

IDENTITY OR SECURITY AUTHENTICATION DEVICE FOR ELECTRONIC SYSTEM USING VISUAL PATTERNS OR CODES

FIELD OF INVENTION

[01] My invention relates in general to methods and systems for executing electronic transactions with identity or security authentication over computer networks, and relates in particular to such methods and systems incorporating the use of mobile devices such as smartphone, tablet personal computers, and laptop computers.

BACKGROUND OF THE INVENTION

[02] Increasingly, consumers demand easier, safer, and more informative ways to pay for goods and services at a point of sale. Notwithstanding mobile device (e.g., smartphones, etc.) omnipresence, consumers generally resort to traditional payment methods such as physical currency, electronic payment cards, and the like. However, these traditional payment methods generally require consumers to carry a physical wallet, maintain an inventory of currency, etc. Additionally, such traditional payment methods raise security concerns, which often require underlying banks to reissue new cards, compensate for stolen money, etc. Stolen payment credentials highlight some of the traditional payment drawbacks, which result in losses of billions of dollars per year

[03] The used of smartphone has became so prevalent that consumers are using it to pay for common goods or services. Examples of smartphone payment or fund transfer system are "Alipay" by Alibaba Group, "WeChat Pay" by Tencent Holding, "GrabPay" by GrabTaxi Holding Pte Ltd, "LiquidPay" by Liquid Group, "PayNow" by Network for Electronic Transfers (Singapore) Pte Ltd, "PayLah!" by

DBS Bank, "Pay Anyone" by OCBC Bank and etc. In the "Alipay" and "WeChat Pay" system, both used the scanning of QR (Quick Response) code with the smartphone. QR-code is a type of matrix barcode or two-dimensional barcode that is readable by optical device like camera. Unlike the current credit-debit card system and NFC (Near Field Communication) technology, the QR-code payment system require little hardware installation. This make the QR-code payment system easy to be implemented with little cost involved. This advantage creates a way out for hackers to exploit which will be illustrated later. It is one of the objectives of my invention to close this security gap.

[04] Fig 1 shows an example of the QR-code payment system that is used commonly in China. A first pattern or QR-code pattern 104 is pasted on the glass panel of a chicken rice stall 102 that belong to a chicken rice stall owner 106. When a buyer 108 wants to purchase the product (example, a plate of chicken rice) from the stall owner 106, the buyer 108 takes out a mobile device or smartphone 202 and tap her finger on a smartphone payment application 204 shown in Fig 2. The smartphone application 204 launches and prompts the buyer 108 for a range of option shown in Fig 3. The buyer 108 tap on a transfer account button 302 and a camera function will be activated as shown in Fig 4. The buyer 108 directs her camera at the pattern 104 and aligns it to within a camera box 402 shown in Fig 4. The smartphone application 204 automatically captures the pattern 104 and transmits an image of the pattern 104 to a payment server computer 404 through wireless communication technology (Example, mobile 3G, 4G, 5G, wifi, bluetooth and etc). The payment server computer 404 authenticates the pattern 104 and transmits an authenticated result back to the smartphone 202. Upon receiving the authenticated result, the smartphone application 204 proceeds to the next

step in Fig 5. A target account name 502 indicates the target account to transfer payment, in this case "BTC chicken rice". The buyer 108 taps on a number pad 510 and the payment amount will be displayed in a transfer amount textbox 504. The buyer 108 may tap on a transfer note textbox 506 to input additional information. The buyer 108 tap on a transfer button 508 to start the payment transfer process. Upon confirmation from the payment server computer 404, a transfer confirmation notice 602 will be displayed in Fig 6. The notice 602 will indicate the date and time of the payment transfer.

- [05]** The problem with the above third party payment system is that it can be hacked by hackers. Fig 10 and Fig 11 shows an example of how hackers can take advantage of this system. Hackers will wait for night time where there are nobody around the chicken rice stall 102 to paste a hacker's QR-code pattern 1002 over the QR-code pattern 104. During the normal operating hours, the stall owner 106 may not notice the changes and continue with his normal work routine. Buyer who wants to buy from the stall owner 106 will proceed to scan the hacker's QR-code pattern 1002 as shown in Fig 12. The smartphone 202 transmits an image of the hacker's QR-code pattern 1002 to the payment server computer 404 for final confirmation shown in Fig 13. Buyer enter the transfer amount using the number pad 510 and tap on the transfer button 508 to confirm. At this point in time, the buyer may not notice that a hacker's transfer title 1302, "BTO chicken rice", shown in Fig 13 is slightly different from the correct transfer title 502, "BTC chicken rice". This process may be repeated over a long period until the stall owner 106 find the time to check his account, but it may be too late. To ensure that this problem does not occur, the stall owner 106 may need to constantly check his personal smartphone to make sure that money is transferred to his

account correctly. This action make it operational inconvenient for the stall owner 106 and slow down the buying process.

[06] Fig 20 shows another method of QR-code third party payment system. A electronic device with image scanner or QR-code scanner 2004 is placed at a bread stall 2002 that belong to a bread stall owner 2006. The QR-code scanner 2004 is used to accept payment from a buyer 2008. A QR-code scanner screen 2104 will display the necessary information as shown in Fig 21. The bread stall owner 2006 operate the scanner 2004 using a QR-code scanner keyboard 2102. In Fig 22, the buyer 2008 wants to purchase the product (example, a loaf of bread) from the bread stall owner 2006, the buyer 2008 take out the smartphone 202 and taps on the smartphone payment application 204. The smartphone application 204 launches and prompt the buyer 2008 for a range of option shown in Fig 23. The buyer 2008 taps her finger on a generate personal QR-code button 2302. The smartphone 202 communicate with the payment server computer 404 through wireless communication technology and display a personal QR-code 2404 and a personal barcode 2402 shown in Fig 24. The buyer 2008 placed the smartphone 202 with the QR-code 2404 and the personal barcode 2402 facing a QR-code scanner sensor 2502 in Fig 25. The QR-code scanner 2004 captures an image of the personal QR-code 2404 and the personal barcode 2402 and communicate with the payment server computer 404 to begin the payment transfer. The payment server computer 404 executes the order and transmits the payment order to the smartphone 202. The smartphone 202 displays a payment confirmation screen as shown in Fig 26. A target account name 2602 indicates the target account, in this case "BTC bread stall". A transfer amount textbox 2604 indicates the amount to transfer. The buyer 2008 taps on a confirm transfer

button 2606 to authorize and complete the payment.

[07] The above method of payment transfer is also prone to hacking. Hackers may create a hacker's application (Example, a game application) for buyer to download to his smartphone for free. When buyer download and launch the hacker's application, it will clone a copy of the identity information of the smartphone payment application 204. The identity information will be transmitted to hacker's smartphone or computer. Hacker make use of the identity information to purchase expensive goods or services from stalls using the process similar to Fig 20 to 26. Buyer may not notice the criminal acts until it is too late. To prevent this from happening, it may be necessary to implement a 2FA (Two factors authentication) using SMS (Short Message Service) system. But the addition of the 2FA will slow down the transaction process drastically while the buyer wait for the 2FA SMS to be transmitted to his smartphone. During peak sales period, this will adversely slow down the transaction process and affect sales. Alternatively, a password system may be implemented during the final transaction confirmation step in Fig 26. But the password can easily be stolen by hacker's trojan horse software and the buyer may forgot his or her password. It is one of the objectives of my invention to provide a secure and convenient way of payment transfer without significantly slowing down the transaction process.

[08] In many occasion, smartphone user may need to transfer money to his friends or families for various reasons. The third party mobile and online payment platform allows user to do this with his smartphone. Fig 30 illustrates the process of transferring money from the user to his friend. User taps the smartphone phone application 204 on the smartphone 202. Similarly, the user's friend taps a smartphone application 3004 on a friend's smartphone 3002. In Fig 31, user taps

on a transfer to friend button 3102 while user's friend taps on a generate personal QR-code button 3104. User direct the smartphone 202 so that an image of a personal QR-code 3202 and a personal bar code 3204 is displayed within the camera box 402 shown in Fig 32. The smartphone payment application 204 captures the image and transmits it to the payment server computer 404 for authentication. After authentication, the user will proceed to the next step shown in Fig 33. The user check a target account name 3302 to make sure that it is correct and enter the transfer amount into a transfer amount textbox 3304 using a number pad 3310. User also enter a short description of the money transfer into a transfer note textbox 3306 and tap on a transfer button 3308. The payment server computer 404 receives the transfer order and approves it. User receives a transfer acknowledgement message 3402 shown in Fig 34. At the same time, user's friend also receives a transfer acknowledgement message 3404.

- [09]** Similar to previous transfer method, the above method of transfer between friends and families is prone to hacking. Hackers may find a way to steal the identity information of the user smartphone payment application 204 and do a illegal money transfer similar to Fig 30 to 34.
- [10]** Beside payment of goods and services, consumers are increasingly using their smartphone for various activities. One of them is to make inquiry on products and services. As such, advertisers place QR-code in their outdoor advertisement so that potential customer can use their smartphone to scan and access their official website for more information or transaction. Fig 40 shows an example of outdoor advertisement at a bus stop 4002. A potential customer 4004 waiting at the bus stop 4002 notices a advertisement stand 4006. The advertisement stand 4006 depicts a "SIDA Jackson world tour concert" with a ten percent discount on ticket

price if customer use their smartphone to scan a concert QR-code 4102 as shown in Fig 41. The customer 4004 takes out the smartphone 202 and launches the smartphone payment application 204. The customer 4004 taps his finger on a scan website QR-code button 4202 shown in Fig 42 and directs the smartphone 202 so that an image of the QR-code 4102 fit into the camera box 402 as shown in Fig 43. The smartphone 202 launches an internet browser and directs it to a ticketing website URL 4402 (www.ticket.com) shown in Fig 44. URL is the acronym of Uniform Resource Locator. The customer 4004 place his order, enter his credit card information and complete the concert tickets purchase.

[11] The above method of outdoor advertisement is prone to hacking. Hackers can paste a hacker QR-code 5002 on the glass panel of the advertisement stand 4006 shown in Fig 50. When the customer 4004 try to scan the hacker QR-code 5002 in Fig 51, he may not notice the correct concert QR-code 4102 behind. This will take the customer 4004 to a hacker's website where he enters his credit card information and complete the transaction. As seen from Fig 52, the interface is nearly identical to the actual ticketing website in Fig 44. The only difference is the ticketing website URL 4402 (www.ticket.com) is slightly different from a hacker website URL 5202 (www.tiket.com).

[12] As the growth of electronic payment increases, there is a need for an authentication systems and method that provide greater and more reliable security and convenience than currently available. It is the objective of my invention to provide a convenient and more secure way of doing electronic transaction.

SUMMARY OF THE INVENTION

[13] In accordance with one embodiment, a series of authentication patterns is placed beside the QR-code pattern 104 (Fig 1). The series of authentication patterns are determined by an authentication server computer. The authentication server computer will change the orientation and order of each pattern on a regular basis and timing (Example, everyday at 7am). The food stall owner 106 (Fig 1) will be informed on the order and orientation of the authentication patterns through email, SMS (Short Message Service), voice call or a special smartphone application. Upon received of the order and orientation of the authentication patterns, the food stall owner 106 will adjust and place the authentication patterns beside the QR-code 104. The buyer 108 will scan the QR-code 104 together with the authentication pattern. The smartphone payment application 204 will capture an image of the QR-code 104 and the authentication pattern and transmit it to the payment server computer 404. The payment server computer 404 will match the authentication patterns with the authentication server computer before approving the transaction order.

BRIEF DESCRIPTION OF THE DRAWING

[14] In the drawings, closely related figures have the same number but different alphabetic suffixes.

[15] FIG 1 shows a chicken rice stall using QR-code payment system.

[16] FIG 2 shows a smartphone with a payment application icon.

[17] FIG 3 shows a smartphone payment application menu interface.

[18] FIG 4 shows a smartphone capturing an image of a QR-code pattern and communicating with a payment server computer.

- [19]** FIG 5 shows a smartphone input screen of a payment order.
- [20]** FIG 6 shows a smartphone confirmation screen of an approved payment order.
- [21]** FIG 10 shows a QR-code sticker being used by hacker.
- [22]** FIG 11 shows a hacker's QR-code sticker being pasted over an authentic QR-code.
- [23]** FIG 12 shows a smartphone capturing an image of a hacker's QR-code.
- [24]** FIG 13 shows a smartphone input screen for payment to a hacker's account.
- [25]** FIG 20 shows a bread stall using QR-code payment system.
- [26]** FIG 21 shows a QR-code scanner.
- [27]** FIG 22 shows a smartphone and a QR-code scanner.
- [28]** FIG 23 shows a payment application menu in a smartphone.
- [29]** FIG 24 shows a smartphone with a generated QR-code and barcode.
- [30]** FIG 25 shows a QR-code scanner capturing an image of a QR-code and barcode on a smartphone.
- [31]** FIG 26 shows a smartphone input screen of a payment order.
- [32]** FIG 30 shows two smartphones used in money transfer.
- [33]** FIG 31 shows a menu interface of two smartphones.
- [34]** FIG 32 shows a smartphone capturing an image of a QR-code and barcode on another smartphone.
- [35]** FIG 33 show a smartphone input screen for a money transfer.
- [36]** FIG 34 shows a money transfer confirmation notice of two smartphones.
- [37]** FIG 40 shows a bus stop with an advertisement stand.
- [38]** FIG 41 shows an advertisement poster in an advertisement stand.
- [39]** FIG 42 shows a smartphone payment application menu interface.
- [40]** FIG 43 shows a smartphone capturing an image of a QR-code of a website.

- [41]** FIG 44 shows a smartphone directed to a ticket purchasing website.
- [42]** FIG 50 shows a hacker's QR-code pasted above an authentic QR-code of an advertisement.
- [43]** FIG 51 shows a smartphone capturing an image of a hacker's QR-code of a website.
- [44]** FIG 52 shows a smartphone directed to a hacker's ticket purchasing website.
- [45]** FIG 100 shows a chicken rice stall using a QR-code payment system with a security authentication device.
- [46]** FIG 101 shows a close up view of a QR-code with a security authentication device.
- [47]** FIG 102 shows another close up view of a QR-code with a security authentication device.
- [48]** FIG 103 shows another close up view of a QR-code with a security authentication device.
- [49]** FIG 104 shows an exploded view of a security authentication device.
- [50]** FIG 105 shows an exploded back view of a security authentication device.
- [51]** FIG 106 shows a smartphone with a SMS (Short Message Service) message.
- [52]** FIG 107 shows a smartphone with detail of a SMS message which allows a user to set the patterns of a security authentication device.
- [53]** FIG 108 shows a decoding patterns for a security authentication device.
- [54]** FIG 109 shows a payment application in a smartphone.
- [55]** FIG 110 shows a payment application menu screen in a smartphone.
- [56]** FIG 111 shows a smartphone capturing an image of a QR-code and a security authentication device.
- [57]** FIG 112 shows a closer view of an image of a QR-code and a security

authentication device in a smartphone.

- [58]** FIG 113 shows a fund transfer input screen in a smartphone.
- [59]** FIG 114 shows a fund transfer confirmation notice in a smartphone.
- [60]** FIG 120 shows a noodle stall using an electronic scanner for a QR-code payment system.
- [61]** FIG 121 shows a payment application menu in a smartphone.
- [62]** FIG 122 shows a generated QR-code and barcode in a smartphone.
- [63]** FIG 123 shows the back view of a smartphone with a security authentication device attached.
- [64]** FIG 124 shows an exploded view of a security authentication device.
- [65]** FIG 125 shows another exploded view of a security authentication device.
- [66]** FIG 126 shows another exploded view of a security authentication device.
- [67]** FIG 127 shows a security authentication device being detached.
- [68]** FIG 128 shows a security authentication device being moved to the front of a smartphone.
- [69]** FIG 129 shows a security authentication device being placed on a designated location of a smartphone.
- [70]** FIG 130 shows a QR-code and a security authentication device being scanned by an electronic scanner.
- [71]** FIG 131 shows a fund transfer input screen in a smartphone.
- [72]** FIG 140 shows a user's smartphone and a friend's smartphone used in fund transfer between friends.
- [73]** FIG 141 shows a user's smartphone capturing an image of a QR-code, a barcode and a security authentication device of a friend's smartphone.
- [74]** FIG 142 shows a user's smartphone capturing an image of a personal security

authentication device.

- [75]** FIG 143 shows a fund transfer input screen of a user's smartphone.
- [76]** FIG 144 shows a fund transfer confirmation notice of a user's smartphone and a friend's smartphone.
- [77]** FIG 150 show a chat application in a smartphone.
- [78]** FIG 151 shows a chat group screen in a smartphone.
- [79]** FIG 152 shows a chat message in a smartphone.
- [80]** FIG 153 shows a chat message being selected in a smartphone.
- [81]** FIG 154 shows a smartphone capturing an image of a security authentication device.
- [82]** FIG 155 shows a fund transfer input screen of a smartphone.
- [83]** FIG 156 shows a fund transfer confirmation notice in a smartphone.
- [84]** FIG 157 shows a fund transfer confirmation message in a chat message.
- [85]** FIG 160 shows an advertisement stand with a QR-code and a security authentication device.
- [86]** FIG 161 shows a close view of a QR-code and a security authentication device.
- [87]** FIG 162 shows a close view of a security authentication device used in an advertisement stand.
- [88]** FIG 163 shows a close view of a notice in an advertisement stand.
- [89]** FIG 164 shows a smartphone capturing an image of a QR-code and a security authentication device in an advertisement stand.
- [90]** FIG 165 shows a message in a smartphone.
- [91]** FIG 166 shows a ticket purchase website in a smartphone.
- [92]** FIG 170 shows a "Geo-fencing" parking location for bicycle renting.
- [93]** FIG 171 shows a QR-code and a security authentication device used for "Geo-

fencing" of bicycle renting.

- [94]** FIG 180 shows a food vending machine using a QR-code and a security authentication device.
- [95]** FIG 181 shows a close view of a QR-code and a security authentication device used for a food vending machine.
- [96]** FIG 182 shows a payment application in a smartphone.
- [97]** FIG 183 shows a menu screen of a payment application in a smartphone.
- [98]** FIG 184 shows a SMS message in a smartphone.
- [99]** FIG 185 shows a menu screen of a payment application in a smartphone.
- [100]** FIG 186 shows a smartphone capturing an image of a personal security authentication device.
- [101]** FIG 187 shows a smartphone capturing an image of a QR-code and a security authentication device of a vending machine.
- [102]** FIG 188 shows a fund transfer input screen in a smartphone.
- [103]** FIG 200 shows a commuter entering a train station.
- [104]** FIG 201 shows a commuter standing inside a image capture area of a train station.
- [105]** FIG 202 shows a camera scanning an image of a commuter facial pattern and a security authentication device.
- [106]** FIG 203 shows a close view of a commuter and a security authentication device.
- [107]** FIG 204 shows a commuter entering a gate of a train station.
- [108]** FIG 210 shows a menu screen of a payment application in a smartphone.
- [109]** FIG 211 shows a setting menu of a payment application in a smartphone.
- [110]** FIG 212 shows a setting of a set of parameters used for a security authentication device.

[111] FIG 220 shows a summary of how the various applications are integrated with my invention.

[112] FIG 221 shows a configuration of how the various application are integrated with my invention.

[113] FIG 230 shows an embodiment of a security authentication device.

[114] FIG 231 shows an exploded view of a security authentication device.

[115] FIG 232 shows an exploded back view of a security authentication device.

[116] FIG 240 shows an embodiment of a security authentication device.

[117] FIG 241 shows a close view of a security authentication device.

[118] FIG 242 shows an exploded view of a security authentication device.

[119] FIG 243 shows an exploded back view of a security authentication device.

[120] FIG 250 shows an exploded view of a security authentication devices using structural depression to create different patterns.

[121] FIG 251 shows an exploded back view of a security authentication device using structural depression to create different patterns.

[122] FIG 260 shows an exploded view of a security authentication with additional orientation of the pattern structure.

[123] FIG 261 shows an exploded back view of a security authentication with additional orientation of the pattern structure.

DRAWINGS - Reference Numerals

102	Chicken rice stall
104	First pattern or QR-code pattern
106	Chicken rice stall owner
108	Buyer

202	Mobile device or smartphone
204	Smartphone payment application
302	Transfer account button
402	Camera box
404	Payment server computer
502	Target account name
504	Transfer amount textbox
506	Transfer note textbox
508	Transfer button
510	Number pad
602	Transfer confirmation notice
1002	Hacker's QR-code pattern
1302	Hacker's transfer title
2002	Bread stall
2004	Electronic device with image scanner or QR-code scanner
2006	Bread stall owner
2008	Buyer
2102	QR-code scanner keyboard
2104	QR-code scanner screen
2302	Generate personal QR-code button
2402	Personal barcode
2404	Personal QR-code
2502	QR-code scanner sensor
2602	Target account name
2604	Transfer amount textbox

2606	Confirm transfer button
3002	Friend's smartphone
3004	Smartphone payment application
3102	Transfer to friend button
3104	Generate personal QR-code button
3202	Personal QR-code
3204	Personal bar code
3302	Target account name
3304	Transfer amount textbox
3306	Transfer note textbox
3308	Transfer button
3310	Number pad
3402	Transfer acknowledgement message
3404	Transfer acknowledgement message
4002	Bus stop
4004	Potential customer
4006	Advertisement stand
4102	Concert QR-code
4202	Scan website QR-code button
4402	Ticketing website URL
5002	Hacker QR-code
5202	Hacker website URL
10002	Second pattern or security authentication device
10202	Padlock
10302	Adhesive tape

10402	Holder structure
10404	Piece of solid structure with pattern or one dot pattern structure
10406	Two dots pattern structure
10408	Three dots pattern structure
10410	Holder cap
10602	SMS notice
10604	Mobile device or smartphone
10702	SMS message
10902	Mobile device or smartphone
10904	Smartphone payment application
11002	Transfer to account button
11102	Camera box
11202	Start pattern
11204	End pattern
11206	First pattern
11208	Second pattern
11210	Third pattern
11302	Transfer button
11402	Transfer confirmation notice
11404	Animation pattern
12002	Noodle stall
12004	Electronic device with image scanner or QR-code scanner
12006	Noodle stall owner
12008	Buyer
12102	Smartphone

12104	Generate QR-code button
12202	Personal barcode
12204	Personal QR-code
12302	Security authentication device
12402	Adhesion layer
12404	Base structure
12406	Holding plug
12408	Holder structure
12410	Holder cap
12412	Extraction hole
12414	One dot pattern structure
12416	Two dot pattern structure
12418	Three dot pattern structure
12602	Holding hole
12802	Authentication code box
13002	QR-code scanner sensor
13102	Confirm transfer button
13104	Server computer
14002	Transfer to friends button
14004	Friend's smartphone
14006	Generate personal QR-code button
14102	Camera box
14104	QR-code
14106	Barcode
14108	Security authentication device

14202	Security authentication device
14204	Camera box
14302	Number pad
14304	Transfer button
15002	Smartphone
15004	Chat application
15102	Friends group button
15202	Chat message
15302	Select indication box
15304	Transfer fund button
15402	Security authentication device
15404	Camera box
15406	Server computer
15502	Number pad
15504	Transfer button
15602	Fund transfer confirmation notice
15702	Fund transfer message
16002	Advertisement stand
16004	Concert QR-code
16102	Security authentication device
16104	Power cable
16106	Battery pack
16202	First connector plug
16204	Second connector plug
16208	Start pattern

16210	First electronic display
16212	Second electronic display
16214	Third electronic display
16216	End pattern
16302	Security authentication notice
16402	Smartphone
16502	Security authentication message
16602	Security authentication symbol
16604	Website link
17002	Bicycle
17004	Bicycle QR-code
17006	QR-code
17008	"Geo-fencing" location
17102	Booking complete notice
17104	Security authentication device
18002	Foods vending machine
18004	Buyer
18102	Vending machine QR-code
18104	Vending machine security authentication device
18106	Purchase instruction notice
18108	Food availability display
18110	Packet of chicken rice
18202	Smartphone
18204	"Pay App2" icon
18302	Reset DA-Code button

18402	SMS message
18404	Personal security authentication device
18502	Transfer to account button
18802	Target account name
18804	Food price
18806	Add note textbox
18808	Transfer button
20002	Train station
20102	Commuter
20104	Image capture area
20106	Smartphone
20108	Camera
20110	Computer
20202	Security authentication device
20204	Image authentication notice
20402	Gate
21002	Smartphone
21004	Setting button
21102	DA-code button
21202	DA-code reset frequency list box
21204	Reset time list box
21206	Delivery method list box
23002	Security authentication device
24002	QR-Code
24004	Security authentication device

24102	Start pattern
24104	First rectangular pattern
24106	Second semicircle pattern
24108	Third triangular pattern
24110	Forth trapezoid pattern
24112	End pattern
24114	Pattern plate
24202	Main body
24206	Lock plate
24208	Padlock
24302	Plate notch
24304	Alignment holes

DETAILED DESCRIPTION OF THE INVENTION

[124] One embodiment of my invention is a second pattern or security authentication device 10002 (Also refer here as DA-Code or Daily Authentication Code) illustrated in Fig 100. The device 10002 is placed below the QR-code pattern 104 of the chicken rice stall 102 shown in Fig 101. The device 10002 can be placed at any location around the QR-code pattern 104 in any orientation. The device 10002 is secured to the glass panel using a adhesive tape 10302 and locked from tempering using a padlock 10202 shown in Fig 102 and Fig 103.

[125] Fig 104 and Fig 105 show an exploded view of the security authentication device 10002. The security authentication device 10002 comprises of a few elements. Three of these elements are make up of a piece of solid structure with pattern or one dot pattern structure 10404, a two dots pattern structure 10406 and a three

dots pattern structure 10408. The one dot pattern structure 10404 has two sides of different variation. One side of the one dot pattern structure 10404 is black dot on white background while the other side is white dot on black background. These variations is repeated for the two dots pattern structure 10406 and three dots pattern structure 10408. It is to be appreciated that various patterns (Example, square, triangle, oval, animal shape, human shape, object shape and etc.), colors and materials may be used for each of the pattern structure. The pattern structures 10404, 10406 and 10408 are inserted into a holder structure 10402 in any orientation and order. A holder cap 10410 is inserted at the end of the holder structure 10402 so that the padlock 10202 can be used to lock the security authentication device 10002.

[126] To understand the operation of the security authentication device 10002, let's take a look at the daily operation of the chicken rice stall owner 106. Every morning, the server computer 404 generates a random orientation and order of the security authentication device 10002 and transmits it to a mobile device or smartphone 10604 by SMS (Short Message Service) in Fig 106. Before the stall owner 106 start his business, he will take out the smartphone 10604 to check for a daily SMS notice 10602. The stall owner 106 taps his finger on the SMS notice 10602. The smartphone 10604 open the SMS notice 10602 to show a SMS message 10702 shown in Fig 107. The stall owner 106 unlocks the padlock 10202 to re-orientate and re-order the pattern structures 10404, 10406 and 10408 according to the SMS message 10702. The orientation of these structures is based on Fig 108. In this case, the SMS message 10702, "(1-black-dot,up-left) (3-black-dot,up-right) (2-white-dot,up)", corresponds to the patterns orientation of "#01", "#18" and "#13" in Fig 108. Fig 102 shows the final pattern order and

orientation of the security authentication device 10002. This order and orientation will be valid until the next day (7:00 am). When that happened, the order and orientation of the security authentication device 10002 will be randomly changed and another new SMS message will be transmitted to the smartphone 10604. The stall owner 106 proceed to start his business without worry of hacker infiltration. It is to be appreciated that the valid duration and time of each SMS message 10702 can be modified by the stall owner 106. For example, the stall owner 106 may operate his business from 5pm to 11pm. So he may set the change in the order and orientation of the security authentication device 10002 and SMS message 10702 to be transmitted on 4pm on a weekly basis.

[127] There are two advantages of using the SMS (Short Message Service) system. Firstly, it is a very common and reliable system of message delivery. Secondly, the SMS system is a separate smartphone application from the payment application 204. Hackers may be able to hack the payment application 204, but they will not be able to read the SMS message and proceed with the hacking methods discussed in Fig 20 to 34. This is provided that the user did not change his smartphone 202 setting to allow permission access of his SMS application to the payment application 204. This setting can be manually set in most modern day smartphone operating system (Example, Android and IOS). It is to be appreciated that my invention may use other form of message delivery system like computer generated voice call, emails or other smartphone messaging application. It may also incorporate the order and orientation change message into the payment application 204, but this may diminish its security protection.

[128] Going back to the chicken rice stall in Fig 100, the buyer 108 intends to buy a plate of chicken rice from the chicken rice stall owner 106. The buyer 108 take

out a mobile device or smartphone 10902 and tap her finger on a smartphone payment application 10904 shown in Fig 109. To pay for the plate of chicken rice, the buyer 108 tap her finger on a transfer to account button 11002 in Fig 110. The smartphone payment application 10904 activate its camera in Fig 111. The buyer 108 points her camera such that the QR-code pattern 104 and the security authentication device 10002 are inside a camera box 11102. The smartphone payment application 10904 captures an image of the QR-code pattern 104 together with the security authentication device 10002 and transmits the information to the payment server computer 404 for authentication and approval.

[129] To decode the security authentication device 10002, a pattern recognition software detect a start pattern 11202 and a end pattern 11204 shown in Fig 112. The orientation of the start pattern 11202 will be used later in the decoding process of the security authentication device 10002. All the patterns between the start pattern 11202 and the end pattern 11204 become valid patterns for authentication. In this case, a first pattern 11206, a second pattern 11208 and a third pattern 11210 become the valid patterns. These patterns will be assessed based on the orientation of the start pattern 11202 to match the order and orientation of the correct setting in the server computer 404.

[130] Referring to Fig 113, the server computer 404 verify that the QR-code pattern 104 match the security authentication device 10002 and notify the smartphone payment application 10904. The buyer 108 verify the payment transfer information and taps her finger on a transfer button 11302. A transfer confirmation notice 11402 shows the completion of the payment transfer in Fig 114. The buyer 108 shows the screen shot of the transfer confirmation notice 11402 to the chicken rice stall owner 106. The chicken rice stall owner 106

checks that the transfer confirmation notice 11402 is correct before handing over the plate of chicken rice. To increase the ease and effectiveness of this checking process, an animation pattern 11404 is shown. In this case, the animation pattern 11404 is a dancing pig. It is to be appreciated that the pattern 11404 may also be a static pattern instead of a animated one. The animation pattern 11404 may be anything that is easily identify by the chicken rice stall owner 106, example a snoring dog, a flying chicken, a jumping sheep and etc. The animation pattern 11404 will also be changed when the order and orientation of the pattern structures 10404, 10406 and 10408 in the security authentication device 10002 change.

[131] Fig 120 shows another embodiment on the application of my invention. A buyer 12008 decides to buy a bowl of noodle from a noodle stall 12002. A noodle stall owner 12006 directs the buyer 12008 to make payment using a electronic device with image scanner or QR-code scanner 12004. The buyer 12008 takes out a smartphone 12102 in Fig 121 and launch a smartphone payment application. The buyer 12008 taps her finger on a generate personal QR-code button 12104. A personal QR-code 12204 and a personal barcode 12202 is generated as shown in Fig 122. The buyer 12008 flip the smartphone 12102 over, revealing a security authentication device 12302 behind the smartphone 12102 as shown in Fig 123.

[132] Fig 124 to Fig 126 show various exploded view of my invention or the security authentication device 12302 at different angles. An adhesion layer 12402 is placed between the back of the smartphone 12102 and a base structure 12404. A holder structure 12408 and a holder cap 12410 sit on top of the base structure 12404 and secured by friction with a holding plug 12406 and a holding hole

12602 (Shown in Fig 126) on the holder cap 12410. A similar holding hole and holding plug mechanism is implemented for the holder structure 12408. A one dot pattern structure 12414, a two dot pattern structure 12416 and a three dot pattern structure 12418 are orientated and inserted into the holder structure 12408 based on a SMS message from a server computer similar to the SMS message in Fig 107. The holder cap 12410 is inserted into the end of the holder structure 12408. An extraction hole 12412 on the holder cap 12410 is used to facilitate the removal of the security authentication device 12302.

[133] Referring to Fig 127, the buyer 12008 removes the security authentication device 12302 and places it on an authentication code box 12802 shown in Fig 128 and Fig 129. While holding the security authentication device 12302 with the smartphone 12102, the buyer 12008 places it below the QR-code scanner 12004 in Fig 130. A QR-code scanner sensor 13002 captures an image of the personal QR-code 12204, the personal barcode 12202 and the security authentication device 12302. The image is transmitted to a server computer 13104 in Fig 131. The server computer 13104 authenticates the payment order and the buyer 12008 authorizes the payment transfer by tapping her finger on a confirm transfer button 13102.

[134] Fig 140 shows another embodiment on the application of my invention for the transfer of fund between friends or individuals. The user's smartphone 12102 is used in this illustration to transfer fund to a friend's smartphone 14004. The user tap on a transfer to friends button 14002 while the friend tap on a generate personal QR-code button 14006. Referring to Fig 141, the user point his smartphone camera such that an image of a QR-code 14104, a barcode 14106 and a security authentication device 14108 of the friend's smartphone 14004 are

captured within a camera box 14102. To authenticate the user identity, the user remove a security authentication device 14202 from the back of the smartphone 12102 and capture an image in a camera box 14204 shown in Fig 142. These images are captured and transmitted to the server computer 13104 for authentication. Upon authentication, the smartphone 12102 prompt the user to enter the transfer amount using a number pad 14302 and tap on a transfer button 14304 as shown in Fig 143. The final fund transfer confirmation notice is shown in Fig 144.

[135] Fig 150 to Fig 157 show another embodiment on the application of my invention used in the transfer of fund in a smartphone chat application. In Fig 150, the user tap his finger on a chat application 15004 on a smartphone 15002. This action will launch the chat application shown in Fig 151. The user tap a friends group button 15102 and the smartphone 15002 enter into a chat session shown in Fig 152. The user reads a chat message 15202 and wants to transfer fund to his friend, so he tap and hold his finger on the chat message 15202. The chat message 15202 becomes selected which is indicated by a select indication box 15302 shown in Fig 153. To transfer fund, the user tap on a transfer fund button 15304. The smartphone 15002 goes into camera mode in Fig 154. The user point the smartphone 15002 such that an image of a security authentication device 15402 is inside a camera box 15404. The smartphone 15002 captures the image and transmits it to a server computer 15406 for authentication. The security authentication device 15402 is placed on the back of the smartphone 15002 for easy access. After authentication, the smartphone 15002 proceed to prompt the user to input and confirm the amount of fund to be transferred. This is done using a number pad 15502 and tapping on a transfer button 15504 in Fig

155. Fig 156 shows a fund transfer confirmation notice 15602 and Fig 157 shows a fund transfer message 15702 in the chat application 15004. The same method of authentication shown in Fig 154 can also be used during the process of login to website account as replacement to the current 2FA (Two Factors Authentication) system using SMS (Short Message Service). Similarly, it can also be used to unlock encrypted files (example of encrypted files with file name extension of zip, 7z, bzip2, gzip, tar, wim, xz and etc.) with or without a pre-determined password.

[136] Referring to Fig 160, we now look at another embodiment on the application of my invention. A concert QR-code 16004 is place in a advertisement stand 16002 that offer discount for user who use their smartphone to scan the QR-code 16004 and purchase online. A security authentication device 16102 is place below the QR-code 16004 in Fig 161. This is to prevent hackers from hijacking the QR-code and scam users as discussed in Fig 50 to 51. The security authentication device 16102 is powered by a battery pack 16106 through a power cable 16104. Fig 162 shows a closer view of the security authentication device 16102. A start pattern 16208 and an end pattern 16216 is used for the decryption of the security authentication device 16102. A first electronic display panel 16210, a second electronic display panel 16212 and a third electronic display panel 16214 are placed between the start pattern 16208 and the end pattern 16216. These panels may be implemented using LED (Light emitting diode) technology, LCD (Liquid crystal display) technology and etc. The pattern within these electronic display panel 16210, 16212 and 16214 will change on a periodic basis that is in synchronization with an authentication server computer. A second connector plug 16204 is used for connection between the power cable 16104 and the battery

pack 16106. A first connector plug 16202 is available for a technical or maintenance team to connect to a computer for the updating of time and uploading of electronic data.

[137] Continuing from Fig 163, a security authentication notice 16302 is display above the concert QR-code 16004 reminding user to take note. In Fig 164, User take out a smartphone 16402 to capture an image of the concert QR-code 16004 together with the security authentication device 16102. Upon authentication with the server computer 15406, the smartphone 16402 display a security authentication message 16502 as shown in Fig 165. The security authentication notice 16502 assures user the validity of the concert QR-code 16004. In Fig 166, the smartphone 16402 launches an internet browser and brings the user to a correct concert website link 16604 to purchase concert tickets. A security authentication symbol 16602 is displayed beside the website link 16604 to re-assure user.

[138] We will now take a look at another embodiment on the application of my invention. In Singapore and many countries, the concept of bicycle sharing is becoming a common activities. Bicycle sharing or renting companies like "Ofo" and "Mobike" offer dockless system that users can unlock for a fee using their smartphone. After usage, users normally park the bicycle at a location of their convenient. This is creating a huge problem in term of blocking access to walk way and causing a danger to pedestrians and road users. To overcome this problem, some companies implement "Geo-fencing" to make it mandatory for bicycle users to park it a specific location after use. "Geo-fencing" is a virtual perimeter for a real-world geographic area. This can be implemented using location aware device of a location based service (LBS) when user enters or

exits a geo-fence. This method of implementation may not be cost effective. As such, my invention offer an alternative to do "Geo-fencing" without incurring high cost.

[139] Fig 170 shows the application of my invention for the purpose of "Geo-fencing" for renting of bicycle or personal mobility device. Some examples of bicycle renting in Singapore include Ofo a Beijing-based bicycle sharing company, Mobike by Beijing Mobike Technology Co Ltd, AnyWheel, SG Bike and etc. To start a bicycle renting session, a user scan a bicycle QR-code 17004 using his smartphone to unlock a bicycle 17002. When the user reaches his destination and wants to complete his booking, he will locate a "Geo-fencing" location 17008 using his smartphone with GPS (Global Positioning System) turn on. User push the bicycle 17002 to the "Geo-fencing" location 17008. After parking the bicycle, the user proceed to a QR-code 17006 near the "Geo-fencing" location 17008. In Fig 171, the user finds a booking complete notice 17102 and use his smartphone to capture an image of the QR-code 17006 together with a security authentication device 17104. The user will find it hard to circumvent this system because the patterns on the security authentication device 17104 change on a periodic basis. This change may depend on the job schedule of the bicycle sharing company's maintenance crews or done randomly.

[140] Fig 180 shows another embodiment on the application of my invention in a foods vending machine 18002. A buyer 18004 approaches the vending machine 18002 to purchase his dinner. In Fig 181, the buyer 18004 decide to purchase a packet of chicken rice 18110. The buyer 18004 can check the availability of his purchase base on a food availability display 18108. A purchase instruction notice 18106 is displayed beside a vending machine QR-code 18102 and a vending machine

security authentication device 18104. The buyer 18004 takes out a smartphone 18202 and tap on a "Pay App2" icon 18204 in Fig 182. The buyer 18004 tap on a reset DA-code button 18302 in Fig 183 to change the pattern of his personal security authentication device. This is to ensure better protection. The buyer 18004 switch to his SMS (Short Message Service) application in Fig 184. A SMS message 18402 arrives in his smartphone 18202 that indicate the new pattern and orientation of a personal security authentication device 18404. To increase the security protection level, the SMS message 18402 is schedule to automatically delete after twenty minutes. The buyer 18004 dismantle and re-assemble the security authentication device 18404 according to the SMS message 18402. The buyer 18004 is now ready to purchase food from the vending machine 18002. The buyer switch back to his "Pay App2" application and tap on a transfer to account button 18502 in Fig 185. The smartphone 18202 prompt the buyer 18004 to capture an image of the personal security authentication device 18404 to authenticate his identity as shown in Fig 186. After authentication, the buyer 18004 capture an image of the vending machine QR-Code 18102 together with the vending machine security authentication device 18104 in Fig 187. Fig 188 shows the final step in the purchase. The buyer 18004 verify a target account name 18802 tallies with the vending machine 18002, enter the value of a food price 18804, input the food code into a add note textbox 18806 and tap on a transfer button 18808. Once the information are verified and authenticated, the vending machine 18002 will proceed to heat up the correct food package and deposit it into the collection point. The buyer 18004 collect the food package and the transaction complete.

[141] Fig 200 shows another embodiment on the application of my invention in a train

station 20002. In Fig 201, a commuter 20102 approaches and stands on a image capture area 20104 and take out a smartphone 20106. A computer 20110 scan the commuter 20102 using a camera 20108. The camera 20108 capture an image of the facial pattern of the commuter 20102 and a security authentication device 20202 that is mounted on the back of the smartphone 20106. This is shown in Fig 202. The computer 20110 transmits the image to a authentication server computer and authenticates the identity of the commuter 20102. An image authentication notice 20204 on the computer 20110 shows the authentication result. Fig 203 shows a close up view of the commuter 20102 and the security authentication device 20202. In Fig 204, a gate 20402 opens and allows the commuter 20102 to enter the train station 20002 to board a train for his destination. When the commuter 20102 arrives at his destination, a similar facial recognition system together with my invention are used before he leave the train station. The cost of the commute is computed and deducted automatically from the commuter 20102 bank or financial account. It is to be appreciated that the above application of my invention can also be implemented in other security authentication sectors. These sectors include smart lock for home, offices, factories, automated clearance system for airport, door access control system for high security building, facial recognition for automotive and etc.

[142] Fig 210 to 212 illustrate some user defined settings in a smartphone 21002 that is relevant to my invention. A user taps on a setting button 21004 as shown in Fig 210. To go to the setting of my invention, the user taps on a DA-code button 21102 in Fig 211. Fig 212 shows the various setting meant for my invention. A DA-code reset frequency list box 21202 allow the user to set the criteria where the pattern orientation and order of user's security authentication device change.

The default value is daily which is a predetermined duration of twenty four hours. The user also can set it to once every two days, weekly, monthly and etc. The user may also set the reset frequency based on a transaction amount which is a predetermined amount of accumulated fund that has been transferred out. For example, the user may set the reset frequency list box 21202 to "Every \$200" so that the pattern orientation and order changes whenever two hundred dollars of the transaction amount is reached (For example, "\$200", "\$400", "\$600" and so on). A reset time list box 21204 defines the suitable time where the changes occur. In this case, the reset time is set to 7am to 8am. A security server computer will transmit its SMS or notice to the user smartphone within this period. Over time, it becomes a habit for the user to check for this SMS at this time to re-adjust his security authentication device. A delivery method list box 21206 allows the user to choose how he want to received the notice. In this case, the user choose to received the notice in SMS that will be automatically deleted after 20 minutes from the time of notice transmitted. The user may change this setting to email, computer generated voice message and etc.

[143] Fig 220 shows a summary of how the various applications are integrated with my invention. Fig 221 shows another configuration of the system where the security authentication server computer is communicated directly to the smartphones 10902 (Fig 109) and the QR-code scanner 12004 (Fig 120).

[144] Fig 230 to 232 shows another embodiment of my invention. A security authentication device 23002 is shown that is similar to Fig 103. The main difference is an increased in the number of pattern structures from three pattern structures in Fig 103 to eight pattern structures in Fig 230. This increased will significantly increased the number of possible combination and further enhanced

the security level of my invention.

[145] Another embodiment of my invention is shown in Fig 240. A security authentication device 24004 is placed below a QR-Code 24002. To decode the security authentication device 24004, the image is captured with a smartphone and transmitted to a server computer. The server computer detect a start pattern 24102 and an end pattern 24112 on a pattern plate 24114. This is to determine the location of the visual patterns used for the authentication. A first rectangular pattern 24104, a second semicircle pattern 24106, a third triangular pattern 24108 and a forth trapezoid pattern 24110 are used for the authentication process. Fig 242 shows an exploded view of the security authentication device 24004. The pattern plate 24114 is detachable from a main body 24202. The pattern plate 24114 is orientated according to a SMS (Short Message Service) message transmitted to the user's smartphone on a periodical basis. A lock plate 24206 is inserted into the main body 24202 and locked using a padlock 24208. Fig 243 shows the back view of the security authentication device 24004. A plate notch 24302 can be inserted into a number of alignment holes 24304 according to different requirement.

[146] Fig 250 and 251 show another embodiment of my invention. This embodiment is similar to Fig 104. The difference is that Fig 250 uses structural depression to create the different patterns instead of printing the pattern on the flat surface structure.

[147] Fig 260 and Fig 261 show another embodiment of my invention similar to Fig 104. The advantage of this embodiment is that it allow additional orientation of the pattern structure. This will increase the total number combination on how the patterns can be orientated and enhanced the security level.

[148] The description above is mainly using the QR-Code as an illustration. My invention can also be used for other visual pattern which include, but are not limited to, EAN13 (European/International Article Number), EAN8, CODE39, CODE93, CODE128, Data Matrix, Sticky Bits, bar codes, facial pattern, finger print pattern, palm print pattern, eye iris pattern and the like.

[149] It is of course to be understood that the embodiments described herein is merely illustrative of the principles of the invention. A wide variety of modifications thereto may be effected by persons skilled in the art without departing from the spirit and scope of my invention as set forth in the following claims.

[150] From the description above, a number of advantages of some embodiments of my invention become evident:

- (a) A simple and low cost implementation of my invention that can significantly increase the security level of the various electronic systems.
- (b) Users need to set the patterns of my invention once per day (or periodically) and security protection is ensured for that period of time. Over time, it becomes a simple habit for user to perform. This is more convenient compare to the current 2FA (Two factors authentication) system using SMS (Short message service) where the user has to wait for some time before the SMS arrive in his smartphone.
- (c) Hackers can no longer steal money from stall owner by secretly pasting their own QR-code over the original one as shown in Fig 10 to 13 and Fig 100 to 114.
- (d) Hackers who managed to clone the identity of a user's smartphone payment application can no longer used it to purchase items or services from legal business entities as shown in Fig 20 to 26 and Fig 120 to 131.

- (e) Fund transfer between friends and families become significantly secured using a third parties smartphone payment application or a smartphone chat application as shown in Fig 140 to 144 and Fig 150 to 157.
- (f) Usage of QR-code placed at public area for advertisement or vending machine become significantly secured as shown in Fig 50 to 52 and Fig 160 to 166.
- (g) A low cost method of implementation in the renting of bicycle or personal mobility device for the return of these items to predetermine location after used. This is shown in Fig 170.
- (h) Reduce the needs for facial recognition system to accurately differentiate facial pattern with high similarity (example of a person who has a twin brother or sister). This is illustrated in Fig 200 to 204. The system only need to ensure that the patterns of the security authentication device is not repeated between people with high similar facial pattern.
- (i) A nationwide centralized security authentication server computers can be implemented to monitor and authenticate the patterns of individual security authentication device. This will make it easier to for the authority to make sure that the server computers security is highly controlled and its security flaws are updated frequently. This is illustrated in Fig 220.
- (j) Users have direct control over the security of the smartphone. My invention will give the users a greater sense of security thereby encouraging them to use their smartphone for digital payments and transactions. This will help to accelerate nations into the digital frontier.

[151] CLAIMS

What is claimed is:

1. An identity or security authentication device, comprising:

- a. a first electronic device,
- b. a first pattern,
- c. a plurality of second patterns,
- d. a second electronic device, and
- e. a server computer.

whereby said server computer generates said plurality of second patterns, said server computer transmits said plurality of second patterns to said first electronic device, said second electronic device captures an image of said plurality of second patterns together with said first pattern, said second electronic device transmits said image to said server computer, said server computer authenticates said plurality of second patterns and said first pattern to create an authenticated result, and said server computer transmits said authenticated result to said second electronic device.

2. The device of claim 1, wherein said first electronic device and said second electronic device are selected from the group consisting of mobile device, smartphone, image scanner, tablet computer, desktop computer and laptop.

3. The device of claim 1, wherein said first pattern is selected from the group consisting of quick response code, barcode, EAN13, EAN8, CODE39, CODE93, CODE128, Data Matrix, Sticky Bits, iris pattern, facial pattern,

palm print pattern and finger print pattern.

4. The device of claim 1, wherein said plurality of second patterns are printed on a plurality of solid structures.
5. The device of claim 1, wherein said plurality of second patterns consist of a start pattern, follow by a plurality of patterns and complete with an end pattern.
6. The device of claim 1, wherein said server computer generates said plurality of second patterns after a predetermined time duration has lapsed.
7. The device of claim 1, wherein said server computer generates said plurality of second patterns after a predetermined fund transfer amount has exceeded.
8. An identity or security authentication device, comprising:
 - a. a electronic device,
 - b. a plurality of patterns, and
 - c. a server computer.

whereby said server computer generates said plurality of patterns, said server computer transmits said plurality of patterns to said electronic device, said electronic device captures an image of said plurality of patterns, said electronic device transmits said image to said server computer, said server

computer authenticates said plurality of patterns to create an authenticated result, and said server computer transmits said authenticated result to said electronic device.

9. The device of claim 8, wherein said electronic device is selected from the group consisting of mobile device, smartphone, image scanner, tablet computer, desktop computer and laptop.
10. The device of claim 8, wherein said plurality of patterns are printed on a plurality of solid structures.
11. The device of claim 8, wherein said plurality of patterns consist of a start pattern, follow by a plurality of patterns and complete with an end pattern.
12. The device of claim 8, wherein said server computer generates said plurality of patterns after a predetermined time duration has lapsed.
13. The device of claim 8, wherein said server computer generates said plurality of patterns after a predetermined fund transfer amount has exceeded.
14. A method of identity or security authentication, comprising:
 - a. generating a plurality of second patterns,
 - b. transmitting said second patterns,
 - c. receiving said plurality of second patterns on a first electronic device,

- d. providing a first pattern,
 - e. capturing an image of said plurality of second patterns together with said first pattern on a second electronic device,
 - f. transmitting said image to a server computer,
 - g. authenticating said image in said server computer to create an authentication result, and
 - h. transmitting said authentication result to said second electronic device.
15. The method of claim 14, wherein said printing of said plurality of second patterns is done on a plurality of solid structures.
16. The method claim 14, wherein said generating of said plurality of second patterns is repeated after a predetermined time duration has lapsed.
17. The method claim 14, wherein said generating of said plurality of second patterns is repeated after a predetermined fund transfer amount has exceeded.
18. A method of identity or security authentication, comprising:
- a. generating a plurality of patterns,
 - b. transmitting said patterns,
 - c. receiving said plurality of patterns on an electronic device,
 - d. capturing an image of said plurality of patterns using said electronic device,
 - e. transmitting said image to a server computer,

- f. authenticating said image in said server computer to create an authentication result, and
 - g. transmitting said authentication result to said electronic device.
19. The method of claim 18, wherein said printing of said plurality of pattern is done on a plurality of solid structures.
20. The method of claim 18, wherein said generating of said plurality of patterns is repeated after a predetermined time duration has lapsed.