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 7 and Fig 8 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 702 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 702 as shown in Fig 9. The smartphone 202 transmits an image of the hacker's QR-code pattern 702 to the payment server computer 404 for final confirmation shown in Fig 10. 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 1002, "BTO chicken rice", shown in Fig 10 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 11 shows another method of QR-code third party payment system. A electronic device with image scanner or QR-code scanner 1104 is placed at a bread stall 1102 that belong to a bread stall owner 1106. The QR-code scanner 1104 is used to accept payment from a buyer 1108. A QR-code scanner screen 1204 will display the necessary information as shown in Fig 12. The bread stall owner 1106 operate the scanner 1104 using a QR-code scanner keyboard 1202. In Fig 13, the buyer 1108 wants to purchase the product (example, a loaf of bread) from the bread stall owner 1106, the buyer 1108 take out the smartphone 202 and taps on the smartphone payment application 204. The smartphone application 204 launches and prompt the buyer 1108 for a range of option shown in Fig 14. The buyer 1108 taps her finger on a generate personal QR-code button 1402. The smartphone 202 communicate with the payment server computer 404 through wireless communication technology and display a personal QR-code 1504 and a personal barcode 1502 shown in Fig 15. The buyer 1108 placed the smartphone 202 with the QR-code 1504 and the personal barcode 1502 facing a QR-code scanner sensor 1602 in Fig 16. The QR-code scanner 1104 captures an image of the personal QR-code 1504 and the personal barcode 1502 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 17. A target account name 1702 indicates the target account, in this case "BTC bread stall". A transfer amount textbox 1704 indicates the amount to transfer. The buyer 1108 taps on a confirm transfer

button 1706 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 11 to Fig 17. 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 17. 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 18 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 1804 on a friend's smartphone 1802. In Fig 19, user taps

on a transfer to friend button 1902 while user's friend taps on a generate personal QR-code button 1904. User direct the smartphone 202 so that an image of a personal QR-code 2002 and a personal bar code 2004 is displayed within the camera box 402 shown in Fig 20. 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 21. The user check a target account name 2102 to make sure that it is correct and enter the transfer amount into a transfer amount textbox 2104 using a number pad 2110. User also enter a short description of the money transfer into a transfer note textbox 2106 and tap on a transfer button 2108. The payment server computer 404 receives the transfer order and approves it. User receives a transfer acknowledgement message 2202 shown in Fig 22. At the same time, user's friend also receives a transfer acknowledgement message 2204.

[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 18 to Fig 22.

[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 23 shows an example of outdoor advertisement at a bus stop 2302. A potential customer 2304 waiting at the bus stop 2302 notices a advertisement stand 2306. The advertisement stand 2306 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 2402 as shown in Fig 24. The customer 2304 takes out the smartphone 202 and launches the smartphone payment application 204. The customer 2304 taps his finger on a scan website QR-code button 2502 shown in Fig 25 and directs the smartphone 202 so that an image of the QR-code 2402 fit into the camera box 402 as shown in Fig 26. The smartphone 202 launches an internet browser and directs it to a ticketing website URL 2702 (www.ticket.com) shown in Fig 27. URL is the acronym of Uniform Resource Locator. The customer 2304 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 2802 on the glass panel of the advertisement stand 2306 shown in Fig 28. When the customer 2304 try to scan the hacker QR-code 2802 in Fig 29, he may not notice the correct concert QR-code 2402 behind. This will take the customer 2304 to a hacker's website where he enters his credit card information and complete the transaction. As seen from Fig 30, the interface is nearly identical to the actual ticketing website in Fig 27. The only difference is the ticketing website URL 2702 (www.ticket.com) is slightly different from a hacker website URL 3002 (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.

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

FIG 2 shows a smartphone with a payment application icon.

FIG 3 shows a smartphone payment application menu interface.

FIG 4 shows a smartphone capturing an image of a QR-code pattern and

communicating with a payment server computer.

FIG 5 shows a smartphone input screen of a payment order.

FIG 6 shows a smartphone confirmation screen of an approved payment order.

FIG 7 shows a QR-code sticker being used by hacker.

FIG 8 shows a hacker's QR-code sticker being pasted over an authentic QR-code.

FIG 9 shows a smartphone capturing an image of a hacker's QR-code.

FIG 10 shows a smartphone input screen for payment to a hacker's account.

FIG 11 shows a bread stall using QR-code payment system.

FIG 12 shows a QR-code scanner.

FIG 13 shows a smartphone and a QR-code scanner.

FIG 14 shows a payment application menu in a smartphone.

FIG 15 shows a smartphone with a generated QR-code and barcode.

FIG 16 shows a QR-code scanner capturing an image of a QR-code and barcode on a smartphone.

FIG 17 shows a smartphone input screen of a payment order.

FIG 18 shows two smartphones used in money transfer.

FIG 19 shows a menu interface of two smartphones.

FIG 20 shows a smartphone capturing an image of a QR-code and barcode on another smartphone.

FIG 21 show a smartphone input screen for a money transfer.

FIG 22 shows a money transfer confirmation notice of two smartphones.

FIG 23 shows a bus stop with an advertisement stand.

FIG 24 shows an advertisement poster in an advertisement stand.

FIG 25 shows a smartphone payment application menu interface.

FIG 26 shows a smartphone capturing an image of a QR-code of a website.

FIG 27 shows a smartphone directed to a ticket purchasing website.

FIG 28 shows a hacker's QR-code pasted above an authentic QR-code of an advertisement.

FIG 29 shows a smartphone capturing an image of a hacker's QR-code of a website.

FIG 30 shows a smartphone directed to a hacker's ticket purchasing website.

FIG 31 shows a chicken rice stall using a QR-code payment system with a security authentication device.

FIG 32 shows a close up view of a QR-code with a security authentication device.

FIG 33 shows another close up view of a QR-code with a security authentication device.

FIG 34 shows another close up view of a QR-code with a security authentication device.

FIG 35 shows an exploded view of a security authentication device.

FIG 36 shows an exploded back view of a security authentication device.

FIG 37 shows a smartphone with a SMS (Short Message Service) message.

FIG 38 shows a smartphone with detail of a SMS message which allows a user to set the patterns of a security authentication device.

FIG 39 shows a decoding patterns for a security authentication device.

FIG 40 shows a payment application in a smartphone.

FIG 41 shows a payment application menu screen in a smartphone.

FIG 42 shows a smartphone capturing an image of a QR-code and a security authentication device.

FIG 43 shows a closer view of an image of a QR-code and a security authentication device in a smartphone.

FIG 44 shows a fund transfer input screen in a smartphone.

FIG 45 shows a fund transfer confirmation notice in a smartphone.

FIG 46 shows a noodle stall using an electronic scanner for a QR-code payment

system.

FIG 47 shows a payment application menu in a smartphone.

FIG 48 shows a generated QR-code and barcode in a smartphone.

FIG 49 shows the back view of a smartphone with a security authentication device attached.

FIG 50 shows an exploded view of a security authentication device.

FIG 51 shows another exploded view of a security authentication device.

FIG 52 shows another exploded view of a security authentication device.

FIG 53 shows a security authentication device being detached.

FIG 54 shows a security authentication device being moved to the front of a smartphone.

FIG 55 shows a security authentication device being placed on a designated location of a smartphone.

FIG 56 shows a QR-code and a security authentication device being scanned by an electronic scanner.

FIG 57 shows a fund transfer input screen in a smartphone.

FIG 57A shows a QR-code being scanned by an electronic scanner.

FIG 57B shows a security authentication device being scanned by an electronic scanner.

FIG 58 shows a user's smartphone and a friend's smartphone used in fund transfer between friends.

FIG 59 shows a user's smartphone capturing an image of a QR-code, a barcode and a security authentication device of a friend's smartphone.

FIG 60 shows a user's smartphone capturing an image of a personal security authentication device.

FIG 61 shows a fund transfer input screen of a user's smartphone.

FIG 62 shows a fund transfer confirmation notice of a user's smartphone and a friend's smartphone.

FIG 62A shows a user's smartphone capturing an image of a QR-code and a barcode of a friend's smartphone.

FIG 62B shows a user's smartphone capturing an image of a security authentication device of a friend's smartphone.

FIG 62C shows a user's smartphone capturing an image of a personal security authentication device.

FIG 62D shows a fund transfer input screen of a user's smartphone.

FIG 62E shows a fund transfer confirmation notice of a user's smartphone and a friend's smartphone.

FIG 63 show a chat application in a smartphone.

FIG 64 shows a chat group screen in a smartphone.

FIG 65 shows a chat message in a smartphone.

FIG 66 shows a chat message being selected in a smartphone.

FIG 67 shows a smartphone capturing an image of a security authentication device.

FIG 68 shows a fund transfer input screen of a smartphone.

FIG 69 shows a fund transfer confirmation notice in a smartphone.

FIG 70 shows a fund transfer confirmation message in a chat message.

FIG 71 shows an advertisement stand with a QR-code and a security authentication device.

FIG 72 shows a close view of a QR-code and a security authentication device.

FIG 73 shows a close view of a security authentication device used in an advertisement stand.

FIG 74 shows a close view of a notice in an advertisement stand.

FIG 75 shows a smartphone capturing an image of a QR-code and a security authentication device in an advertisement stand.

FIG 76 shows a message in a smartphone.

FIG 77 shows a ticket purchase website in a smartphone.

FIG 78 shows a "Geo-fencing" parking location for bicycle renting.

FIG 79 shows a QR-code and a security authentication device used for "Geo-fencing" of bicycle renting.

FIG 80 shows a food vending machine using a QR-code and a security authentication device.

FIG 81 shows a close view of a QR-code and a security authentication device used for a food vending machine.

FIG 82 shows a payment application in a smartphone.

FIG 83 shows a menu screen of a payment application in a smartphone.

FIG 84 shows a SMS message in a smartphone.

FIG 85 shows a menu screen of a payment application in a smartphone.

FIG 86 shows a smartphone capturing an image of a personal security authentication device.

FIG 87 shows a smartphone capturing an image of a QR-code and a security authentication device of a vending machine.

FIG 88 shows a fund transfer input screen in a smartphone.

FIG 89 shows a commuter entering a train station.

FIG 90 shows a commuter standing inside a image capture area of a train station.

FIG 91 shows a camera scanning an image of a commuter facial pattern and a security authentication device.

FIG 92 shows a close view of a commuter and a security authentication device.

FIG 93 shows a commuter entering a gate of a train station.

FIG 94 shows a menu screen of a payment application in a smartphone.

FIG 95 shows a setting menu of a payment application in a smartphone.

FIG 96 shows a setting of a set of parameters used for a security authentication device.

FIG 97 shows a summary of how the various applications are integrated with my invention.

FIG 98 shows a configuration of how the various application are integrated with my invention.

FIG 99 shows an embodiment of a security authentication device.

FIG 100 shows an exploded view of a security authentication device.

FIG 101 shows an exploded back view of a security authentication device.

FIG 102 shows an embodiment of a security authentication device.

FIG 103 shows a close view of a security authentication device.

FIG 104 shows an exploded view of a security authentication device.

FIG 105 shows an exploded back view of a security authentication device.

FIG 106 shows an exploded view of a security authentication devices using structural depression to create different patterns.

FIG 107 shows an exploded back view of a security authentication device using structural depression to create different patterns.

FIG 108 shows an exploded view of a security authentication with additional orientation of the pattern structure.

FIG 109 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
702	Hacker's QR-code pattern
1002	Hacker's transfer title
1102	Bread stall
1104	Electronic device with image scanner or QR-code scanner
1106	Bread stall owner
1108	Buyer
1202	QR-code scanner keyboard
1204	QR-code scanner screen
1402	Generate personal QR-code button

1502	Personal barcode
1504	Personal QR-code
1602	QR-code scanner sensor
1702	Target account name
1704	Transfer amount textbox
1706	Confirm transfer button
1802	Friend's smartphone
1804	Smartphone payment application
1902	Transfer to friend button
1904	Generate personal QR-code button
2002	Personal QR-code
2004	Personal bar code
2102	Target account name
2104	Transfer amount textbox
2106	Transfer note textbox
2108	Transfer button
2110	Number pad
2202	Transfer acknowledgement message
2204	Transfer acknowledgement message
2302	Bus stop
2304	Potential customer
2306	Advertisement stand
2402	Concert QR-code
2502	Scan website QR-code button
2702	Ticketing website URL

2802	Hacker QR-code
3002	Hacker website URL
3102	Second pattern or security authentication device
3302	Padlock
3402	Adhesive tape
3502	Holder structure
3504	Piece of solid structure with pattern or one dot pattern structure
3506	Two dots pattern structure
3508	Three dots pattern structure
3510	Holder cap
3702	SMS notice
3704	Mobile device or smartphone
3802	SMS message
4002	Mobile device or smartphone
4004	Smartphone payment application
4102	Transfer to account button
4202	Camera box
4302	Start pattern
4304	End pattern
4306	First pattern
4308	Second pattern
4310	Third pattern
4402	Transfer button
4502	Transfer confirmation notice
4504	Animation pattern

4602	Noodle stall
4604	Electronic device with image scanner or QR-code scanner
4606	Noodle stall owner
4608	Buyer
4702	Smartphone
4704	Generate QR-code button
4802	Personal barcode
4804	Personal QR-code
4902	Security authentication device
5002	Adhesion layer
5004	Base structure
5006	Holding plug
5008	Holder structure
5010	Holder cap
5012	Extraction hole
5014	One dot pattern structure
5016	Two dot pattern structure
5018	Three dot pattern structure
5202	Holding hole
5402	Authentication code box
5602	QR-code scanner sensor
5702	Confirm transfer button
5704	Server computer
5802	Transfer to friends button
5804	Friend's smartphone

5806	Generate personal QR-code button
5902	Camera box
5904	QR-code
5906	Barcode
5908	Security authentication device
6002	Security authentication device
6004	Camera box
6102	Number pad
6104	Transfer button
6302	Smartphone
6304	Chat application
6402	Friends group button
6502	Chat message
6602	Select indication box
6604	Transfer fund button
6702	Security authentication device
6704	Camera box
6706	Server computer
6802	Number pad
6804	Transfer button
6902	Fund transfer confirmation notice
7002	Fund transfer message
7102	Advertisement stand
7104	Concert QR-code
7202	Security authentication device

7204	Power cable
7206	Battery pack
7302	First connector plug
7304	Second connector plug
7308	Start pattern
7310	First electronic display
7312	Second electronic display
7314	Third electronic display
7316	End pattern
7402	Security authentication notice
7502	Smartphone
7602	Security authentication message
7702	Security authentication symbol
7704	Website link
7802	Bicycle
7804	Bicycle QR-code
7806	QR-code
7808	"Geo-fencing" location
7902	Booking complete notice
7904	Security authentication device
8002	Foods vending machine
8004	Buyer
8102	Vending machine QR-code
8104	Vending machine security authentication device
8106	Purchase instruction notice

8108	Food availability display
8110	Packet of chicken rice
8202	Smartphone
8204	"Pay App2" icon
8302	Reset DA-Code button
8402	SMS message
8404	Personal security authentication device
8502	Transfer to account button
8802	Target account name
8804	Food price
8806	Add note textbox
8808	Transfer button
8902	Train station
9002	Commuter
9004	Image capture area
9006	Smartphone
9008	Camera
9010	Computer
9102	Security authentication device
9104	Image authentication notice
9302	Gate
9402	Smartphone
9404	Setting button
9502	DA-code button
9602	DA-code reset frequency list box

9604	Reset time list box
9606	Delivery method list box
9702	Food stall with QR-code
9704	Food stall with QR-code scanner
9706	Friend to friend fund transfer
9708	Advertiser web server Computer
9710	Third Party Payment Server Computer
9712	Fund transfer through chat group
9714	Security Authentication Server Computer
9716	Train server computer
9718	Advertisement stand website access
9720	Bicycle renting server computer
9722	Vending machine server computer
9724	Train security and payment
9726	Bicycle renting Geo-Fencing
9728	Vending machine payment
9802	SMS System
9804	Email System
9902	Security authentication device
10202	QR-Code
10204	Security authentication device
10302	Start pattern
10304	First rectangular pattern
10306	Second semicircle pattern
10308	Third triangular pattern

10310 Forth trapezoid pattern

10312 End pattern

10314 Pattern plate

10402 Main body

10406 Lock plate

10408 Padlock

10502 Plate notch

10504 Alignment holes

DETAILED DESCRIPTION OF THE INVENTION

[15] One embodiment of my invention is a second pattern or security authentication device 3102 (Also refer here as DA-Code or Daily Authentication Code) illustrated in Fig 31. The device 3102 is placed below the QR-code pattern 104 of the chicken rice stall 102 shown in Fig 32. The device 3102 can be placed at any location around the QR-code pattern 104 in any orientation. The device 3102 is secured to the glass panel using a adhesive tape 3402 and locked from tempering using a padlock 3302 shown in Fig 33 and Fig 34.

[16] Fig 35 and Fig 36 show an exploded view of the security authentication device 3102. The security authentication device 3102 comprises of a few elements. Three of these elements are make up of a piece of solid structure with coding pattern or one dot pattern structure 3504, a two dots pattern structure 3506 and a three dots pattern structure 3508. The one dot pattern structure 3504 has two sides of different variation. One side of the one dot pattern structure 3504 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 3506 and three

dots pattern structure 3508. 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 3504, 3506 and 3508 are inserted into a holder structure 3502 in any orientation and order. A holder cap 3510 is inserted at the end of the holder structure 3502 so that the padlock 3302 can be used to lock the security authentication device 3102.

[17] To understand the operation of the security authentication device 3102, 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 3102 and transmits it to a mobile device or smartphone 3704 by SMS (Short Message Service) in Fig 37. Before the stall owner 106 start his business, he will take out the smartphone 3704 to check for a daily SMS notice 3702. The stall owner 106 taps his finger on the SMS notice 3702. The smartphone 3704 open the SMS notice 3702 to show a SMS message 3802 shown in Fig 38. The stall owner 106 unlocks the padlock 3302 to re-orientate and re-order the pattern structures 3504, 3506 and 3508 according to the SMS message 3802. The orientation of these structures is based on Fig 39. In this case, the SMS message 3802, "(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 39. Fig 33 shows the final pattern order and orientation of the security authentication device 3102. 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 3102 will be randomly changed and another new SMS message will be transmitted to the smartphone 3704. 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 3802 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 3102 and SMS message 3802 to be transmitted on 4pm on a weekly basis.

[18] 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 11 to 22. 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.

[19] Going back to the chicken rice stall in Fig 31, 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 4002 and tap her finger on a smartphone payment application 4004 shown in Fig 40. To pay for the plate of chicken rice, the buyer 108 tap her finger on a transfer to account button 4102 in Fig 41. The smartphone payment application 4004 activate its camera in Fig 42. The buyer

108 points her camera such that the QR-code pattern 104 and the security authentication device 3102 are inside a camera box 4202. The smartphone payment application 4004 captures an image of the QR-code pattern 104 together with the security authentication device 3102 and transmits the information to the payment server computer 404 for authentication and approval.

[20] To decode the security authentication device 3102, a pattern recognition software detect a start pattern 4302 and a end pattern 4304 shown in Fig 43. The orientation of the start pattern 4302 will be used later in the decoding process of the security authentication device 3102. All the patterns between the start pattern 4302 and the end pattern 4304 become valid patterns for authentication. In this case, a first pattern 4306, a second pattern 4308 and a third pattern 4310 become the valid patterns. These patterns will be assessed based on the orientation of the start pattern 4302 to match the order and orientation of the correct setting in the server computer 404.

[21] Referring to Fig 44, the server computer 404 verify that the QR-code pattern 104 match the security authentication device 3102 and notify the smartphone payment application 4004. The buyer 108 verify the payment transfer information and taps her finger on a transfer button 4402. A transfer confirmation notice 4502 shows the completion of the payment transfer in Fig 45. The buyer 108 shows the screen shot of the transfer confirmation notice 4502 to the chicken rice stall owner 106. The chicken rice stall owner 106 checks that the transfer confirmation notice 4502 is correct before handling over the plate of chicken rice. To increase the ease and effectiveness of this checking process, an animation pattern 4504 is shown. In this case, the animation pattern 4504 is a dancing pig. It is to be appreciated that the pattern 4504 may also be a static pattern instead of a

animated one. The animation pattern 4504 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 4504 will also be changed when the order and orientation of the pattern structures 3504, 3506 and 3508 in the security authentication device 3102 change.

[22] Fig 46 shows another embodiment on the application of my invention. A buyer 4608 decides to buy a bowl of noodle from a noodle stall 4602. A noodle stall owner 4606 directs the buyer 4608 to make payment using a electronic device with image scanner or QR-code scanner 4604. The buyer 4608 takes out a smartphone 4702 in Fig 47 and launch a smartphone payment application. The buyer 4608 taps her finger on a generate personal QR-code button 4704. A personal QR-code 4804 and a personal barcode 4802 is generated as shown in Fig 48. The buyer 4608 flip the smartphone 4702 over, revealing a security authentication device 4902 behind the smartphone 4702 as shown in Fig 49.

[23] Fig 50 to Fig 52 show various exploded view of my invention or the security authentication device 4902 at different angles. An adhesion layer 5002 is placed between the back of the smartphone 4702 and a base structure 5004. A holder structure 5008 and a holder cap 5010 sit on top of the base structure 5004 and secured by friction with a holding plug 5006 and a holding hole 5202 (Shown in Fig 52) on the holder cap 5010. A similar holding hole and holding plug mechanism is implemented for the holder structure 5008. A one dot pattern structure 5014, a two dot pattern structure 5016 and a three dot pattern structure 5018 are orientated and inserted into the holder structure 5008 based on a SMS message from a server computer similar to the SMS message in Fig 38. The holder cap 5010 is inserted into the end of the holder structure 5008. An

extraction hole 5012 on the holder cap 5010 is used to facilitate the removal of the security authentication device 4902.

[24] Referring to Fig 53, the buyer 4608 removes the security authentication device 4902 and places it on an authentication code box 5402 shown in Fig 54 and Fig 55. While holding the security authentication device 4902 with the smartphone 4702, the buyer 4608 places it below the QR-code scanner 4604 in Fig 56. A QR-code scanner sensor 5602 captures an image of the personal QR-code 4804, the personal barcode 4802 and the security authentication device 4902. The image is transmitted to a server computer 5704 in Fig 57. The server computer 5704 authenticates the payment order and the buyer 4608 authorizes the payment transfer by tapping her finger on a confirm transfer button 5702.

[25] Beside the method of payment transfer shown in Fig 53 to Fig 57, the image capturing process of the QR-code scanner sensor 5602 can be splitted up into two steps. The first step shown in Fig 57A is done by placing the smartphone 4702 below the QR-code scanner 4604. The QR-code scanner sensor 5602 captures an image of the personal QR-code 4804 and the personal barcode 4802. A audible beep sound is activated to alert the buyer 4608 to proceed to the second step. In the second step shown in Fig 57B, the smartphone 4702 is flipped over so that an image of the security authentication device 4902 is captured by the QR-code scanner sensor 5602. A second audible beep sound is activated to inform the buyer 4608 of a successful scan. A similar authentication process to Fig 57 proceed to complete the payment transfer.

[26] Fig 58 shows another embodiment on the application of my invention for the transfer of fund between friends or individuals. The user's smartphone 4702 is used in this illustration to transfer fund to a friend's smartphone 5804. The user

tap on a transfer to friends button 5802 while the friend tap on a generate personal QR-code button 5806. Referring to Fig 59, the user point his smartphone camera such that an image of a QR-code 5904, a barcode 5906 and a security authentication device 5908 of the friend's smartphone 5804 are captured within a camera box 5902. To authenticate the user identity, the user remove a security authentication device 6002 from the back of the smartphone 4702 and capture an image in a camera box 6004 shown in Fig 60. These images are captured and transmitted to the server computer 5704 for authentication. Upon authentication, the smartphone 4702 prompt the user to enter the transfer amount using a number pad 6102 and tap on a transfer button 6104 as shown in Fig 61. The final fund transfer confirmation notice is shown in Fig 62.

[27] Fig 62A to Fig 62E shows another method of fund transfer between friends or individual similar to Fig 58 to Fig 62. Similar to Fig 59, the scanning of the QR-code 5904, the barcode 5906 and the security authentication device 5908 is divided into two steps. The first step is shown in Fig 62A where the user's smartphone 4702 captures an image of the friend's QR-code 5904 and barcode 5906. The second step is shown in Fig 62B where the user's smartphone 4702 captures another image of the friend's security authentication device 5908. To authenticate the user identity, the user remove a security authentication device 6002 from the back of the smartphone 4702 and capture an image in a camera box 6004 shown in Fig 62C. Upon authentication, the smartphone 4702 prompt the user to enter the transfer amount using a number pad 6102 and tap on a transfer button 6104 as shown in Fig 62D. The final fund transfer confirmation notice is shown in Fig 62E.

[28] Fig 63 to Fig 70 show another embodiment on the application of my invention used in the transfer of fund in a smartphone chat application. In Fig 63, the user tap his finger on a chat application 6304 on a smartphone 6302. This action will launch the chat application shown in Fig 64. The user tap a friends group button 6402 and the smartphone 6302 enter into a chat session shown in Fig 65. The user reads a chat message 6502 and wants to transfer fund to his friend, so he tap and hold his finger on the chat message 6502. The chat message 6502 becomes selected which is indicated by a select indication box 6602 shown in Fig 66. To transfer fund, the user tap on a transfer fund button 6604. The smartphone 6302 goes into camera mode in Fig 67. The user point the smartphone 6302 such that an image of a security authentication device 6702 is inside a camera box 6704. The smartphone 6302 captures the image and transmits it to a server computer 6706 for authentication. The security authentication device 6702 is placed on the back of the smartphone 6302 for easy access. After authentication, the smartphone 6302 proceed to prompt the user to input and confirm the amount of fund to be transferred. This is done using a number pad 6802 and tapping on a transfer button 6804 in Fig 68. Fig 69 shows a fund transfer confirmation notice 6902 and Fig 70 shows a fund transfer message 7002 in the chat application 6304. The same method of authentication shown in Fig 67 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.

[29] Referring to Fig 71, we now look at another embodiment on the application of my

invention. A concert QR-code 7104 is place in a advertisement stand 7102 that offer discount for user who use their smartphone to scan the QR-code 7104 and purchase online. A security authentication device 7202 is place below the QR-code 7104 in Fig 72. This is to prevent hackers from hijacking the QR-code and scam users as discussed in Fig 28 to Fig 29. The security authentication device 7202 is powered by a battery pack 7206 through a power cable 7204. Fig 73 shows a closer view of the security authentication device 7202. A start pattern 7308 and an end pattern 7316 is used for the decryption of the security authentication device 7202. A first electronic display panel 7310, a second electronic display panel 7312 and a third electronic display panel 7314 are placed between the start pattern 7308 and the end pattern 7316. 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 7310, 7312 and 7314 will change on a periodic basis that is in synchronization with an authentication server computer. A second connector plug 7304 is used for connection between the power cable 7204 and the battery pack 7206. A first connector plug 7302 is available for a technical or maintenance team to connect to a computer for the updating of time and uploading of electronic data.

[30] Continuing from Fig 74, a security authentication notice 7402 is display above the concert QR-code 7104 reminding user to take note. In Fig 75, User take out a smartphone 7502 to capture an image of the concert QR-code 7104 together with the security authentication device 7202. Upon authentication with the server computer 6706, the smartphone 7502 display a security authentication message 7602 as shown in Fig 76. The security authentication notice 7602 assures user the validity of the concert QR-code 7104. In Fig 77, the smartphone 7502

launches an internet browser and brings the user to a correct concert website link 7704 to purchase concert tickets. A security authentication symbol 7702 is displayed beside the website link 7704 to re-assure user.

[31] 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 at 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.

[32] Fig 78 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 7804 using his smartphone to unlock a bicycle 7802. When the user reaches his destination and wants to complete his booking, he will locate a "Geo-fencing" location 7808 using his smartphone with GPS (Global Positioning System) turn on. User push the bicycle 7802 to the "Geo-fencing" location 7808. After parking the bicycle, the

user proceed to a QR-code 7806 near the "Geo-fencing" location 7808. In Fig 79, the user finds a booking complete notice 7902 and use his smartphone to capture an image of the QR-code 7806 together with a security authentication device 7904. The user will find it hard to circumvent this system because the patterns on the security authentication device 7904 change on a periodic basis. This change may depend on the job schedule of the bicycle sharing company's maintenance crews or done randomly.

[33] Fig 80 shows another embodiment on the application of my invention in a foods vending machine 8002. A buyer 8004 approaches the vending machine 8002 to purchase his dinner. In Fig 81, the buyer 8004 decide to purchase a packet of chicken rice 8110. The buyer 8004 can check the availability of his purchase base on a food availability display 8108. A purchase instruction notice 8106 is displayed beside a vending machine QR-code 8102 and a vending machine security authentication device 8104. The buyer 8004 takes out a smartphone 8202 and tap on a "Pay App2" icon 8204 in Fig 82. The buyer 8004 tap on a reset DA-code button 8302 in Fig 83 to change the pattern of his personal security authentication device. This is to ensure better protection. The buyer 8004 switch to his SMS (Short Message Service) application in Fig 84. A SMS message 8402 arrives in his smartphone 8202 that indicate the new pattern and orientation of a personal security authentication device 8404. To increase the security protection level, the SMS message 8402 is schedule to automatically delete after twenty minutes. The buyer 8004 dismantle and re-assemble the security authentication device 8404 according to the SMS message 8402. The buyer 8004 is now ready to purchase food from the vending machine 8002. The buyer switch back to his "Pay App2" application and tap on a transfer to account

button 8502 in Fig 85. The smartphone 8202 prompt the buyer 8004 to capture an image of the personal security authentication device 8404 to authenticate his identity as shown in Fig 86. After authentication, the buyer 8004 capture an image of the vending machine QR-Code 8102 together with the vending machine security authentication device 8104 in Fig 87. Fig 88 shows the final step in the purchase. The buyer 8004 verify a target account name 8802 tallies with the vending machine 8002, enter the value of a food price 8804, input the food code into a add note textbox 8806 and tap on a transfer button 8808. Once the information are verified and authenticated, the vending machine 8002 will proceed to heat up the correct food package and deposit it into the collection point. The buyer 8004 collect the food package and the transaction complete.

[34] Fig 89 shows another embodiment on the application of my invention in a train station 8902. In Fig 90, a commuter 9002 approaches and stands on a image capture area 9004 and take out a smartphone 9006. A computer 9010 scan the commuter 9002 using a camera 9008. The camera 9008 capture an image of the facial pattern of the commuter 9002 and a security authentication device 9102 that is mounted on the back of the smartphone 9006. This is shown in Fig 91. The computer 9010 transmits the image to a authentication server computer and authenticates the identity of the commuter 9002. An image authentication notice 9104 on the computer 9010 shows the authentication result. Fig 92 shows a close up view of the commuter 9002 and the security authentication device 9102. In Fig 93, a gate 9302 opens and allows the commuter 9002 to enter the train station 8902 to board a train for his destination. When the commuter 9002 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 9002 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.

[35] Fig 94 to Fig 96 illustrate some user defined settings in a smartphone 9402 that is relevant to my invention. A user taps on a setting button 9404 as shown in Fig 94. To go to the setting of my invention, the user taps on a DA-code button 9502 in Fig 95. Fig 96 shows the various setting meant for my invention. A DA-code reset frequency list box 9602 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 9602 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 9604 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 9606 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.

[36] Fig 97 shows a summary of how the various applications are integrated with my invention. Fig 98 shows another configuration of the system where the security authentication server computer is communicated directly to the smartphones 4002 (Fig 40) and the QR-code scanner 4604 (Fig 46).

[37] Fig 99 to Fig 101 shows another embodiment of my invention. A security authentication device 9902 is shown that is similar to Fig 34. The main difference is an increased in the number of pattern structures from three pattern structures in Fig 34 to eight pattern structures in Fig 99. This increased will significantly increased the number of possible combination and further enhanced the security level of my invention.

[38] Another embodiment of my invention is shown in Fig 102. A security authentication device 10204 is placed below a QR-Code 10202. To decode the security authentication device 10204, the image is captured with a smartphone and transmitted to a server computer. The server computer detect a start pattern 10302 and an end pattern 10312 on a pattern plate 10314 in Fig 103. This is to determine the location of the visual patterns used for the authentication. A first rectangular pattern 10304, a second semicircle pattern 10306, a third triangular pattern 10308 and a forth trapezoid pattern 10310 are used for the authentication process. Fig 104 shows an exploded view of the security authentication device 10204. The pattern plate 10314 is detachable from a main body 10402. The pattern plate 10314 is orientated according to a SMS (Short Message Service) message transmitted to the user's smartphone on a periodical basis. A lock plate

10406 is inserted into the main body 10402 and locked using a padlock 10408. Fig 105 shows the back view of the security authentication device 10204. A plate notch 10502 can be inserted into a number of alignment holes 10504 according to different requirement.

[39] Fig 106 and Fig 107 show another embodiment of my invention. This embodiment is similar to Fig 35. The difference is that Fig 106 uses structural depression to create the different patterns instead of printing the pattern on the flat surface structure.

[40] Fig 108 and Fig 109 show another embodiment of my invention similar to Fig 35. 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.

[41] 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, Data Matrix, Sticky Bits, bar codes, facial pattern, finger print pattern, palm print pattern, eye iris pattern and the like.

[42] 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.

[43] 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 7 to Fig 10 and Fig 31 to Fig 45.

(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 11 to Fig 26 and Fig 46 to Fig 57. 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 58 to Fig 62 and Fig 63 to Fig 70.

(e) Usage of QR-code placed at public area for advertisement or vending machine become significantly secured as shown in Fig 28 to Fig 30 and Fig 71 to Fig 77.

(f) 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 78.

(g) 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 89 to Fig 93. The system only need to ensure that the patterns of the security authentication device is not

repeated between people with high similar facial pattern.

(h) 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 97.

(i) 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.

(j) In the event that hackers hack the security authentication server computer or any of the server computers shown in Fig 97 and Fig 98, the recovery procedure is simply to reset all the orientation and order of all the security authentication device 3102 of all its users. Subsequently, the SMS notice 3702 will be send out to all its users for the recovery process to complete.

(k) As shown in Fig 46 to Fig 70, my invention has no real need to use sensitive biometric information of users. Example of such sensitive biometric information include finger print, palm print, iris pattern and voice pattern. This is the reason my invention is superior over other authentication system that uses sensitive biometric information. For these other authentication system, sensitive biometric information may be encrupted and send over the internet infrastructure. If hackers found a way into these information by hacking the internet infrastructure or servers, these sensitive information will become available to the hackers' communities. These sensitive information will be forever in the hand of hackers' communities,

there is no way to take them back. Users cannot change their biometric information. At some point in the future, criminal organization may acquire these information and use it to commit illegal activities that will come back to haunt the users.

(l) In the event that hackers hack the security authentication server computer or any of the server computers shown in Fig 97 and Fig 98, the hackers would have to make illegal fund transfer or payment as fast as possible, in large amount and multiple time. This is because the order and orientation of the security authentication device 3102 will be changed within less than twenty four hours. This will make it easier for frauds detection algorithms in the server computers to detect the hack, reset the security authentication device 3102, and inform the user.

[44] 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 multiple time authentication second patterns,

    d. a second electronic device,

    e. a server computer , and

    f. a plurality of pattern solid structures.

    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 pattern solid structures are arrange to match said second patterns, said second electronic device captures at least one image of said pattern solid structures and said first pattern, said second electronic device transmits a set of digital data packet or packets based on said image or images to said server computer, said server computer authenticates said digital data packet or packets 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, 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 pattern solid structures consist of a start pattern, follow by a plurality of coding patterns and complete with an end pattern.

5. The device of claim 1, wherein said server computer repeatedly generates a new set of said plurality of second patterns after a predetermined time duration has lapsed.

6. The device of claim 1, wherein said server computer repeatedly generates a new set of said plurality of second patterns after a predetermined fund transfer amount has exceeded.

7. An identity or security authentication device, comprising:

a. a electronic device,

b. a plurality of multiple time authentication patterns,

c. a server computer , and

f. a plurality of pattern solid structures.

whereby said server computer generates said plurality of patterns, said server computer transmits said plurality of patterns to said electronic device, said solid structures are arrange to match said patterns, said electronic device

captures at least one image of said pattern solid structures, said electronic device transmits a set of digital data packet or packets based on said image or images to said server computer, said server computer authenticates said digital data packet or packets to create an authenticated result, and said server computer transmits said authenticated result to said electronic device.

8. The device of claim 7, wherein said electronic device is selected from the group consisting of mobile device, smartphone, image scanner, tablet computer, desktop computer and laptop.

9. The device of claim 7, wherein said plurality of pattern solid structures consist of a start pattern, follow by a plurality of coding patterns and complete with an end pattern.

10. The device of claim 7, wherein said server computer repeatedly generates a new set of said plurality of patterns after a predetermined time duration has lapsed.

11. The device of claim 7, wherein said server computer repeatedly generates a new set of said plurality of patterns after a predetermined fund transfer amount has exceeded.

12. A method of identity or security authentication, comprising:

a. generating a plurality of multiple time authentication second patterns by a

server computer,

b. transmitting said second patterns from the server computer to a first electronic device,

c. receiving said plurality of second patterns on said first electronic device,

d. arranging a plurality of pattern solid structures to match said second patterns,

e. providing a first pattern,

f. capturing at least one image of said pattern solid structures and said first pattern on a second electronic device,

g. transmitting a set of digital data packet or packets based on said image or images to a server computer by said second electronic device,

h. authenticating said digital data packet or packets in said server computer to create an authentication result, and

i. transmitting said authentication result to said second electronic device.

13. The method of claim 12 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.

14 The method of claim 12 wherein said pattern solid structures consist of a start pattern, follow by a plurality of coding patterns and complete with an end pattern.

15. The method claim 12, wherein said generating of said plurality of second

patterns is repeated after a predetermined time duration has lapsed.

16. The method claim 12, wherein said generating of said plurality of second patterns is repeated after a predetermined fund transfer amount has exceeded.

17 A method of identity or security authentication, comprising:

a. generating a plurality of multiple time authentication patterns by a server computer,
b. transmitting said patterns from the server computer to an electronic device,
c. receiving said plurality of patterns on said electronic device,
d. arranging a plurality of pattern solid structures to match said patterns,
e. capturing at least one image of said pattern solid structures using said electronic device,
f. transmitting a set of digital data packet or packets based on said image or images to a server computer by said electronic device,
g. authenticating said digital data packet or packets in said server computer to create an authentication result, and
h. transmitting said authentication result to said electronic device.

18. The method of claim 17 wherein said pattern solid structures consist of a start pattern, follow by a plurality of coding patterns and complete with an end pattern.

19. The method claim 17, wherein said generating of said plurality of patterns is repeated after a predetermined fund transfer amount has exceeded.

20. The method of claim 17, wherein said generating of said plurality of patterns is repeated after a predetermined time duration has lapsed.