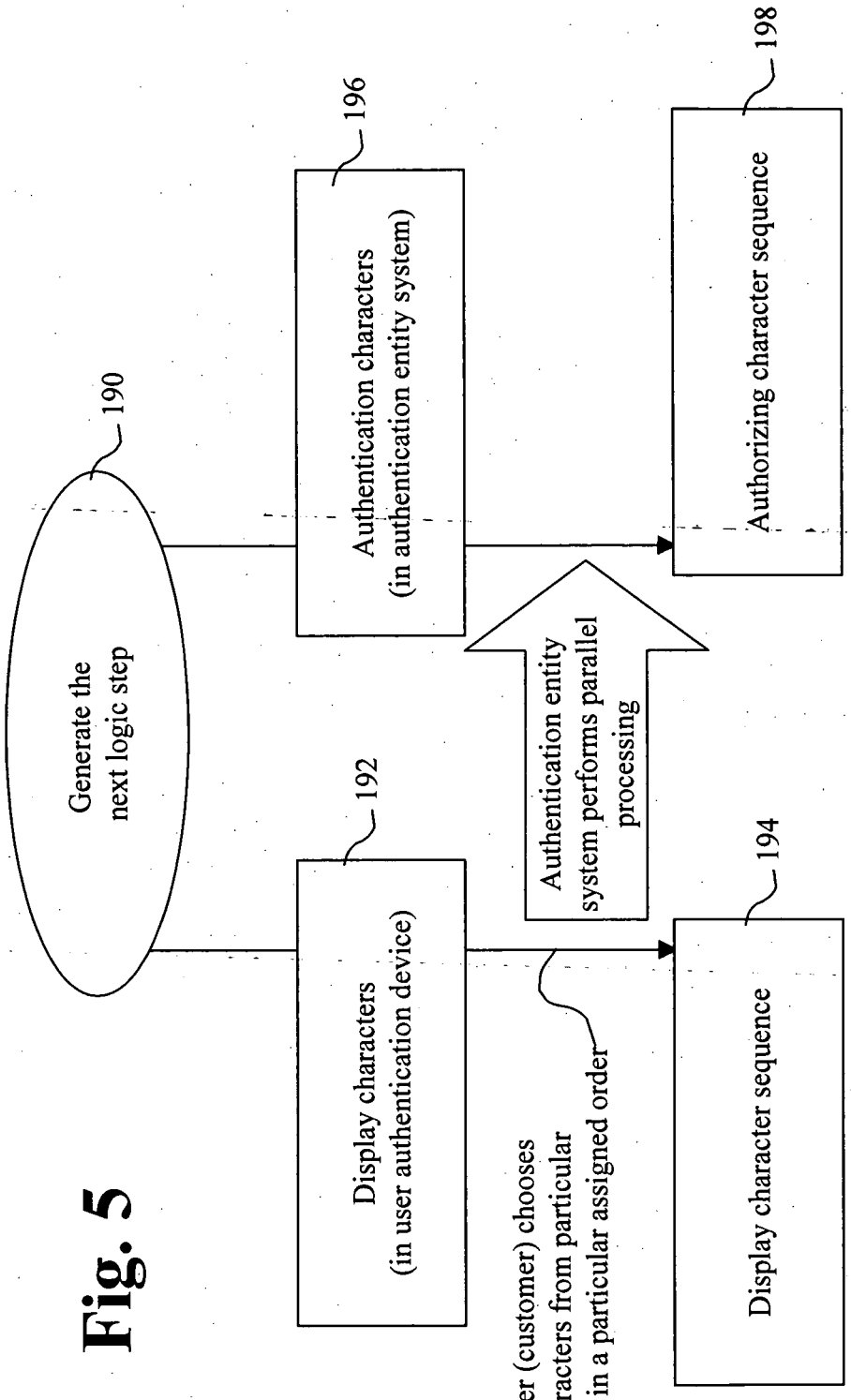

Generate the next logic step
190
Display characters (in user authentication device)
192
Authentication characters (in authentication entity system)
196
Authentication entity system performs parallel processing
User (customer) chooses characters from particular positions, in a particular assigned order
Display character sequence
194
Authorizing character sequence
198

Fig. 5

Fig. 6

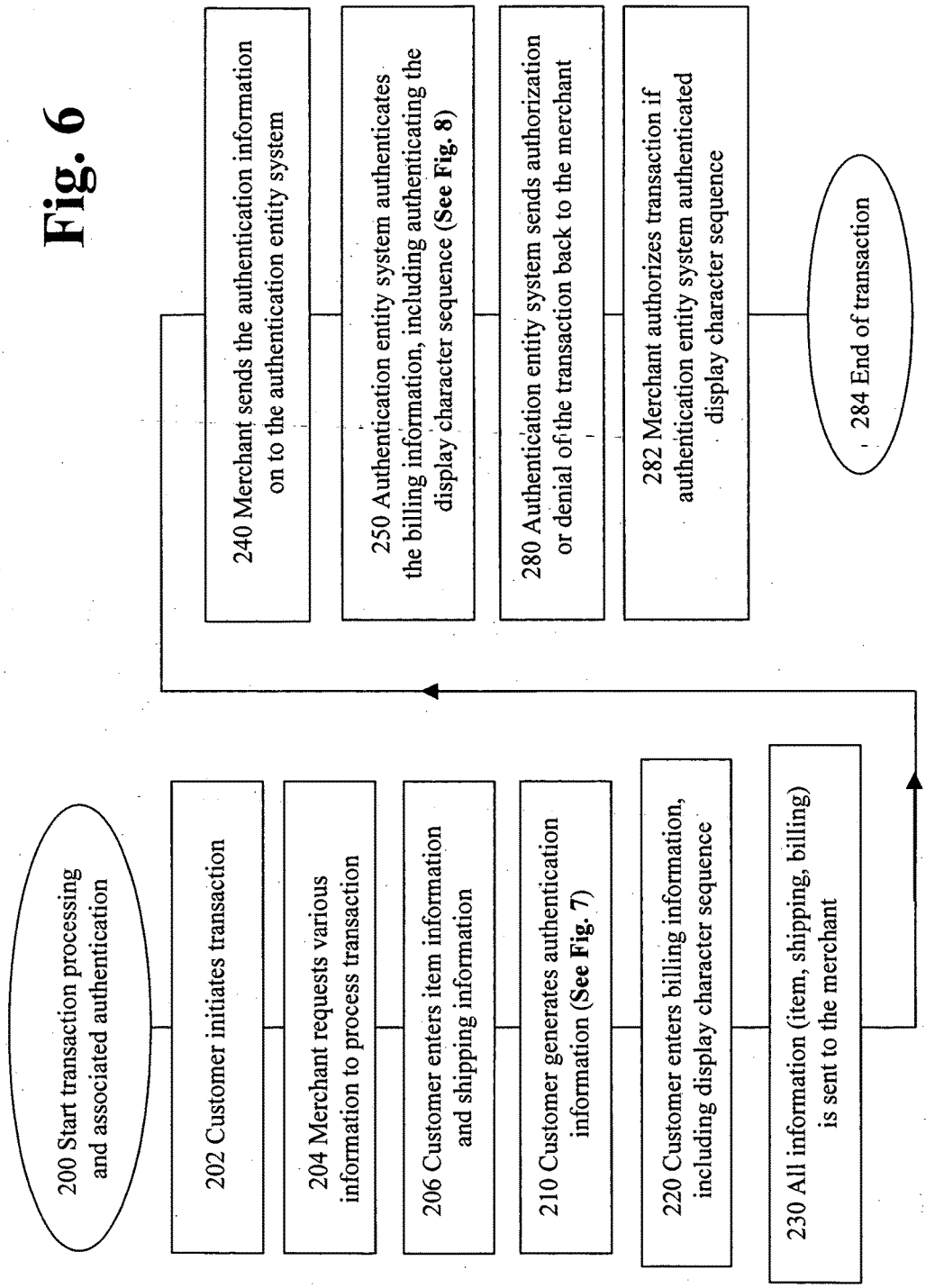

200 Start transaction processing and associated authentication
202 Customer initiates transaction
204 Merchant requests various information to process transaction
206 Customer enters item information and shipping information
210 Customer generates authentication information (See Fig. 7)
220 Customer enters billing information, including display character sequence
230 All information (item, shipping, billing) is sent to the merchant
240 Merchant sends the authentication information on to the authentication entity system
250 Authentication entity system authenticates the billing information, including authenticating the display character sequence (See Fig. 8)
280 Authentication entity system sends authorization or denial of the transaction back to the merchant
282 Merchant authorizes transaction if authentication entity system authenticated display character sequence
284 End of transaction

Fig. 7

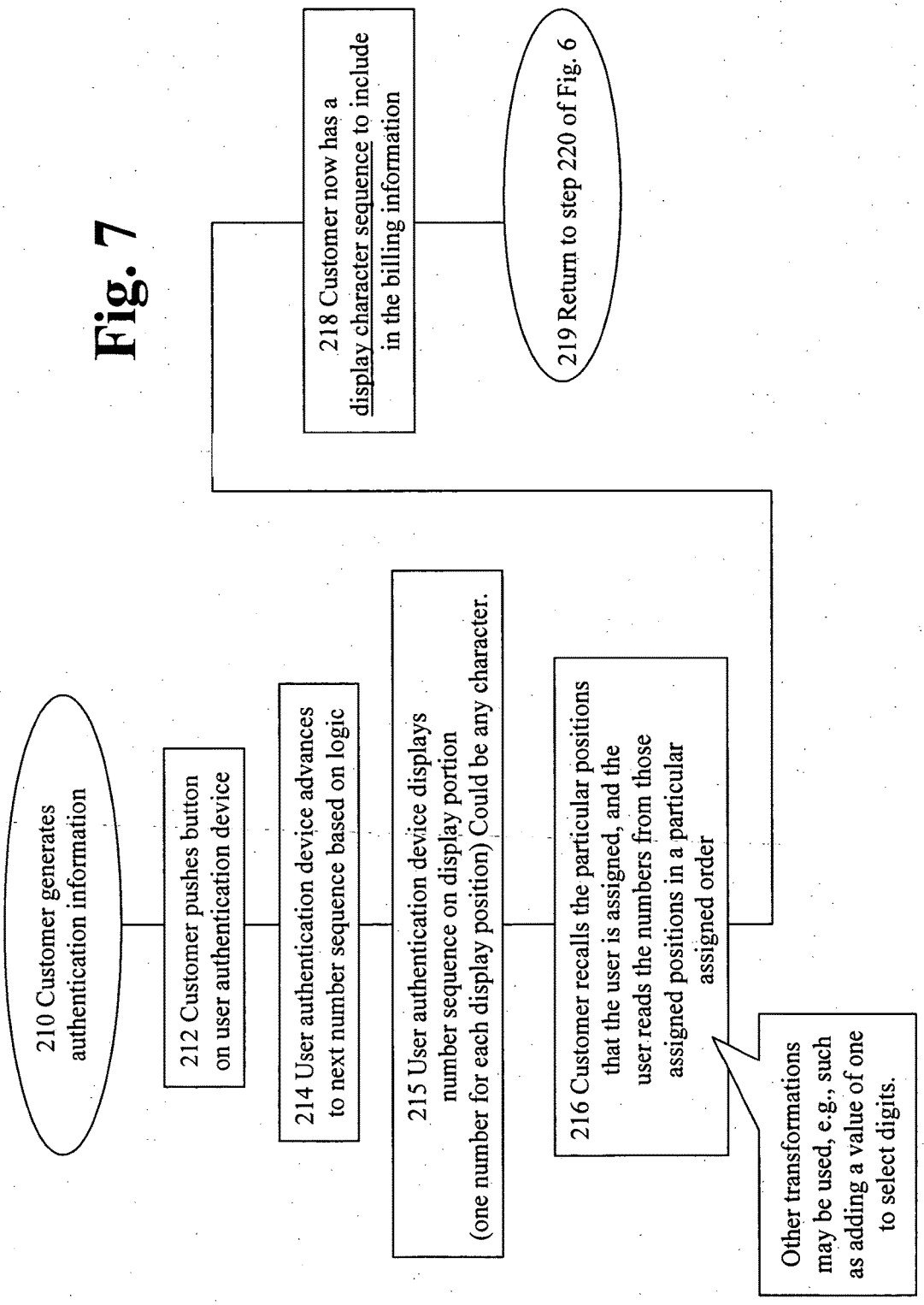

210 Customer generates authentication information
212 Customer pushes button on user authentication device
214 User authentication device advances to next number sequence based on logic
215 User authentication device displays number sequence on display portion (one number for each display position) Could be any character.
216 Customer recalls the particular positions that the user is assigned, and the user reads the numbers from those assigned positions in a particular assigned order
Other transformations may be used, e.g., such as adding a value of one to select digits.
218 Customer now has a display character sequence to include in the billing information
219 Return to step 220 of Fig. 6

Fig. 8

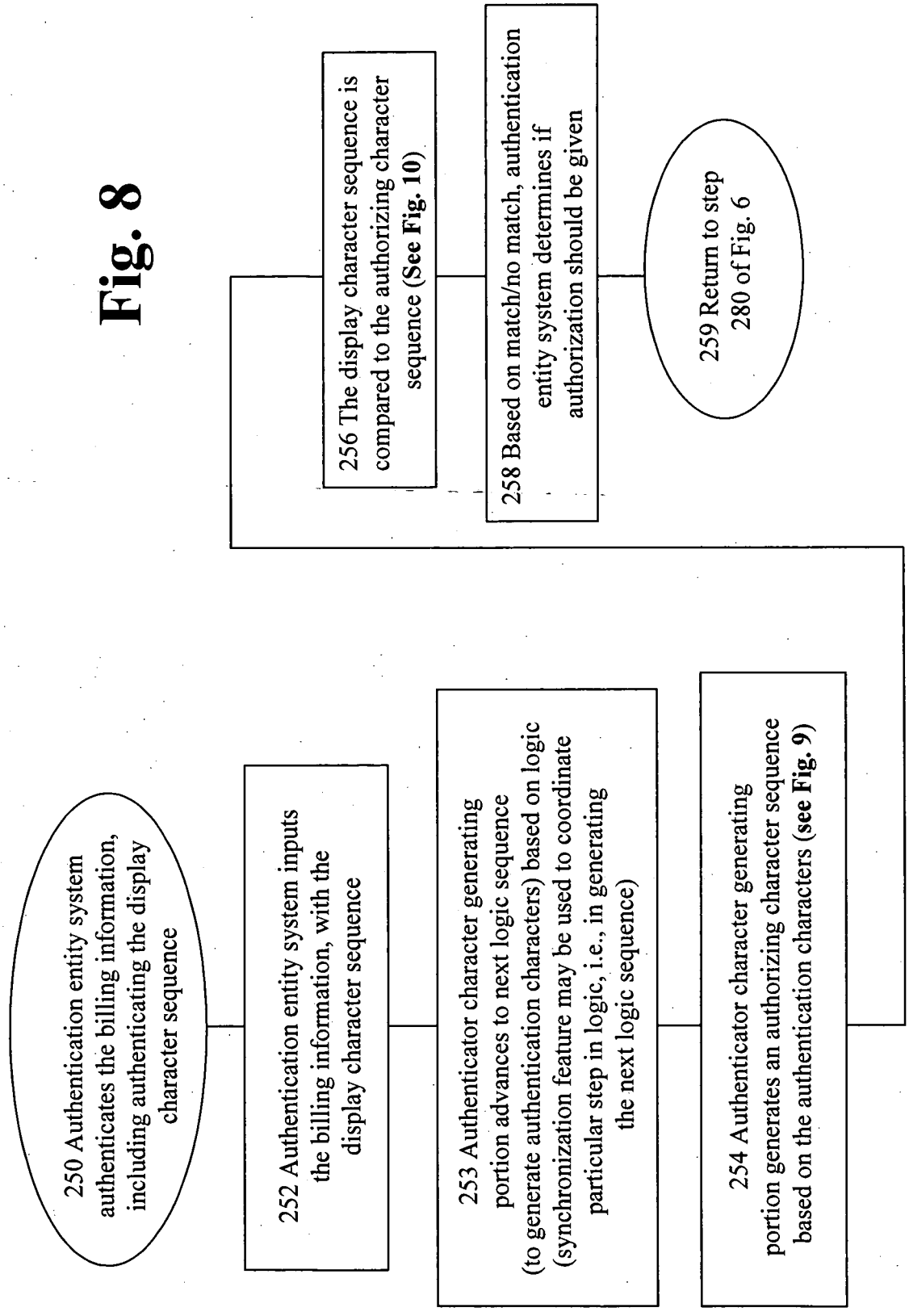
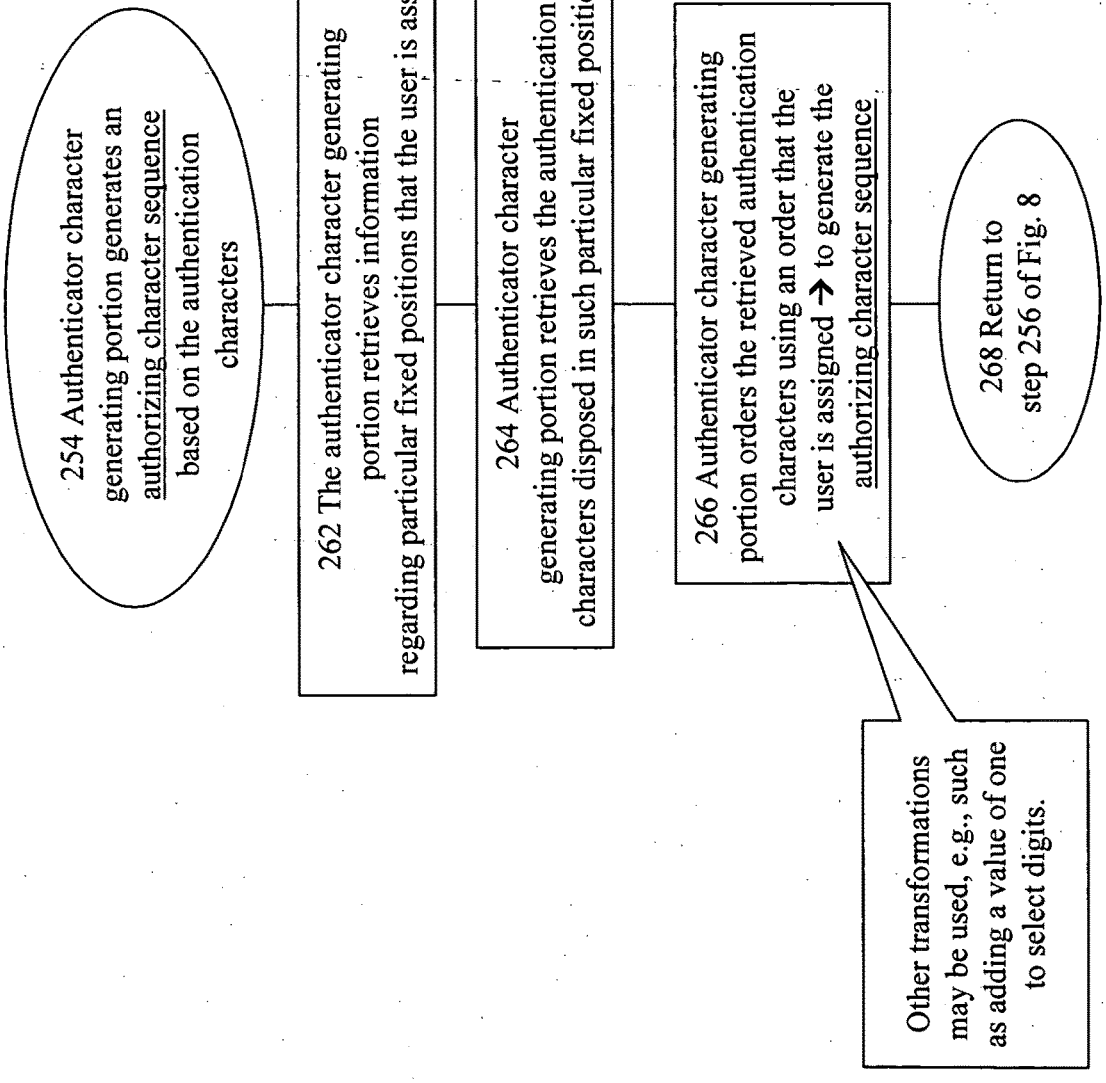

250 Authentication entity system authenticates the billing information, including authenticating the display character sequence
252 Authentication entity system inputs the billing information, with the display character sequence
253 Authenticator character generating portion advances to next logic sequence (to generate authentication characters) based on logic (synchronization feature may be used to coordinate particular step in logic, i.e., in generating the next logic sequence)
254 Authenticator character generating portion generates an authorizing character sequence based on the authentication characters (see Fig. 9)
256 The display character sequence is compared to the authorizing character sequence (See Fig. 10)
258 Based on match/no match, authentication entity system determines if authorization should be given
259 Return to step 280 of Fig. 6

Fig. 9


254 Authenticator character generating portion generates an authorizing character sequence based on the authentication characters
262 The authenticator character generating portion retrieves information regarding particular fixed positions that the user is assigned
264 Authenticator character generating portion retrieves the authentication characters disposed in such particular fixed positions
266 Authenticator character generating portion orders the retrieved authentication characters using an order that the user is assigned → to generate the authorizing character sequence
268 Return to step 256 of Fig. 8
Other transformations may be used, e.g., such as adding a value of one to select digits.

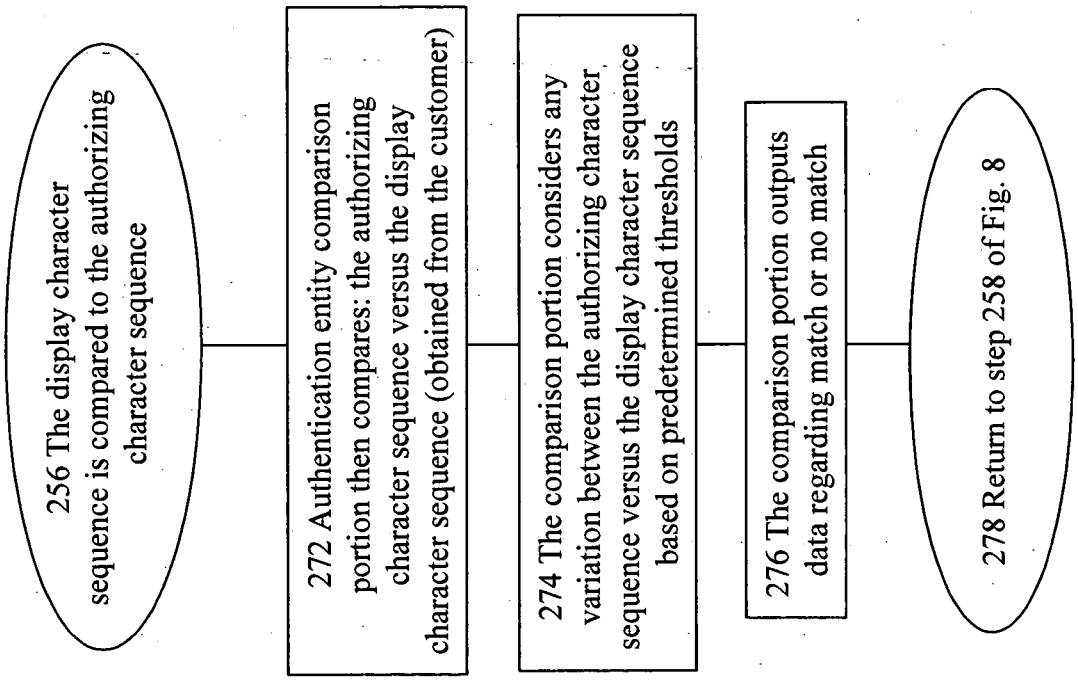
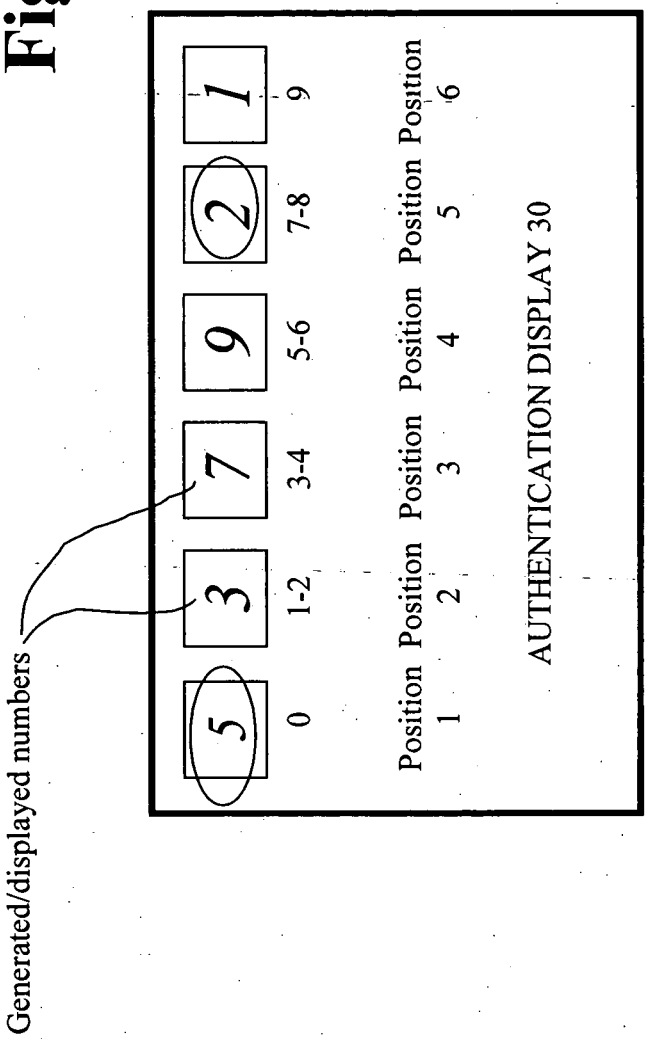

256 The display character sequence is compared to the authorizing character sequence
272 Authentication entity comparison portion then compares: the authorizing character sequence versus the display character sequence (obtained from the customer)
274 The comparison portion considers any variation between the authorizing character sequence versus the display character sequence based on predetermined thresholds
276 The comparison portion outputs data regarding match or no match
278 Return to step 258 of Fig. 8

Fig. 10

Fig. 11


Generated/displayed numbers
5
3
7
9
2
1
0
1-2
3-4
5-6
7-8
9
Position 1
Position 2
Position 3
Position 4
Position 5
Position 6
AUTHENTICATION DISPLAY 30

SYSTEMS AND METHODS FOR MULTIFACTOR AUTHENTICATION

CROSS REFERENCE TO PROVISIONAL APPLICATIONS

[0001] This application is a Continuation-in-Part (CIP) application of U.S. patent application Ser. No. 10/419,107 filed Apr. 21, 2003 (Attorney Docket No. 47004.000204), which is a Continuation-in-Part (CIP) application of U.S. patent application Ser. No. 10/105,471 filed Mar. 25, 2002, both of which are incorporated into the present application in their entirety.

[0002] The subject matter of this application is related to the subject matter of U.S. Provisional Application Ser. No. 60/646,622 filed Jan. 26, 2005 (Attorney Docket No. 47004.000322), assigned or under obligation of assignment to the same entity as this application, from which application priority is claimed for the present application. The subject matter of this application is also related to the subject matter of U.S. Provisional Application Ser. No. 60/661,488 filed Mar. 15, 2005 (Attorney Docket No. 47004.000322), assigned or under obligation of assignment to the same entity as this application, from which application priority is claimed for the present application. Provisional application U.S. Ser. No. 60/646,622 and Provisional application U.S. Ser. No. 60/661,488 are both incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

[0003] Authenticating people, particularly remotely, has been a difficult operation to make resistant to attack. Since single authenticating techniques are vulnerable to theft, it has become attractive to various groups to devise ways to do multi factor authentication, where more than one of (something you have, something you know, something you are) is used in demonstrating the identity of a person whose identity is to be established.

[0004] Typically, doing this has involved using relatively complex or expensive devices such as cards with keyboards on them (where you authenticate to the card and then use it), fingerprint readers, or digital certificates requiring public/private encryption to validate the presenter is in possession both of a password and of a private key.

[0005] All this complexity has delayed widespread use of such systems, since the cost of giving out hundreds of millions of copies of them has been kept high by the need to authenticate two or more things, and the cost of building the system components.

SUMMARY AND BRIEF DESCRIPTION OF THE INVENTION

[0006] The invention provides an authentication system and method. In particular, the invention provides a method for performing a financial authentication utilizing a token associated with a user, the method comprising the token generating a set of display characters that are viewable by the user, the token generating the display characters using logic; the user transforming a portion of the set of display characters using a transformation process, based on knowledge of the user, so as to form a display character sequence; the user outputting the display character sequence to an authentication entity; and the authentication entity authenticating the display character sequence using the logic and knowledge of the transformation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The present invention can be more fully understood by reading the following detailed description together with the accompanying drawings, in which any like reference indicators are used to designate like elements, and in which:

[0008] FIG. **1** is a diagram showing aspects of an encryption process in accordance with one embodiment of the invention;

[0009] FIG. **2** is a flowchart showing further aspects of the encryption process in accordance with one embodiment of the invention;

[0010] FIG. **3** is a block diagram showing an authentication system in accordance with one embodiment of the invention;

[0011] FIG. **4** is a block diagram showing further details of an authentication system, and in particular the authentication entity system, in accordance with one embodiment of the invention;

[0012] FIG. **5** is a diagram showing processing associated with display characters in accordance with one embodiment of the invention;

[0013] FIG. **6** is a high level flowchart showing an authentication process in accordance with one embodiment of the invention;

[0014] FIG. **7** is a flowchart showing further details of the "customer generates authentication information" step of FIG. **6** in accordance with one embodiment of the invention;

[0015] FIG. **8** is a flowchart showing in further detail the "authentication entity system authenticates the billing information, including authenticating the display character sequence" step of FIG. **6** in accordance with one embodiment of the invention;

[0016] FIG. **9** is a flowchart showing in further detail the "authenticator character generating portion generates an authorizing character sequence based on the authentication characters" step of FIG. **8** in accordance with one embodiment of the invention;

[0017] FIG. **10** is a flowchart showing in further detail the "display character sequence is compared to the authorizing character sequence" step of FIG. **8** in accordance with one embodiment of the invention; and

[0018] FIG. **11** is a diagram showing further aspects of an encryption process relating to a purchase amount in accordance with one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0019] Hereinafter, various aspects of embodiments of the invention will be described. As used herein, any term in the singular may be interpreted to be in the plural, and alternatively, any term in the plural may be interpreted to be in the singular.

[0020] What is proposed here is a system and method which provides a form of two factor authentication which resists theft of the authentication tokens even by someone who can intercept the authentication messages in total, in accordance with one embodiment of the invention. The invention can be supported using relatively very simple hardware.

[0021] One embodiment uses a token which displays numbers that change (either with time or with uses, but in ways that cannot be easily predicted by observation) but whose values can be tracked and predicted by an authenticating authority (who issued the tokens generally). In accordance with one embodiment of the invention, the token will display a set of numbers which will have their positions labeled (e.g., 1 through 6, for a 6 digit display). FIG. **1** is a diagram illustrating such a token **100**.

[0022] In accordance with one embodiment of the invention, a customer will be told ahead of time, "choose three positions of the display **10**, as shown in FIG. **1**, you will select in order, and remember the positions and order you picked." The customer authenticates by getting his token to display a new set of numbers (which should change so that their values are effectively unpredictable), and then to report the values in the three positions he chose and told the authenticating authority about earlier.

[0023] FIG. **1** shows the display of the token **100** in an "off" position. Once the customer activates the display in some manner, i.e., pushes a button, the token is turned on, and numbers are seen on the display. Thus, as shown in FIG. **1**, suppose the display **10** reads: and the customer decided to report position 5, 1, and 4 in that order. The customer would then transmit the 5th, 1st, and 4th digits in order: 2 5 9

[0024] Note that this authenticates the customer as an individual since the customer demonstrates that he knows the pattern registered earlier, but also it shows the customer has the token he was given. Thus, at a stroke he has provided a two factor authenticator. Note too that someone who can see the digits sent cannot replay them usefully. That person does not know the pattern, nor does she have the token, and she must have both to use the token successfully.

[0025] In accordance with one embodiment of the invention, another set of labels may be provided under the display, like 01, 23; 45, 67, 89. In processing a transaction, the customer is asked, later in a transaction, to encode a few digits of the transaction amount as positions of the display, and then requested to transmit the digits. This too can be easily verified by a payment processor (who has the amount as part of a payment record), and it shows that someone with the token agreed to the payment amount. In effect, this is a signing by the customer (who would have authenticated as an individual moments before with the same token) of the transaction amount. Similarly, any external observer will be unable to deduce any of this from the digits transmitted. The customer may be told what the purchase amount is. Accordingly, for example, if the customer is told the purchase amount was $872.00, the customer would report the characters shown in the position five, position five and position two, i.e., if the display was labeled 0, 1-2, 3-4, 5-6, 7-8, 9.

[0026] In further illustration, FIG. **11** shows a token **30** so labeled. In this example, the displayed number is 5 3 7 9 2 1. Accordingly, with a purchase amount of $872, the customer would report the displayed numbers in the positions, 5, 5, 2, i.e., the customer would report the numbers 2 2 3. In this manner, an authentication entity can confirm that the customer indeed knows what the customer is agreeing to, e.g., a dollar amount. It is appreciated that such processing adds complexity, but may be desired in some circumstances, e.g., in high dollar transactions. To reduce the complexity, a prompt screen might be provided to the customer so as to take them through the process, e.g., a window on a web page.

[0027] It is appreciated that an alternative data manipulation that can be done by the user-customer could be used here instead of the pattern selection described above. That is, the customer does need to manipulate the displayed numbers in some manner known to him (and the authenticating authority) so as to generate an output from such manipulation. However, the selection scheme described above may be desirable since it appears easy to use and remember by the customer

[0028] In implementation of the invention, it is not needed that numbers be used on the display. That is, any of a wide variety of graphics, letters, symbols, glyphs, runes, images or other indicia, for example, might be used in lieu (or in combination) with numbers.

[0029] It should be appreciated that the various features of the present invention may be used in conjunction with other encryption technology and/or features. In particular, the various features of the present invention may be used in combination with any of the features described in U.S. patent application Ser. No. 10/419,107 filed Apr. 21, 2003 (attorney docket number 47004.000204), which is incorporated herein by reference in its entirety.

[0030] In explanation of further aspects, in accordance with one embodiment of the invention, the problem being addressed is in the area of authentication. Authentication of customers to a bank is vital since the entire business is involved with caring for other peoples' money and using it per their instructions. If the owners cannot be identified, their instructions cannot be followed and the business collapses. When trying to identify people over computer links, this is harder than otherwise. One of the major issues is that spyware and other man in the middle attacks on information passed for authentication are very common. By providing people with a token that can produce an effectively random number which an authority can compute as well, anytime it is needed, people might be able to prove clearly that they have the token. Unfortunately, theft of tokens (even from the mails) is also common. It is desirable in addition to know for high value transactions that one is dealing with the person who claims to be dealing with you rather than knowing only that whoever you are dealing with has the person's token. Moreover, while it is common practice just to ask for another password or PIN (personal identification number), these are all too easily intercepted. The proposed scheme here solves those problems.

[0031] Hereinafter, the invention will be described from a further perspective, in accordance with one embodiment. Given that two parties who must authenticate one to the other both have means to generate an effectively random number (which means it is computationally infeasible to compute the next such number from the prior ones without a secret shared by the two) which can nevertheless be generated by both and tracked so that the one doing the authentication can (1) figure out the value the other one has, (2) find some transformation of the number or part of it which can be easily done by hand, and (3) have both parties agree to this transform (which can be thought of as a simple encryption) ahead of time. Now when the one not doing the authentication needs to authenticate the other, make sure they have generated a "random" number and have the one being authenticated perform the agreed on operation and report the value thereof. This may be as simple as picking an order in which to report several of the digits of the random number, as described above. Then, the one doing the authen-

tication performs the same transform on his copy of the random number and checks if the value is correct. Note that anyone observing the numbers picked will see only the random numbers, not the secret method by which they were produced, and thus will have nothing very useful in attempting a replay or PIN theft.

[0032] To explain further, the ideas of doing a second encryption, and that of permuting numbers or using a Caesar cipher, are old. However, the scheme here, because it is used with effectively random numbers, is much stronger than a permutation or Caesar cipher or other hand encryption method because of the absence of usable order in the material being encoded. An attacker must solve a cipher on a "plaintext" random number which in general is generated every time needed and used once. This makes it exceedingly difficult for a man in the middle to steal the person's authentication. Also, whatever token system is used to provide the pseudo random numbers and track them or synchronize them needs no additional complexity. This makes the scheme more cost effective than systems using conventional passwords or PINs, digital certificates, and other such complexities.

[0033] FIG. **2** is a flowchart in accordance with one embodiment of the invention. As shown, the present invention provides a novel way to authenticate a customer or other person.

[0034] The invention might be compared to a known one-time pad. One time pad cryptography is usually illustrated with the pad values being XORed with data. In effect, embodiments of the invention perform an encryption hand operation on display characters displayed by a token. As shown in the example of FIG. **2**, if the "random number" choices are changed appropriately, we could produce 3 digit outputs from 000 to 999, i.e., the entire range possible. This means we may have no test possible to pick the correct key as an observer in the middle. This makes the operation the user undertakes (which might be the illustrated permutation or anything else convenient) far stronger than what the same operation on normal text might be. The user operation remains a simple one, but the fact that it operates on one time data which is effectively random makes it basically as strong as the randomness. Where the cipher and key are well chosen which may be used for computing the numbers to be synchronized the resulting ciphertext may be treated as random and the discussion above holds.

[0035] FIG. **3** is a block diagram showing an authentication system **100** in accordance with one embodiment of the invention. The authentication system **100** includes a user authentication device **120**. The user authentication device **120** may be in the form of a token, for example. The user authentication device **120** provides the user with display characters (for example numbers) **192** (see FIG. **3**) that are used by the user to effect an authentication, as discussed below.

[0036] As shown in FIG. **3**, the user authentication device **120** includes a display character generating portion **124** and a display portion **130**. The display portion **130** includes a plurality of display positions **138**, i.e., display positions (**131-136**). Each display position **138** is a display, i.e., such as an LCD display, that displays a number, or any other character, so as to be visually observed by a user **110**, in accordance with one embodiment of the invention.

[0037] The display character generating portion **124** generates the characters that are displayed in the display portion **130**. In particular, the display character generating portion **124** uses predetermined logic (i.e., a suitable algorithm) to populate the display positions **138**. This logic provides a predetermined progression of numbers, or other characters, that may be similarly generated by an authentication entity system **140**.

[0038] In accordance with one embodiment of the invention, the user authentication device **120** has a button **121**, which may be pressed by a user **110**. Upon pressing the button **121**, the display character generating portion **124** generates the characters that are displayed in the display portion **130**. Accordingly, the user **110** interfaces with the user authentication device **120** using the button and visually, in accordance with one embodiment of the invention.

[0039] The user authentication device **120** further includes a device memory portion **126**. The device memory portion **126** serves as a memory or database, as is needed to perform the various functions of the user authentication device **120**.

[0040] As shown in FIG. **3**, the authentication system **100** also includes an authentication entity system **140** and an illustrative merchant **180**. Illustratively, the user **110** (using the user authentication device **120**) interfaces with the merchant **180** so as effect a desired transaction. The transaction might be over the telephone, the Internet, or any other communication channel, as desired.

[0041] Accordingly, the systems and methods of embodiments of the invention may be used in any "transaction", including a conveyance of information, in which authentication of a user is needed or desired. Such transaction might include a telephone transaction, Internet transaction (such as an Internet purchase), network transaction, infrared transaction, radio signal transaction, credit card transaction, debit card transaction, smart card transaction, ACH transaction, stock trade transaction, mutual fund transaction, swap, PAYPAL® transaction, BILL ME LATER® transaction, electronic funds transfer transaction, financial application transaction, an arrangement to set up payments to an entity, a verification, an ATM transaction, and/or a message, for example. For example, such a transaction might include a message from one human user to another human user, a human user communicating with an electronic device, and/or two electronic devices communicating with each other. The transaction may or may not be in a financial context, i.e., for example, the message might be authorizing the opening of a door or the transfer of a non-financial related message, for example.

[0042] Accordingly, FIG. **3** shows a communication channel **160** over which the transaction is performed. The communication channel **160** carries an authorization request **162**. Subsequent to the request being processed by the authentication entity system **140**, the communication channel **160** then carries an authorization **164**, in the example of FIG. **3**. However, it is of course appreciated that the authentication entity system **140** might alternatively not authorize the requested transaction. As shown in FIG. **3**, the authorization request **162** and the provided authorization is passed through the merchant **180**. However, in an alternative embodiment, the authorization request **162** and/or the authorization provided **164** might be communicated to the authentication entity system **140** in some other manner, such as by some third party, and not via the merchant **180**. Further, it is appreciated that the user authentication device **120** need not take on the form of the device shown in FIGS. **1** and **3**, for example. That is, for example, the user authentication device

120 might be in the form of a software program running on a computer, or in some other alternative form.

[0043] FIG. **4** is a block diagram showing further details of the authentication entity system **140**. The authentication entity system **140** includes an input portion **142** and an entity memory portion **144**. The input portion **142** interfaces with the communication channel **160** so as to communicate data, i.e., such as the authorization request **162** and the authorization provided **164** information. The entity memory portion **144** serves as a database to store various data associated with, and needed by, operation of the authentication entity system **140**.

[0044] The authentication entity system **140** also includes an authenticating processing portion **150**. The authenticating processing portion **150** performs the various processing of the authentication entity system **140**. In particular, the authenticating processing portion **150** includes an authenticator character generating portion **152** and a comparison portion **154**. The authenticator character generating portion **152** generates an authorizing character sequence **198** to be used to authenticate the transaction initiated by the user **110**. In turn, the comparison portion **154** performs a comparison between the authorizing character sequence **198** (generated by the authenticator character generating portion **152**) and the display character sequence **194** (provided by the user-customer).

[0045] FIG. **5** is a diagram showing further features in accordance with one embodiment of the invention. Specifically, FIG. **5** shows aspects of the generation and the manipulation of the display characters **192** (generated by the display character generating portion **124**) and the authentication characters **196** (generated by the authenticator character generating portion **152**). Both the portions (**124**, **152**) use the same logic (i.e., random logic as described above) to generate sets of characters (**192**, **196**) in some predetermined manner. That is, the display character generating portion **124** will generate the same characters as the authenticator character generating portion **152** in a progressive manner. As used herein, the generation of a new set of characters by the portions (**124**, **152**) is characterized as generating the next "logic step". To explain in other words, the display characters **192** associated with a particular logic step, will be the same as the authentication characters **196**, if for the same logic step, in accordance with one embodiment of the invention. Thus, the particular logic step (that each of the display character generating portion **124** and the authenticator character generating portion **152** are at) will dictate the particular set of characters that are generated.

[0046] As described in detail herein, once the display characters **192** are generated on the user authentication device **120**, the user observes only the particular display positions **138** that the user is assigned, i.e., the user might make this choice upon activation of the user authentication device **120**. As described in the example above, the user might have picked the 1, 4 and 5 positions to be the selected positions (from which the user **110** actually uses the characters). The user **110** then orders the select display characters **192** in a predetermined manner. In particular, FIG. **1** described above shows an example of this ordering. Once the selected display characters are ordered, this results in a "display character sequence" **194**, as used herein. It is this display character sequence **194** that is submitted to authenticate the desired transaction, in accordance with one embodiment of the invention in which ordering is used as the transformation to the display characters **192**.

[0047] In a parallel manner to the user **110**, the authentication entity system **140** generates authentication characters **196**, selects particular authentication characters **196** as agreed upon with the customer, and then orders the selected authentication characters **196**. In this manner, the authentication entity system **140** generates a sequence of characters (e.g. a number) that may be compared with the display character sequence **194** (submitted by the user/customer).

[0048] It is appreciated that the authentication entity system **140** may perform variations on the above processing methodology. That is, the authentication entity system **140** may not in fact generate all the authentication characters **196**, but rather only the select authentication characters **196** that will indeed be used in the ordered set, which constitutes the authorizing character sequence **198**. This approach might somewhat limit needed processing since the authentication entity system **140** is of course aware that only select characters in the authentication characters **196** will indeed be used. However, this approach would generally not be performed with the user authentication device **120**, since the inclusion of all the display characters **192** (and subsequent disregarding of some of the display characters **192** by the user **110**) is part of the encryption process.

[0049] In further explanation of the invention, FIG. **6** is a high level flowchart showing an authentication process in accordance with one embodiment of the invention. As shown in FIG. **6**, the process starts in step **200**. Then, in step **202** in this example, the customer initiates a transaction. In this example, the transaction is with a merchant. After step **202**, the process passes to step **204**.

[0050] In step **204**, the merchant requests various information from the customer so as to process the transaction. Accordingly, in step **206**, the customer enters item information, i.e., regarding the particular item that the customer is purchasing, and shipping information. It should of course be appreciated that the merchant may request, and the customer may enter, any of a variety of desired information. After step **206** of FIG. **6**, the customer prepares billing information. Specifically, in step **210**, the customer generates authentication information to accompany the customer's submission of other billing information. Further details of step **210** are described in conjunction with FIG. **7** below.

[0051] Then, in step **220** of FIG. **6**, the customer enters the billing information including authentication information, i.e., including a display character sequence for use by an authentication entity system in authenticating the transaction. After step **220**, the process passes to step **230** of FIG. **6**.

[0052] In step **230**, all the information (item, shipping, billing) that the customer has prepared is sent to the merchant. Then, in step **240**, the merchant sends the authentication information on to the authentication entity system, i.e., for authentication of the transaction that the customer is requesting the merchant to process. Then in step **250**, the authentication entity system authenticates the billing information, including authenticating the display character sequence that the customer has provided. Further details of step **250** are described below with reference to FIG. **8**.

[0053] After step **250** of FIG. **6**, the process passes to step **280**. In step **280**, the authentication entity system sends authorization, or alternatively denial, of the transaction back to the merchant. Then, the process passes to step **282**. In step

282, the merchant authorizes the transaction if the authentication entity system authenticated the display character sequence. It is appreciated that other authentication processing may accompany the authentication of the customer's display character sequence, i.e., such as authentication of a personal identification number (PIN). That is, in general, the systems and methods of the invention as described herein may be used in conjunction with other security/authentication measures or technologies.

[0054] After step **282** of FIG. **6**, the process passes to step **284**. In step **284**, the process of FIG. **6** ends.

[0055] FIG. **7** is a flowchart showing further details of the "customer generates authentication information" step **210** of FIG. **6** in accordance with one embodiment of the invention. The subprocess of FIG. **7** starts in step **210** and passes to step **212**. In step **212**, the customer pushes a button on the user authentication device, which the customer has been provided. In response to the customer pushing the button, or in some other manner interfacing with the user authentication device, in step **214**, the user authentication device advances to a next number sequence based on logic contained in the user authentication device (i.e., the user authentication device **120** displays information associated with the next "logic step" as described above). This logic may be in the form of an algorithm that generates a plurality of display characters in some predetermined manner, i.e., in a manner that an authentication entity system **140** may perform a generation of the same numbers based on the same logic.

[0056] Accordingly, in step **215** of FIG. **7**, the user authentication device displays a number sequence on the display portion, i.e., one number for each display position. However, it is of course appreciated that the invention is not limited to the use of numbers. That is, any suitable character or other indicia might be used in lieu of or in conjunction with numbers.

[0057] Then, in step **216**, the customer recalls the particular positions that the user is assigned. That is, out of six display positions, the customer only uses three numbers (associated with three display positions) so as to generate a display character sequence. In step **216**, the customer further reads the numbers from those particular assigned positions in a particular assigned order. Accordingly, in step **218**, the customer now has a display character sequence to include in the billing information.

[0058] After step **218**, the process passes to step **219** of FIG. **7**. In step **219**, the process returns to step **220** of FIG. **6**.

[0059] FIG. **8** is a flowchart showing in further detail the "authentication entity system authenticates the billing information, including authenticating the display character sequence" step **250** of FIG. **6** in accordance with one embodiment of the invention. The subprocess of FIG. **8** starts in step **250** and passes to step **252**.

[0060] In step **252** of FIG. **8**, the authentication entity system inputs the billing information, including the display character sequence from the customer. Then, in step **253**, the authenticator character generating portion (in the authentication entity system) advances to the next logic step, i.e., in parallel to the user authentication device **120**. That is, the authenticator character generating portion generates authentication characters based on the same logic as is implemented in the user authentication device. It should be appreciated that some synchronization feature may be used to coordinate the particular step in logic, i.e., in generating the next logic step. After step **253** of FIG. **8**, the process passes to step **254**.

[0061] In step **254**, the authenticator character generating portion in the authentication entity system generates an authorizing character sequence based on the authentication characters. Further details of step **254** are discussed below with reference to FIG. **9**. Then, in step **256** of FIG. **8**, the display character sequence is compared to the authorizing character sequence. Further details of step **256** are discussed below with reference to FIG. **10**. After step **256**, the process passes to step **258**.

[0062] In step **258** of FIG. **8**, based on a match or no match, the authentication entity system determines if authorization should be given. Then in step **259** of FIG. **8**, the subprocess of FIG. **8** returns to step **280** of FIG. **6**.

[0063] FIG. **9** is a flowchart showing in further detail the "authenticator character generating portion generates an authorizing character sequence based on the authentication characters" step **254** of FIG. **8** in accordance with one embodiment of the invention. In this illustrative subprocess, after starting in step **254** of FIG. **9**, the subprocess passes to step **262**. In step **262**, the authenticator character generating portion retrieves information regarding particular fixed positions that the user is assigned. Then, the process passes to step **264**.

[0064] In step **264**, the authenticator character generating portion retrieves the authentication characters disposed in such particular fixed positions. This processing is in parallel to the selection of numbers (from the display positions) as is performed by the customer. The, in step **266**, the authenticator character generating portion orders the retrieved authentication characters using an order that the user is assigned. As a result, the authenticator character generating portion generates an "authorizing character sequence", which is to be compared with the "display character sequence" that is provided by the user. As shown in FIG. **9**, other transformation processes might be used in lieu of ordering select characters. That is, any suitable transformation, e.g. such as ordering or adding a value of one, might be used to convert a plurality of selected characters (shown on the token display) to a display character sequence.

[0065] Thus, as otherwise noted herein, it is appreciated that some other transformation might be used in lieu of the ordering of the display characters **192**. For example, numbers might be added, some mathematical transformation may be applied, and/or the same number might be used twice, for example, as well as other variations described herein.

[0066] After step **266** of FIG. **9**, the process passes to step **268**. In step **268**, the subprocess of FIG. **9** returns to step **256** of FIG. **8**.

[0067] FIG. **10** is a flowchart showing in further detail the "display character sequence is compared to the authorizing character sequence" step **256** of FIG. **8** in accordance with one embodiment of the invention. After starting in step **256** of FIG. **10**, the subprocess passes to step **272**.

[0068] In step **272**, the authentication entity comparison portion compares: the authorizing character sequence versus the display character sequence (obtained from the customer). After step **272**, the process passes to step **274**. In step **274**, the comparison portion considers any variation between the authorizing character sequence versus the display character sequence based on predetermined thresholds.

[0069] In other words, it might be the situation that the display character sequence does not exactly match the authorizing character sequence. However, if the variation is limited, then the variation might be acceptable so that the authentication entity system will still authenticate the transaction. The particulars of what is acceptable and what is not acceptable variation may be based on thresholds, as is desired.

[0070] After step **274** of FIG. **10**, the process passes to step **276**. In step **276**, the comparison portion outputs data regarding match or no match back to the merchant. As a result, the merchant will process or not process the desired transaction. Then, in step **278** of FIG. **10**, the process returns to step **258** of FIG. **8**. Processing then continues as described above with reference to FIG. **8**.

[0071] In summary, in accordance with one embodiment of the invention, the scheme described herein uses the idea of a remote token synchronized with or tracked with a central authentication database, and uses a cipher as the secret to authenticate the user. The use of the cipher, which may typically be relatively simple, together with the remote token system provides a novel combination in accordance with one embodiment of the invention.

[0072] In accordance with embodiments of the invention, the method described herein may be implemented in innumerable different ways, i.e., such as picking different simple ciphers. But there must be local and remote effectively random numbers, in accordance with one embodiment of the invention, so that a simple operation on the numbers can be computed by a person and used to authenticate that the person is the right person to be using the token, rather than simply confirming that the toke is correct.

[0073] In summary, the invention relates to the notion of using second encryption with a token that generates changing numbers, so that the second encryption embeds or combines additional information with the token's number, so that authentication depends on both. The additional information might be a pattern or other information remembered by an individual, some parameter (like amount) of a payment or transaction, or any other information it is desired to verify.

[0074] The invention further relates to the notion of combining information in such a way that someone who can figure what the token will be generating might use it to reconstruct some information remotely, with no fear of the information being intercepted by man in the middle attacks. For example, this functionality is discussed above in conjunction with using a purchase amount to generate a display character sequence, i.e., using the purchase amount and matching digits (of the purchase amount) with labels under the display positions.

[0075] As discussed above, the authentication entity system **140** authenticates a display character sequence that is provided by the customer. In accordance with one embodiment of the invention, the authentication entity system **140** does not allow multiple submissions of a display character sequence. To explain, the multiple submission checking portion **156** (of the authentication entity system **140**) may perform a check on a newly submitted display character sequence. This check determines whether the particular display character sequence has been previously submitted, e.g., previously submitted in a particular period of time. If the multiple submission checking portion **156** determines that the particular display character sequence has been previously submitted, the authenticating processing portion **150** will not authenticate the display character sequence. For example, this might occur in the situation when a customer fails to press button **121** (on the user authentication device **120**) to generate a new number sequence. That is, a repeat display character sequence (based on the repeat number sequence) will not be authenticated. The check for multiple display character sequences provides a further fraud prevention measure. To effect such checking, it should of course be appreciated that the authenticating processing portion **150** may be provided with the ability to keep track of which display character sequences have been observed.

[0076] As described above, in accordance with one embodiment of the invention, the customer pushes a button on the user authentication device **120** and a number sequence is displayed. From the number sequence, the customer selects characters to form the display character sequence. It is appreciated that if the number sequence is all fives, i.e., 5 5 5 5 5 5 (or even 2 2 2 2 4 4), then the particular order that the user has selected will be irrelevant. For this reason, the content of the number sequence displayed on the user authentication device **120** may want to be controlled, i.e., so as to avoid excessive repeat of numbers or other characters.

[0077] In accordance with a further aspect of the invention, it is appreciated that it may be needed to synchronize the user authentication device **120** with the authenticating processing portion **150**. For example, it might be the situation that the user authentication device **120** has been exposed to multiple presses of the button (e.g., by a child). If the authenticating processing portion **150** receives a display character sequence that does not match with the next generated authorizing character sequence, the authenticating processing portion **150** may "run ahead." That is, the authenticating processing portion **150** may run ahead with the authorizing character sequences assuming that there have been presses of the button **121** which were not submitted to the authentication entity system **140**. The authenticating processing portion **150** may run ahead some predetermined number of times, until it finds a match, or alternately it reaches the predetermined number of times and concludes the display character sequence should not be authenticated.

[0078] Other approaches may be used to synchronize the user authentication device **120** to the authenticating processing portion **150**. For example, all the display characters (displayed on the user authentication device **120**) may be provided to the authenticating processing portion **150** (in the order that the characters are displayed) so as to perform synchronization. That is, given all the display characters in the displayed order, the authenticating processing portion **150** can then determine the correct point in the progression of the authentication characters.

[0079] Alternatively, the customer may provide two sets of display characters or two sets of display character sequences. These two sets, for example, might then be used by the authenticating processing portion **150** to synchronize with the user authentication device **120**. i.e., based on the two sets of display characters, the authenticating processing portion **150** could determine where in the progression the user authentication device **120** is disposed.

[0080] In accordance with one embodiment of the invention, the user authentication device **120** may be used in multiple manners. For example, a customer may use the authentication device **120** to generate the display character

sequence as described above, i.e., by selecting the display characters in a particular order. Such use may be implemented for Internet transactions, for example. However, in one embodiment, the same user authentication device **120** may also be used by submitting all the display characters to the merchant (and in turn the authenticating processing portion **150**). A higher exchange rate may be applied to the second use as compared with the exchange rate applied to the first use. For example, such differential in exchange rate might be applied since the second use bears higher risk than the first use. Illustratively, the second use might occur in a situation in which the user authentication device **120** is used in a restaurant, and a person other than the customer is effecting the transaction.

[0081] In accordance with a further embodiment of the invention, a single token may be given to a family, or provided to be used in some other situation in which multiple persons will use the same token, i.e., the same user authentication device **120**. In this situation, the user authentication device **120** will proceed through a progression of display characters, i.e., upon presses of the button **121**. However, different users of the user authentication device **120** will be assigned different display positions to read characters, as well as a different order in which to place those observed characters. Accordingly, for example, if a brother were provided the display character sequence of FIG. **1**, the brother will give the 2 5 9 number as shown in FIG. **1**. However, if the sister were given the same 5 3 7 9 2 1 display number, the sister might be assigned [position 5] [position 4] [position 1], i.e., and thus her display character sequence would be 2 9 5. Such embodiment allows different persons to collectively use the same user authentication device **120**, while documenting which person used the user authentication device **120** for which transaction. In other words, each persons might be assigned there own display character sequence. Alternatively, it is of course appreciated that multiple tokens may be used in a single household.

[0082] Further, in accordance with one embodiment of the invention, the same person might use the same user authentication device **120**, but be assigned different display character sequences for different uses of the user authentication device **120**. For example, given a display number of 5 3 7 9 2 1, the single user may be assigned ([position 5] [position 4] [position 1] (display character sequence would be 2 9 5)) for effecting financial transaction versus ([position 5][position 1] [position 4] (display character sequence would be 2 5 6)) for opening their garage door.

[0083] Relatedly, it is of course appreciated that the systems and methods of the invention as described herein may be used for any of a variety of situations that an authentication procedure is required. For example, the invention may be used for effecting financial transactions, accessing information, opening doors, controlling access to devices (e.g. access to a computer) and/or other situations where an authentication procedure is needed. In particular the invention may be used to prevent fraud in high risk and/or high value transactions, e.g., Internet, telephone and ATM transactions. It is also to be appreciated that the reduced risk of fraud associated with using the invention might typically result in a lower interchange fee, as compared to financial transactions using other known authentication methods.

[0084] Further, it is appreciated that the authentication device **120** may take any of a variety of forms and/or be combined with other devices. For example, the user authentication device **120** may be used or combined with a cellular phone, a PDA, an RFID device, and/or other devices. For example, it should be appreciated that the display character sequence, as described herein, may be used in the place of a traditional PIN (personal identification number). Accordingly, the display character sequence might be used in an ATM transaction. Such might be used to prevent ATM Fraud.

[0085] Hereinafter, various embodiments and aspects of embodiments will be described.

[0086] In one embodiment, the invention herein described is a method by which token authentication can be incorporated in payment systems with very minor changes at issuer sites and using mainly existing merchant facilities. The method may use a token which will generate a display of numbers which changes either with time or with uses—and whose values are unpredictable to the external observer who has not complete information about the internal (hidden) mechanisms, i.e., processing.

[0087] One aspect of the invention is the use of the display of such a token or the use of a function or selection from that display (the selection or function being done by the customer as something he remembers) as an authenticator reported instead of the existing CVV2 or CVC2 (or equivalent for other card brands) card authenticator string. The CVV2 field is normally printed on the back of payment cards and is often asked for in phone or net transactions. Its value is checked mainly by the card issuer. The checking routine described herein can easily be adapted to check the correctness of the token-derived numbers for that particular token. Accordingly, this field is already present, it is already handled by payment networks. Thus, the use of the display character sequence (in lieu of the CVV2 or CVC2) presents few problems either for merchant expense or network changes and only very minor expense for the issuer.

[0088] As noted above, a further aspect relating to one embodiment of the invention is the use of a token display in place of PIN values. Facilities for entering PIN values already are widespread anywhere payment cards exist, and a replacement for a PIN value where the replacement changes (and especially one which depends on the token the customer has and on the selection pattern he knows) gives a much stronger authentication of the customer than a fixed PIN. Using this replacement may require no new network or merchant changes, and as PINs are checked by issuer only, the changes to issuer system would be basically limited to the PIN validation routines, which are well known and can be readily added to, i.e., so that issuer would validate the display character sequence, as opposed to a PIN.

[0089] Accordingly, in summary, it is noted that the display from a token with a display of variable numbers, or a function or permutation or selection from that display, may be used as an authenticator instead of CVV2 or CVC2 in credit card processing. Further, the display from such a card, or a permutation or selection from such a display, might be used instead of a PIN in card transactions or the logical equivalent thereof.

[0090] As described above, when a customer pushes the button on the token, e.g., the button **121** on the user authentication device **120**, the display will show some numbers. In one embodiment, two digits display the least significant digits of an internal counter and 3 to 6 digits (preferably 6) display part of the result of encrypting the internal counter using an encryption key which is hidden

within the card, and which may different for every card, i.e., the key should be different enough that anyone analyzing the innards of a card cannot compute the key for a different card even though he may know the complete keys of several other cards. Values may be supplied for these "diversified keys". In one embodiment, the encryption algorithm used may be a "strong" crypto algorithm, as strong as triple DES or better, but may depend on the particular use.

[0091] In one embodiment, when the button **121** is pressed, the idea is that the internal counter increments, and the Bank tracks its value, with the aid of the 2 digit low order display. It may be acceptable if the display is in octal radix instead of decimal if cost effective. The display needs to be visible either while the button is pressed, or for an interval after the button is pressed, so that the customer has at least 30 seconds (and preferably longer) to refer to it as he may need to compare it to other displays or transcribe it or recite it over the phone. The button must of course be very well debounced, and could well be used to e.g. drive a one-shot multivibrator so that it could be impossible to increment the counter more than once a minute. Something may be provided to ensure that the counter will increment by one only and not by large counts, i.e., even if the button is electrically noisy.

[0092] In one embodiment, the device may live for the 2-3 years that a credit card is issued for. Thus the power supply must suffice for this and for the expected number of uses the device will have. It may be preferable, in particular from a marketing perspective to have the device housed in a credit card. As noted herein, the incorporation of RFID functions may also be used.

[0093] In accordance with one embodiment of the invention, the invention authenticates a bank to a customers. On web pages we will want to assure customers they are talking to the real bank. Therefore we can ask them for the 2 digit counter display they see on pushing their button, and using our tracking data predict the internal counter value. By encrypting that with the card's key (we may have to ask for customer name or account number too), we can predict the display and tell the customer "your display will read nnnnnnnn if you are talking to the real bank. If not, hang up immediately and give no further information."

[0094] In one embodiment, the token is authenticated to the bank. In this aspect of use of the inventive token, the bank asks a customer to push the button and read the display. The process includes using the 2 digit display (which may be positioned alongside the display characters) to help determine what the counter is and compute the display and see if they match. If they don't, it is possible to try to assume the counter might be 100 or 200 or more. Accordingly, a few more encryptions may be attempted to see if the token value provided by the customer is indeed OK. Accordingly, a 2 digit display may be used in addition to the display of FIG. **1** so as to assist in determining where the customer is disposed in the progression of the token displays, i.e., if the customer's kids have been playing with the token button.

[0095] In accordance with a further aspect of the invention, a process may authenticate the customer to the bank. As described above, each customer is requested to pick an order in which to report digits of the display. We can have the digits numbered in print on the cards to facilitate this. Then the customer pushes his button, reports digits in the order he said he would use. Thus if the display shows: and the customer said he would report digits in order 5, 1, 6, 3 (which he has to remember), he tells us the "77" part (if it is agreed upon for him to do so) and reports 3, 5, 9, 1 (the 5th, 1st, 6th, and 3rd digits of the random part). This relies on the token AND the customer memory. Also anyone in the middle who might be watching or recording what keys are pressed (remember lots of customer PCs have key loggers running) gets only random digits. Thus it doesn't matter if someone tries to record what the customer typed: it will change every time. Notice too that if the customer authenticates this way, it shows he has the token AND knows the pattern all at one go. The number of combinations is 6*5*4*3=360, high enough to cut accidental matches decently. We could ask for more than 4 digits if a higher number of combinations were required.

[0096] As also described above, it may be that we will want to end any web transactions by authenticating a second time, so that a thief who broke in and tried to use the credentials later, i.e., for a different transaction, would be detected.

[0097] In use of the described device for credit card transactions, instead of web, the customer may simply report the value of the display (or possibly the first several digits of the display) when asked for CVV2. It is noted that CVV2 reports may be 5 or more digits long, so the counter value AND some ciphertext could be reported. Alternatively the first part of the ciphertext could be reported for CVV2 if no more than 3 digits were accepted. At the back end, we would assume the counter incremented by 1 and compare, repeating for higher counter values till a comparison matched or we gave up, i.e., we would roll the counter ahead until we identified a match. In accordance with one embodiment of the invention, the back end has to track the counter in all cases. We expect that merchants will quickly start accepting CVV2, and accepting longer CVV2, to handle these devices since the quality of identification will be much higher than otherwise on phone or net orders, and they may eliminate substantial monies in fraud losses for merchants per year.

[0098] As described above, the user authentication device **121**, e.g., a token, of the invention may be in a variety of forms. Also, the user authentication device **120** may be used in conjunction with a variety of features, as described below.

[0099] Optical light emitting devices (OLED) generally need to be fabricated on thin substrates with some electronics to control current flow to the light emitting polymers. It might be sensible to think of building a backplane for such devices (which are very thin and flexible) on which you also etch transistors and the like to perform the counting, debouncing, crypto, and possibly display timing as well, in one embodiment. A bit of flash memory may be built onto this backplane (to hold the counter value and a diversified key, if so desired. This would mean that all connections become part of a printed circuit, and the arrangement might be in the form of a small rectangle laid down in the inside of a card, to be covered by a transparent cover. Then the connections might only be to a battery and button.

[0100] In accordance with one embodiment of the invention, a piezoelectric element may be used for power. In such an arrangement, the customer would press on a printed circle, i.e., to press the element and generate electricity, avoiding button contacts. Also, pressing or bending energy might be used, if workable.

[0101] In accordance with one embodiment of the invention, a thin RFID IC bonded onto a display backplane would

allow the cryptography, accumulation, password setup, etc. all to be done on a not too heavily altered RFID chip.

[0102] Initializing the crypto key might be done via fuses, via RFID, or a capacitive feed scheme which could use pulse trains to set the keys up one bit at a time without needing full contact. This can be shared separately if need be. Other schemes can be used.

[0103] A variety of power sources may be used to power the button **121**. For example, photoelectric cells, electrets, and/or known battery arrangements may be used.

[0104] It is noted that the device must be reliable during its life, even though it will typically live in a wallet or purse.

[0105] In accordance with one embodiment of the invention, the user authentication device **120** may include a display that has 2 parts, i.e., a 2 digit field and a longer field (which might be 6 digits long, for example). Every time the customer presses the button, the 2 digit field increments and the longer field gets a set of what look like random numbers. No two card sequences are like.

[0106] In accordance with one aspect of the invention described above, an authenticating entity may wish to insure that a transaction amount is approved by the customer. The customer may take the first few digits of the amount (the purchase amount) and use them as positions to report on the display. As described above we might have display digits representing 2 digits each and have the customer enter the displayed numbers at those positions. What gets actually transmitted is a few random digits, but they can be checked against the amount as well as the device identity, proving that someone with the same device who authenticated moments before sent an acceptance for the amount of the transaction.

[0107] The systems and methods of the invention provide a wide variety of advantages. In accord with some embodiments, the inventive device may largely eliminate phishing: there is no point in stealing things like card numbers or account numbers when the variable device is required to get money. In accord with some embodiments, the inventive device may vastly reduce phone or net fraud. This will cut both issuer and merchant losses. In accord with some embodiments, the inventive device may eliminate intra-family fraud so long as individual devices are given to each person and so long as the people don't give their patterns away. In accord with some embodiments, the inventive device may make customer data cheaper to handle because less of it will be privacy sensitive. People don't mind when their phone numbers are given out most of the time. If their card number can't be used to rob them or damage their credit, they won't care if it is given out either. In accord with some embodiments, the inventive device may cut fraud in ATMs and/or at merchants if the device is used to generate pseudo PINs which would authenticate transactions. Because the transmitted data is in effect encrypted, even cameras watching PIN pads will be useless in stealing such credentials. It is noted that most merchants have PIN pads already which could be used in implementation of the invention. In addition, the device shows the customer that his credentials are being generated securely and shows that its issuer is doing something very tangible in protecting the customer's identity. The savings to merchants are sizeable and should in addition give some merchants good incentives to prefer these devices and to give incentives to customers to use them.

[0108] Further examples of use of the user authentication device **120**, in accordance with embodiments of the invention, are set forth below.

[0109] In accordance with one embodiment of the invention, for net use, i.e., a purchase over the Internet, the customer might give his username and password. Then, the customer gives the value of the low order digits. The authentication entity then determines what the ciphertext (0:2) should be and conveys such to the customer, telling customer "if this doesn't match your display, you are talking to a fraud site. Then, if ciphertext (0:3) is OK, the authentication entity may ask the customer to enter ciphertext (3:5) and check that it is also valid. For example as used in this example, 3:5 means the digits shown in positions 3, 4 and 5.

[0110] To explain further, in an embodiment, the customer might provide half of the displayed digits to an authentication entity. Based on these provided digits, the authentication entity can then (if needed) determine where the customer is in the progression of the token. The authentication entity can then generate displayed characters (corresponding to those displayed by the customer), and the authentication entity then provides at least a portion of such displayed characters back to the customer. For example, the authentication entity might provide a portion or all of the displayed characters back to the customer. In this manner, the authentication entity knows they are dealing with a particular customer and the customer knows they are dealing with a particular authentication entity. Variations of this embodiment are of course possible regarding what portion of a character displayed is provided by what entity, e.g., what characters are provided by the customer and what characters are provided by the authentication entity.

[0111] Further, the two parties authenticating may of course perform any agreed upon transformation to the characters displayed on the token (or other device), i.e., such as providing select numbers in a particular order, or adding a 1 to each displayed number, for example, or any other suitable transformation. Accordingly, the providing of a select number of digits in a particular order is merely one transformation that might be performed.

[0112] As noted above, the authentication entity might provide a portion or all of the displayed characters back to the customer (or a transform of the displayed characters), and in this manner, the customer knows they are dealing with a particular authentication entity. Alternatively, or in addition to, the authentication entity might provide a portion or all of the next pattern, e.g., the next set of display characters, which may then be verified by the customer. The next pattern may also of course be transformed in some manner. Thus, in some agreed upon manner to authenticate, the authentication entity (or the customer) may convey to the other a portion or all of the display characters (or their equivalent such as the authentication characters **196**), some transform of the display characters, and/or a portion or all of the next set of display characters (which may also be transformed), for example.

[0113] In accordance with one aspect of the invention relating to use with credit card transactions, the issuer might offer a direct validation service to merchants. The issuer could then do as much of the authentication processing as desired. Further, it would place the issuer in a position to check passwords or take a voice sample, or perform various other authentication, as may be desired. Further, the issuer might use ciphertext(3:5) instead of CVV2 in transaction

information that was sent with the charge. It is noted the reported track **2** data may be used to capture two or so digits of low order counter in discretionary data fields. As issuer, we would recognize that the presented CVV2 was a variable one and validate accordingly, i.e., either searching the next several counter values for the customer, or using the discretionary data fields to reduce the amount of crypto to be done, e.g. reduce the need to roll ahead in search of a match.

[0114] In accordance with one embodiment of the invention, for ATM processing, the card may be inserted, and read by the ATM. The card would then be ejected and the customer enters the value of counter low digits, checks that the right ciphertext is displayed by the ATM (i.e., the display character sequence as described above), and only then enters her PIN and/or other ciphertext, as may be desired. This processing would convey the customer had some reason to think the ATM was communicating with the issuer before giving his PIN.

[0115] In accordance with one embodiment of the invention, the system uses different digits of ciphertext to authenticate to the customer that he is talking to the bank first, then to authenticate to the bank that the customer is who he claims to be. That is, the process checks that the card's identity is real. Tying the card to the customer requires asking for another password/PIN, or sampling voice, or the like. It might be that voice or a PIN recognition measures are required for higher value transactions, and not for low value ones.

[0116] For phone orders, the customer may be asked for the low digits of the counter and the ciphertext (at least one of the sets). Either a Bank authentication service could be called with this information and the card number/customer name, or the low digits could be passed in discretionary characters in Track 2 of card image data. (For time based card displays some of the ciphertext could be used as CVV2 not needing any additional data passed back.) Merchants knowing the variable number matched would be assured it would be less likely chargebacks could occur because the authentication was stronger. In one embodiment, the invention would exist on every credit card, and the only area needing change would be the issuer backend, i.e., the routine that checks CVV2. Such backend would know or compute the diversified key on the card, and track and encrypt the card counter and verify the ciphertext. Accordingly, processing change would be negligible.

[0117] In accordance with embodiments of the invention, it is appreciated that non-numeric indicia might be used along with, or in lieu of, the numerics described above, as may be desired. That is any symbol, graphic, picture, or other information representation, for example, might be used in lieu of, or along with, the numerics discussed above, as may be desired.

[0118] Further, it is appreciated that a constant value (i.e., a constant: number, symbol, graphic, picture, or other information representation, for example) might be used along with a variable value, or a set of variable values, which are described above.

[0119] As described above, FIGS. **1-4** and **10** show embodiments of structure and system of the invention. Further, FIGS. **5-10** show various steps in accordance with one embodiment of the invention. It is appreciated that the systems and methods described herein may be implemented using a variety of technologies. Hereinafter, general aspects regarding possible implementation of the systems and methods of the invention will be described.

[0120] It is understood that the system of the invention, and portions of the system of the invention, may be in the form of a "processing machine," such as a general purpose computer, for example. As used herein, the term "processing machine" is to be understood to include at least one processor that uses at least one memory. The at least one memory stores a set of instructions. The instructions may be either permanently or temporarily stored in the memory or memories of the processing machine. The processor executes the instructions that are stored in the memory or memories in order to process data. The set of instructions may include various instructions that perform a particular task or tasks, such as those tasks described above in the flowcharts. Such a set of instructions for performing a particular task may be characterized as a program, software program, or simply software.

[0121] As noted above, the processing machine executes the instructions that are stored in the memory or memories to process data. This processing of data may be in response to commands by a user or users of the processing machine, in response to previous processing, in response to a request by another processing machine and/or any other input, for example.

[0122] As noted above, the processing machine used to implement the invention may be a general purpose computer. However, the processing machine described above may also utilize any of a wide variety of other technologies including a special purpose computer, a computer system including a microcomputer, mini-computer or mainframe for example, a programmed microprocessor, a micro-controller, a peripheral integrated circuit element, a CSIC (Customer Specific Integrated Circuit) or ASIC (Application Specific Integrated Circuit) or other integrated circuit, a logic circuit, a digital signal processor, a programmable logic device such as a FPGA, PLD, PLA or PAL, or any other device or arrangement of devices that is capable of implementing the steps of the process of the invention.

[0123] It is appreciated that in order to practice the method of the invention as described above, it is not necessary that the processors and/or the memories of the processing machine be physically located in the same geographical place. That is, each of the processors and the memories used in the invention may be located in geographically distinct locations and connected so as to communicate in any suitable manner. Additionally, it is appreciated that each of the processor and/or the memory may be composed of different physical pieces of equipment. Accordingly, it is not necessary that the processor be one single piece of equipment in one location and that the memory be another single piece of equipment in another location. That is, it is contemplated that the processor may be two pieces of equipment in two different physical locations. The two distinct pieces of equipment may be connected in any suitable manner. Additionally, the memory may include two or more portions of memory in two or more physical locations.

[0124] To explain further, processing as described above is performed by various components and various memories. However, it is appreciated that the processing performed by two distinct components as described above may, in accordance with a further embodiment of the invention, be performed by a single component. Further, the processing performed by one distinct component as described above

may be performed by two distinct components. In a similar manner, the memory storage performed by two distinct memory portions as described above may, in accordance with a further embodiment of the invention, be performed by a single memory portion. Further, the memory storage performed by one distinct memory portion as described above may be performed by two memory portions.

[0125] Further, various technologies may be used to provide communication between the various processors and/or memories, as well as to allow the processors and/or the memories of the invention to communicate with any other entity; i.e., so as to obtain further instructions or to access and use remote memory stores, for example. Such technologies used to provide such communication might include a network, the Internet, intranet, Extranet, LAN, an Ethernet, or any client server system that provides communication, for example. Such communications technologies may use any suitable protocol such as TCP/IP, UDP, or OSI, for example.

[0126] As described above, a set of instructions is used in the processing of the invention. The set of instructions may be in the form of a program or software. The software may be in the form of system software or application software, for example. The software might also be in the form of a collection of separate programs, a program module within a larger program, or a portion of a program module, for example The software used might also include modular programming in the form of object oriented programming. The software tells the processing machine what to do with the data being processed.

[0127] Further, it is appreciated that the instructions or set of instructions used in the implementation and operation of the invention may be in a suitable form such that the processing machine may read the instructions. For example, the instructions that form a program may be in the form of a suitable programming language, which is converted to machine language or object code to allow the processor or processors to read the instructions. That is, written lines of programming code or source code, in a particular programming language, are converted to machine language using a compiler, assembler or interpreter. The machine language is binary coded machine instructions that are specific to a particular type of processing machine, i.e., to a particular type of computer, for example. The computer understands the machine language.

[0128] Any suitable programming language may be used in accordance with the various embodiments of the invention. Illustratively, the programming language used may include assembly language, Ada, APL, Basic, C, C++, COBOL, dBase, Forth, Fortran, Java, Modula-2, Pascal, Prolog, REXX, Visual Basic, and/or JavaScript, for example. Further, it is not necessary that a single type of instructions or single programming language be utilized in conjunction with the operation of the system and method of the invention. Rather, any number of different programming languages may be utilized as is necessary or desirable.

[0129] Also, the instructions and/or data used in the practice of the invention may utilize any compression or encryption technique or algorithm, as may be desired. An encryption module might be used to encrypt data. Further, files or other data may be decrypted using a suitable decryption module, for example.

[0130] As described above, the invention may illustratively be embodied in the form of a processing machine, including a computer or computer system, for example, that includes at least one memory. It is to be appreciated that the set of instructions, i.e., the software for example, that enables the computer operating system to perform the operations described above may be contained on any of a wide variety of media or medium, as desired. Further, the data that is processed by the set of instructions might also be contained on any of a wide variety of media or medium. That is, the particular medium, i.e., the memory in the processing machine, utilized to hold the set of instructions and/or the data used in the invention may take on any of a variety of physical forms or transmissions, for example. Illustratively, the medium may be in the form of paper, paper transparencies, a compact disk, a DVD, an integrated circuit, a hard disk, a floppy disk, an optical disk, a magnetic tape, a RAM, a ROM, a PROM, a EPROM, a wire, a cable, a fiber, communications channel, a satellite transmissions or other remote transmission, as well as any other medium or source of data that may be read by the processors of the invention.

[0131] Further, the memory or memories used in the processing machine that implements the invention may be in any of a wide variety of forms to allow the memory to hold instructions, data, or other information, as is desired. Thus, the memory might be in the form of a database to hold data. The database might use any desired arrangement of files such as a flat file arrangement or a relational database arrangement, for example.

[0132] In the system and method of the invention, a variety of "user interfaces" may be utilized to allow a user to interface with the processing machine or machines that are used to implement the invention. As used herein, a user interface includes any hardware, software, or combination of hardware and software used by the processing machine that allows a user to interact with the processing machine. A user interface may be in the form of a dialogue screen for example. A user interface may also include any of a mouse, touch screen, keyboard, voice reader, voice recognizer, dialogue screen, menu box, list, checkbox, toggle switch, a pushbutton or any other device that allows a user to receive information regarding the operation of the processing machine as it processes a set of instructions and/or provide the processing machine with information. Accordingly, the user interface is any device that provides communication between a user and a processing machine. The information provided by the user to the processing machine through the user interface may be in the form of a command, a selection of data, or some other input, for example.

[0133] As discussed above, a user interface is utilized by the processing machine that performs a set of instructions such that the processing machine processes data for a user. The user interface is typically used by the processing machine for interacting with a user either to convey information or receive information from the user. However, it should be appreciated that in accordance with some embodiments of the system and method of the invention, it is not necessary that a human user actually interact with a user interface used by the processing machine of the invention. Rather, it is contemplated that the user interface of the invention might interact, i.e., convey and receive information, with another processing machine, rather than a human user. Accordingly, the other processing machine might be characterized as a user. Further, it is contemplated that a user interface utilized in the system and method of the invention

may interact partially with another processing machine or processing machines, while also interacting partially with a human user.

[0134] It will be readily understood by those persons skilled in the art that the present invention is susceptible to broad utility and application. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and foregoing description thereof, without departing from the substance or scope of the invention.

[0135] Accordingly, while the present invention has been described here in detail in relation to its exemplary embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made to provide an enabling disclosure of the invention. Accordingly, the foregoing disclosure is not intended to be construed or to limit the present invention or otherwise to exclude any other such embodiments, adaptations, variations, modifications or equivalent arrangements.

1. A system for processing authentication information associated with a transaction effected by a user, the system comprising:

a user authentication device comprising:

a display comprising a plurality of display positions; and

a user authentication device computer processor generating a display character for each display position based on logic and a predetermined progression, and outputting the display characters to the display positions so as to be readable by the user; and

an authentication entity system comprising:

an input portion that receives an input character sequence consisting of fewer than all of the display characters displayed on the user authentication device; and

an authentication system computer processor that:

generates a set of authenticating characters based on the logic and the predetermined progression and uses a stored user-selected pattern to select fewer than all of the authenticating characters as an authorizing character sequence, the stored user-selected pattern specifying an order of the authentication characters in the authentication character sequence relative to the display positions;

compares the authorizing character sequence to the input character sequence; and

authenticates the transaction based on the comparison.

2. (canceled)

3. The authentication system of claim **1**, wherein the logic further comprises a transformation of data.

4-5. (canceled)

6. The authentication system of claim **1**, wherein the user authentication device is associated with credit card user; and the authentication entity system being maintained by a bank.

7. The authentication system of claim **6**, wherein the logic uses an algorithm to generate the plurality of display characters, the algorithm generating the plurality of display characters in a predetermined manner known to the authentication entity system.

8. The authentication system of claim **1**, wherein the user authentication device further includes a display button, and the user authentication device operable such that pressing of the display button by the user results in the display characters being displayed in the respective display positions.

9. The authentication system of claim **1**, wherein the communication channel is one selected from the group consisting of a telephone line channel, radio signal, infrared and network.

10-11. (canceled)

12. The authentication system of claim **1**, wherein each display character is a number.

13. The authentication system of claim **1**, wherein the user authentication device is in the form of a handheld token.

14. The authentication system of claim **1**, wherein the user authentication device is in the form of a program running on a computer, the computer is connected to a network.

15-38. (canceled)

39. The authentication system of claim **1**, wherein the predetermined transformation includes adding a value of 1 (one) to select characters in the display portion.

40-43. (canceled)

44. An authentication system maintained by an authentication entity that processes authentication information associated with a transaction effected by a user, the authentication system comprising:

an input portion that receives an input character sequence from a customer consisting of fewer than all of the display characters displayed by a user authentication device associated with the customer using a plurality of display positions;

a processing portion comprising at least one computer processor that generates a set of authenticating characters based on logic and users a stored user-selected pattern to select fewer than all of the authenticating characters as an authorizing character sequence, the stored user-selected pattern specifying an order of the authenticating characters in the authenticating character sequence relative to the display positions; and

a comparison portion that compares the authorizing character sequence to the input character sequence and authenticates the transaction based on the comparison;

wherein the display characters and the authenticating characters are generated using the same logic.

45. (canceled)

* * * * *