(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 March 2008 (13.03.2008)

PCT

(10) International Publication Number
WO 2008/028215 A1

(51) International Patent Classification:
G07D 7/12 (2006.01) *G06K 9/00* (2006.01)

(21) International Application Number:
PCT/AU2006/002013

(22) International Filing Date:
31 December 2006 (31.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006904878 7 September 2006 (07.09.2006) AU

(71) Applicant and
(72) Inventor: **WALKER, Matthew** [AU/AU]; 75 Central Avenue, Indooroopilly, Brisbane, Queensland 4068 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to the identity of the inventor (Rule 4.17(i))*

Published:
— *with international search report*

(54) **Title:** VISUAL CODE TRANSACTION VERIFICATION

(57) **Abstract:** The invention is an improved transaction verification method comprising a document, card or electronic apparatus with a transparent optical pattern visible to the user on a transparent window display. The verification process is performed by a user aligning the transparent pattern over a synchronized pattern image. The optical combination of these patterns induces a visual code, to be apparent to the user, which is then manually entered into a remote terminal or directly to the electronic apparatus to verify the transaction.

WO 2008/028215 A1

Description

VISUAL CODE TRANSACTION VERIFICATION

Detailed Description

[1] The present invention relates to a visual code transaction verification method. The method is enabled through a variety of different embodiments. One such embodiment being a standard plastic identification card or document with a recorded static optical pattern printed on a transparent section. Another potential embodiment is a version consisting of an electronic apparatus which consists of a digital transparent display connected to a processor which generates dynamic optical patterns using a cryptographic algorithm, synchronized with either a screen generated pattern image or another similar electronic apparatus, complete with its own electronic transparent display. This electronic apparatus would preferably take the form of a conventional membership card with added electronic functionality.

[2] The user aligns the transparent pattern across a digital screen such as an internet connected computer screen or another electronic apparatus which displays a specific generated pattern image synchronized to correspond to the user's recorded static card pattern or a cryptographic algorithm.

[3] When the transparent optical pattern section displayed on the user's card is aligned correctly, in synchronization with the corresponding generated optical pattern, the overlaid patterns of both layers optically combined will present the card holder with an identifiable series of characters, numbers, shapes or symbols. This unique visual code, which is only decipherable by matching the correctly generated optical patterns, is then manually entered into either the online website form or electronic apparatus to verify the validity of the identification request or transaction.

[4] The optical patterns used in this invention are rendered in a wide variety of possible optical embodiments. These can include anything from the small square patterns depicted in figures 1, 2, 2A, 3, 3A, 4, 5, 5A, 5B, 8, 9 and 10, to any number of other possible shapes which can be manipulated and combined to form a readable pattern. A pattern variation which uses segment display shapes commonly used in digital watches and pocket calculators is depicted in figures 6, 6A and 6B.

[5] Further optical obfuscation security is generated by warping characters or symbols, obfuscation of any straight lines or solid patterns with shades or transparent spotting, using lighter semi-transparent shades overlaid or color mixing effects to create darker or lighter shades and seeding the generated image pattern with false patterns designed to confuse optical analysis when either the transparent pattern or screen generated pattern is displayed independently.

[6] The invention is functional in both an electronic and non electronic method. The

non electronic method can be as simple as printing a static pattern on a transparent window and recording said pattern on a secure centralized database for use in remotely generating a screen image synchronized to the user's static pattern over an internet connection. The electronic version provides for an apparatus with built in dynamic transparent digital display, modified by an internal processor configured with a cryptographic algorithm, which provides a higher level of security for both online verification and electronic apparatus to electronic apparatus transaction verification. The visual code verification invention provides a method for changing the user's remote verification code by adjusting the generated image at the time of transaction verification request. At the same time, neither separate optical pattern individually exposes enough of the visually identifiable code without the presence of the corresponding pattern aligned correctly. This visual code method creates a manipulatable one time password which is very difficult to decipher without the presence of the user's corresponding transparent pattern.

[7] The non electronic embodiment's transparent optical pattern is electronically recorded on a central secure internet connected server so that modification calculations can be made to the screen generated image to induce the readable optical code effect when the user's transparent pattern is correctly placed over the screen generated image. The method is employable for any transaction verification purpose including online card payment transactions and indeed any situation where transaction verification is required. Membership cards or other non electronic embodiments with transparent sections can be produced using cheap existing technology with no specialized electronic identification verification apparatus needed at the user's end or server side. Apparatus with electronic transparent displays and internal processors, whilst more expensive than the non electronic version, enable higher security than traditional hardware tokens as well as improved inter-apparatus transaction possibilities, without expensive communication infrastructure.

[8] A further method of providing a transparent optical pattern utilizes any of the following optical properties to generate the desired optical code effect.

- transparent colored overlays
- transparent holographic material
- transparent prism layers
- transparent polarizing material
- transparent dichroic material
- transparent photochromatic layers

[9] The properties of any of these materials may be used on the transparent window or screen to produce different optical effects which will reveal the visual optical code and therefore enable a greater degree of both cryptographic and optical security.

[10] A second embodiment of the non electronic version involves changing the shape or location of the transparent section and printed code pattern on the document or card as shown in Fig 4 as well as changing the appearance or size of the screen generated image. For added cryptographic security a synchronized image marker can be printed on the document or card as shown in Fig 5. When this synchronized image marker is aligned with a similar marker on or near the generated image it enables the image to have variable sizes and shapes and therefore increases the cryptographic security by obfuscating the relevant card printed pattern image size and overlay location on the generated image.

[11] A further variation on the transaction verification method is shown in Fig 8: A static pattern is printed onto the transparent section of the document or card which is then placed over an animated screen generated pattern which the user stops at the point where the two patterns match. This method makes the visual code easier to see and understand on a variety of screens and other optical situations. Unfavorably, the position and shape of the pattern are static and so the same pattern match views are used each time. This degrades the security of the system if the process is intercepted with a screen and/or key logging program which might be surreptitiously installed on the computer generating the image and receiving the users manual response. The code is thereafter decipherable as a result of the third party's knowledge of the proportional positions and subsequent screen generated pattern image.

[12] A further variation on the transaction verification method is shown in Fig 7: A few small, randomly placed, transparent shapes are left visible on a printed opaque section of the card. This section is then placed over the screen generated image, which is a grid of characters, and the user types in the specific characters which can be viewed through the transparent shapes . This method makes the visual code easier to see and understand on a variety of screens and other optical situations. Unfavorably, the position of transparent shapes is static and so the same proportional views are used each time. This degrades the security of the system if the process is intercepted with a screen and/or key logging program which might be surreptitiously installed on the computer generating the image and receiving the users manual response. The code is thereafter decipherable as a result of the third party's knowledge of the proportional positions and subsequent screen generated images.

[13] The computerized transaction verification method of the non electronic embodiment comprises a secure database of transparent pattern records and a program capable of using these records to generate synchronized screen image patterns for a transaction verification request made from a remote internet connected computer terminal. The user will then correctly align said non electronic embodiment's transparent optical pattern over said screen image pattern, the combination of which

will generate a visual code effect for the user. This unique confirmation code will be manually entered into said remote computer terminal. This method is well adapted to being run over an internet system at such times as identification or transaction verification is required.

[14] A variation of the transaction verification method could include the use of a printed version of the generated image pattern, on a regular piece of paper, which is then used in place of the digital screen and in conjunction with the transparent optical pattern to display the verification code. This variation, while not as flexible as others, provides an extremely cheap method for use in counterfeit packaging verification or situations where electronics are not suitable.

[15] Another embodiment of the invention is a transaction verification apparatus as shown in Fig 10 preferably taking the form of an electronic smart card with a built in transparent digital display, battery, memory, processor and flat keypad. The processor is configured to generate a dynamic optical pattern using a cryptographic algorithm which will then be displayed on the transparent digital display. This dynamic optical pattern, in correct alignment with either a computer screen generated pattern image or another similar electronic apparatus, is configured to reveal a unique visual code to the user which is then directly entered into the flat keypad of the apparatus for transaction verification.

[16] The computerized transaction verification method of the electronic apparatus embodiment comprises a program capable of generating a synchronized screen image pattern for a transaction verification request made from a remote internet connected computer terminal. The user will then correctly align said apparatus transparent optical pattern over said screen image pattern the combination of which will generate a visual code effect for the user. This unique confirmation code will be manually entered into either said remote computer terminal or electronic apparatus for transaction confirmation. The synchronized screen image pattern will be generated based on a secure cryptographic algorithm.

[17] A further variation of the invention includes a sliding protective panel which covers the transparent optical pattern of the card or apparatus when it is not in use.

[18] These and other advantages of the present invention will become apparent to those skilled in the art upon reading and understanding the following detailed description with reference to the accompanying figures.

Background Art

[19] The increasing use of transaction verification throughout the world is most visibly exhibited in the credit card or other card payment systems being used commonly in grocery stores, universities and more increasingly, internet websites. The prevalent problem with remote payment card systems has been remote transaction verification.

The primary method of transaction verification security uses the user's signature which is often signed onto the sales receipt. Apart from being relatively easy to forge, the signature system does not adapt itself to modern remote electronic medium, such as the internet. An early verification method involved a basic Luhn algorithm to generate each unique card number in a non sequential manner which is then verified by testing against the algorithm. It is not intended to be cryptographically secure; it protects against accidental error, not malicious attack. This basic method of verification became increasingly invalid with the advent of the internet, as fraud increased and details of the algorithm became widespread. Today, half of all credit card fraud is conducted online. In response to this widespread fraud, credit card companies have implemented a static CVV (Card Verification Value) number printed on the back or front of cards at time of issue. The CVV, usually a 3 or 4 digit number, is required to be entered at the time of transaction, particularly with online payment. The disadvantage of the CVV number system is that many modern credit card fraud systems use card details including static CVV numbers gained from hacking online shopping payment databases, phishing techniques or screen and keylogging programs installed on the victim's computer system. Obviously, the major drawback to the CVV number system is the static nature of the printed numbers which mean once the card details are compromised the victim can easily be defrauded repeatedly. Furthermore, the simple static nature of the CVV number system method offers little proof that the remote user actually has the physical card in their possession as this simple 3 or 4 digit number can easily be shared alongside other card details. In response to this weak security method some banks have begun issuing members with a one-time password generating electronic device or hardware token. These devices have a small screen and button which, when pressed, generates a one time dynamically changing password using encrypted secret key programming, changing the password code every minute or so. The disadvantages of this system are the enormous expense of buying and issuing these electronic devices, battery maintenance, electronic fragility, inability to carry inside conventional wallets, separation from required membership card, and internal clock synchronization necessary with remote server. Smart Card technology has also been proposed as a secure method. This method has not become widely used, however, due to the issues of remote infrastructure cost and availability, electronic cloning, cost of cards with integrated circuits and fragility of those circuits when in day to day use. Proximity cards used as a payment system in some transportation services have also been proposed. Apart from suffering from the same problems as smart card systems they also have the added security issue of a potential unauthorized third party cloning or charging the card at a distance. The essence of the current problem is the need for a secure one time dynamically manipulatable password transaction verification system

without the associated remote infrastructure costs and electronic security vulnerabilities.

Disclosure of Invention

Technical Problem

[20] Transaction verification minimizing remote specialized electronic hardware, communication and infrastructure costs. Security against modern electronic phishing, keylogging or electronic eavesdropping techniques.

Technical Solution

[21] By using this invention method, transaction verification can be performed over either a universal internet connected computer terminal or directly from another electronic apparatus without using any specialized communication infrastructure. Security is provided by separating the visual optical code into unidentifiable patterns. The dynamic visual code effect is only apparent to the user when physically aligned with its correctly synchronized pattern which defeats most electronic phishing, keylogging or electronic eavesdropping techniques.

Advantageous Effects

[22] The non electronic version benefits from the security of a one time password system combined with the durability associated with not using remote electronics or power source other than a standard internet connected computer terminal, and easily works with cheap existing identification card technology.

[23] The electronic apparatus version, with a transparent digital display, provides extra security with its dynamic transparent display ability as well as internal cryptographic processor which enables a much higher degree of cryptographic strength and apparatus to apparatus transaction verification without needing a direct electronic communication.

[24] Both versions of the invention can easily perform transaction verification operated from a standard secure internet connected database server with little overhead processing needed to authenticate users or verify transactions. The visually obfuscated verification code effect provides excellent security against both on and offline attacks. Easy to use and very adaptable to internet applications the method is able to operate on ubiquitous computer screens available around the world while managed from a secure central server. The minimal use of remote infrastructure, direct electronic communication and dedicated electronic hardware enable extremely cheap setup costs and easy implementation.

[25] The option of no electronic hardware on the non electronic card version improves the durability, security and life of these cards while preventing complex electronic hacking attempts. Unlike Smart Cards and RFID cards, the non electronic cards are not

vulnerable to internal damage from the pressure or flexing incurred with normal use, such as inside a wallet or back pocket. The technology is simple and more resistant to in-shop fraud, for example when the card is passed to a waiter for payment at the end of a meal, as the code is more difficult to memorize with visual cues by potential criminals than the three digit CVV number or replication of the users signature. The technology also works easily alongside existing identification and transaction verification security systems i.e. CVV, Smart Card, RFID, magnetic strip.

Description of Drawings

[26] Although the invention will be described in terms of a specific embodiment as shown in the drawings, it will be readily apparent to those skilled in the art that additional modifications, rearrangements and substitutions can be made without departing from the spirit of the invention. Please note that for the purpose of clear illustration none of the diagram patterns depict semi-transparent shading techniques.

[27] FIG.1 is a pictorial view of an opaque conventional plastic membership card **2** with a transparent window and an example of a possible static printed pattern **1** thereon.

[28] FIG.2 is a pictorial view of the synchronized screen generated image pattern **6** as shown on a typical computer screen **5** .

[29] FIG.2A is an enlarged view of the screen generated image pattern **6** .

[30] FIG.3 is a pictorial view illustrating the user's card **17** placed over a standard computer screen **15** . The card's transparent pattern **16** is aligned over the screen generated image.

[31] FIG.3A is an enlarged view of the specific optical code effect **16** apparent to the user when the transparent card pattern is correctly aligned over the screen generated image pattern.

[32] FIG.4 is a pictorial view of a regular opaque membership card **21** with transparent sections demonstrating a variation on transparent window shape and size, in this particular example takes the form of three separate transparent circular sections **20** .

[33] FIG.5 is a pictorial view illustrating a printed alignment marker **25** on a portion of the transparent window beside printed pattern **26** on a conventional plastic membership card **31** .

[34] FIG.5A is a pictorial view illustrating a synchronized screen generated image pattern **29** which is larger proportioned than the user's synchronized transparent card pattern so as to induce a larger amount of obfuscation pattern security into the screen generated pattern. An alignment marker image **30** is generated with the screen generated image pattern to conform with the known proportional relationship between the user's alignment marker **25** and its transparent card pattern **26** .

[35] FIG.5B is a pictorial view demonstrating the correct alignment of the user's alignment marker **25** over the screen generated alignment marker **30** which creates a

visibly easy synchronized view of both markers **27** . This provides an easy method for the user to align the card over only the relevant portion containing the correctly synchronized pattern to create the password code effect **28** on the screen generated image **29** . This allows increased cryptographic complexity to be introduced into the generated image without affecting the intended password code effect **28** .

[36] FIG.6 is a pictorial view illustrating a possible segment display pattern **33** on a portion of the transparent window on a conventional plastic membership card **32**

[37] FIG.6A is a pictorial view illustrating a synchronized screen generated segment display image pattern **34** which is generated to synchronize with the known segment display type pattern **33** .

[38] FIG.6B is a pictorial view demonstrating the correct alignment of the user's transparent segment display pattern **33** over the screen generated segment display image pattern **34** . The combination of both patterns reveals to the user the intended password code effect **35** .

[39] FIG.7 is a pictorial view demonstrating a variation on the visual code method whereby a conventional plastic membership card **42** with a transparent window is printed with both an alignment marker **36** and a solid pattern which has a number of transparent circles **37** in a pre recorded proportional arrangement.

[40] FIG.7A is a pictorial view illustrating a screen generated image pattern of characters **40** which correspond to the proportional arrangement of the users known printed card holes. An alignment marker image **41** is also included to align the user's card over only the relevant characters.

[41] FIG.7B is a pictorial view demonstrating the card user's correct alignment of the card's alignment marker **36** over the screen generated complimentary alignment marker **41** presenting the user with a synchronized view of both markers **38** . This provides the correct alignment of the card's **37** transparent holes over the relevant screen generated characters **40** which presents the user with the intended password code effect **39** .

[42] FIG.8 is a pictorial view demonstrating a variation on the visual code method whereby a conventional plastic membership card **46** with a transparent window **45** has a specific printed pre recorded pattern.

[43] FIG.8A is a pictorial view illustrating a screen generated image pattern **47** with the user's recorded card pattern hidden at a specific position along the extended pattern.

[44] FIG.8B is a pictorial view demonstrating the card's **46** correct alignment of the card's printed pattern **48** at the matching position over the screen generated image **47** . This position is then used as verification data and manually entered into the computer terminal for verification.

[45] FIG.9 is a pictorial view demonstrating a plastic membership card **54** with an opaque sliding cover **50** protecting both the alignment marker **52** and the transparent

optical window complete with printed pattern **53** . The cover **50** much like a modern computer floppy diskette slides across **51** the transparent window protecting the transparent printed pattern **53** from both damage and remote optical interception when not in use.

[46] FIG.10 shows a preferred embodiment of a trusted transaction verification apparatus. The apparatus comprises a substantially flat housing **63** suitable to work alongside conventional credit card techniques. Housing **63** includes data entry keys **62** preferably of the membrane type in order to reduce thickness of the housing **63** and to provide a robust structure that is not easily damaged by liquids or rough handling. Housing **63** also includes a transparent electronic digital display **61** preferably of an thin, flexible construction. This display **61** should be capable of generating the synchronized optical patterns necessary to provide the user with an optical code effect when placed correctly over either a regular computer display with a generated pattern image or another similar transaction verification apparatus. This display **61** should also be capable of generating a correctly placed alignment marker image **60** if the particular verification method requires this. Housing **63** also includes a metallic contact point **65** for communicating directly with other similar transaction verification apparatus or dedicated security hardware. The internal electronics of the apparatus **64** (schematically indicated by a dashed line) comprise the following interdependent components: a memory unit; an internal clock; a random number generator; a thin power source and a processor configured to generate the digital image pattern, optical code effect and process the cryptographic nature of this pattern as well as verify the users manual code entry.

[47] FIG.11 is a pictorial view demonstrating two similar trusted transaction verification apparatus **63** and **66** verifying a transaction between the two. Both apparatus are similarly entered by their respective owners with the details of a specific transaction through their respective data entry keys **62** . Both apparatus are then aligned on top of each other so as to visually align each others transparent digital display's **61** correctly by use of both apparatus alignment markers **67.** Both apparatus identify each other through their respective metallic contact points **65** and establish a unique identity for each other. This activates the internal electronics **64** to cryptographically generate a synchronized digital pattern on each respective transparent display **61** creating a visual code **68** from the combination of both separate transparent display **61** patterns. This visual code which is apparent to the users of both apparatus is then entered into each apparatus data entry keys **62** by their respective users, providing a secure one time validation of the transaction. The cryptographic algorithms used are based on the respective identity data of the separate apparatus as well as data from both the random number generator and internal clock, the primary security resting on the unique visual

confirmation code **68** which is only synchronized when both patterns are correctly generated.

Mode for Invention

[48] The best form of the invention is the standard plastic identification non electronic PVC card with the optical pattern printed across a transparent strip thereon. The card is then placed in the correct position across an ordinary internet connected computer screen displaying the synchronized image generated from details recorded on a secure database. The readable optical code effect is then manually entered by the user into the internet connected computer which is used to verify authenticity of the remote card holding member. An electronic version of the transaction verification method with greater security and versatility, consists of a smart card with a built in battery and transparent digital display capable of generating a dynamic optical pattern from a cryptographic algorithm in synchronization with either a regular computer screen or another similar apparatus.

Industrial Applicability

[49] Can be used in all transaction verification systems such as verifying electronic cash payments for payment cards as well as verifying remote identification membership cards.

Claims

[1] A method of providing for a trusted authorization of a transaction, comprising: trusted documents, or the like, bearing a transparent optical pattern which when aligned with a synchronized generated pattern produces an optical verification code effect.

[2] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises a substantially flat document or card bearing a transparent optical window printed with optical pattern thereon.

[3] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a holographic transparent section with optical pattern thereon.

[4] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a prism transparent section with optical pattern thereon.

[5] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a polarizing transparent section with optical pattern thereon.

[6] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a dichroic transparent section with optical pattern thereon.

[7] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a color tinted transparent section with optical pattern thereon.

[8] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a transparent section with photochromatic lens with optical pattern thereon.

[9] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein said trusted document, or the like, comprises: a base constructed from a substantially flat document or card; a transparent section with optical pattern thereon; a sliding cover protecting the transparent section.

[10] A method of providing for a trusted authorization of a transaction in any one of claims 1-9, wherein an alignment marker is placed in a recorded fixed location on the document, or the like.

[11] A method of providing for a trusted authorization of a transaction in any one of claims 1-9, wherein an alignment marker is placed in a recorded random location on the document, or the like.

[12] A method for generating a synchronized static optical pattern which corresponds to the transparent optical pattern as in claim 1 for producing an optical verification code effect.

[13] A method for generating a synchronized sequence of optical patterns displayed one after the other which corresponds to the transparent optical pattern as in claim 1 for producing an optical verification code effect.

[14] A method for generating a synchronized static transparent optical pattern which corresponds to the transparent optical pattern as in claim 1 for producing an optical verification code effect.

[15] A method for generating a synchronized sequence of transparent optical patterns displayed one after the other which corresponds to the transparent optical pattern as in claim 1 for producing an optical verification code effect.

[16] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein verification is completed over the Internet via user entry of said optical verification code in any one of claims 12-15.

[17] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein verification is completed between a user and a apparatus at the same physical location via user entry of said optical verification code in any one of claims 12-15.

[18] A method of providing for a trusted authorization of a transaction as recited in claim 1, wherein verification is completed between a user and a apparatus on a trusted computer network via user entry of said optical verification code in any one of claims 12-15.

[19] A method of providing for a trusted authorization of a transaction, comprising: A trusted authentication apparatus for generating a transparent optical pattern which corresponds to a generated optical pattern for producing an optical verification code effect, comprising: transparent digital pattern display; communication interface; a memory unit; a power source; a processor configured to a set of operations comprising: generating a digital optical pattern for said transparent digital pattern display.

[20] A method of providing for a trusted authorization of a transaction, comprising: A verification apparatus for generating an optical pattern which corresponds to the

transparent optical pattern in any one of claims 1-9, 14, 15 or 19, for producing an optical verification code effect, comprising: digital pattern display; communication interface; a memory unit; a power source; a processor configured to a set of operations comprising: generating a optical pattern for said digital pattern display.

[21] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said processor further comprises generating a random number.

[22] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said memory unit contains a set of stored working keys.

[23] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said processor further comprises a symmetric encryption of said random number as recited in claim 21 using said set of working keys as in claim 22 that are stored in said memory.

[24] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said processor further comprises generating a signature by a cryptographic algorithm.

[25] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said processor further comprises generating a set of session keys by a cryptographic algorithm.

[26] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20 further comprising a synchronized internal clock.

[27] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20 further comprising a GPS receiver.

[28] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said apparatus is responsive to a personal identification code.

[29] A method of providing for a trusted authorization of a transaction as recited in claim 28, wherein said personal identification code comprises a code entered with a trusted keypad of said trusted authentication apparatus.

[30] A method of providing for a trusted authorization of a transaction as recited in claim 28, wherein said personal identification code is responsive to a biometric input from a user entered with a trusted biometric input apparatus.

[31] A method of providing for a trusted authorization of a transaction as recited in claim 28, wherein said personal identification code is responsive to a signature input from a user entered with a trusted signature input apparatus.

[32] A method of providing for a trusted authorization of a transaction as recited in claim 28, wherein said personal identification code is responsive to a voice input

from a user entered with a trusted microphone.

[33] A method of providing for a trusted authorization of a transaction as recited in claims 19 or 20, wherein said processor is responsive to whether said personal identification code as in any one of claims 28-32 corresponds to a stored personal identification code, said stored personal identification code is stored in said memory of said authentication apparatus, and said stored personal identification code is associated with an authentic user of said trusted authentication apparatus.

[34] A method of providing for a trusted authorization of a transaction as recited in claim 19, wherein said transparent optical pattern is generated using a cryptographic algorithm based on users personal information code as in any one of claims 28-33.

[35] A method of providing for a trusted authorization of a transaction as recited in claim 19, wherein said transparent optical pattern is generated using a cryptographic algorithm based on user's random number as recited in claim 21.

[36] A method of providing for a trusted authorization of a transaction as recited in claim 19, wherein said transparent optical pattern is generated using a cryptographic algorithm based on said signature as recited in claim 24.

[37] A method of providing for a trusted authorization of a transaction as recited in claim 19, wherein said transparent optical pattern is generated using a cryptographic algorithm based on said session keys as recited in claim 25.

[38] A method of providing for a trusted authorization of a transaction as recited in claim 19, wherein said transparent optical pattern is generated using a cryptographic algorithm based on said synchronized clock as recited in claim 26.

[39] A method of providing for a trusted authorization of a transaction as recited in claim 19, wherein said transparent optical pattern is generated using a cryptographic algorithm based on said GPS receiver as recited in claim 27.

[40] A method of providing for a trusted authorization of a transaction as in any one of claims 34-39, wherein said cryptographic algorithm process comprises a Data Encryption Standard (DES) cyclic block code (CBC) manipulation detection code (MDC).

[41] A method of providing for a trusted authorization of a transaction as in any one of claims 34-39, wherein said cryptographic algorithm process comprises MD5 or SHA-1.

[42] A method of providing for a trusted authorization of a transaction as in any one of claims 34-39, wherein said cryptographic algorithm process comprises a Public Key Infrastructure (PKI) encryption algorithm using a private key.

[43] A method of providing for a trusted authorization of a transaction as recited of claim 19 or 20, wherein said optical pattern incorporates an alignment marker.

[44] A method of providing for a trusted authorization of a transaction as recited of claim 19 or 20, wherein said optical pattern is digitally recorded onto a secure database.

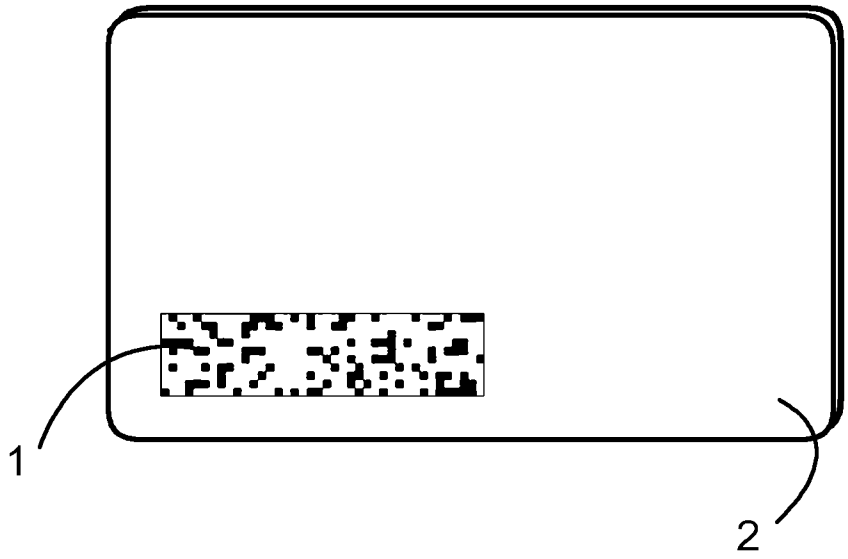
[45] A method of providing for a trusted authorization of a transaction as recited of claim 43, wherein said alignment marker is digitally recorded onto a secure database.

[46] A method of providing for a trusted authorization of a transaction as recited of claim 19 or 20, wherein said optical pattern changes after a predetermined time interval.

[47] A method of providing for a trusted authorization of a transaction as recited of claim 19 or 20 wherein the processor is also configured to determine if the intended readable optical verification code effect generated from the transparent optical pattern according to claim 14 or 15 placed over the generated optical pattern as recited in claim 12 or 13 is consistent with a user entered code.

[48] A method of providing for a trusted authorization of a transaction as recited in claim 19 wherein two separate trusted authentication apparatus generated transparent optical patterns are aligned over each other to generate an optical verification code effect.

FIG.1



[Fig. 2]

FIG.2

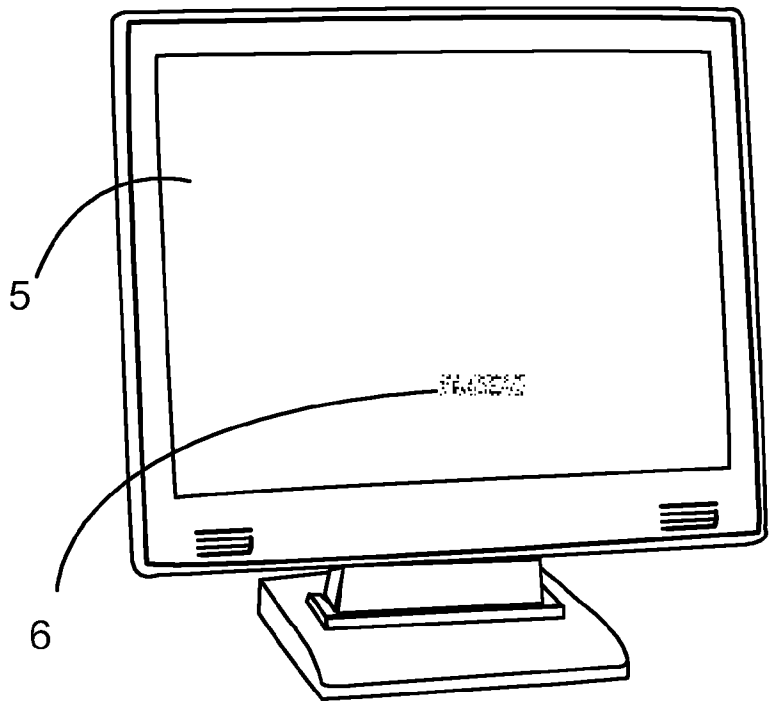


FIG.2A

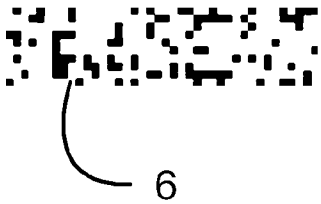


FIG.3

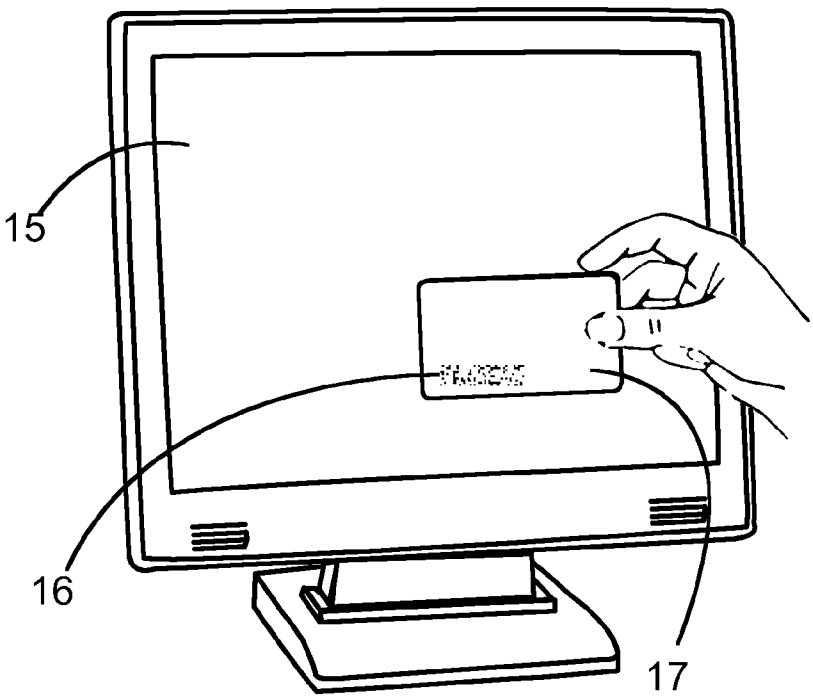
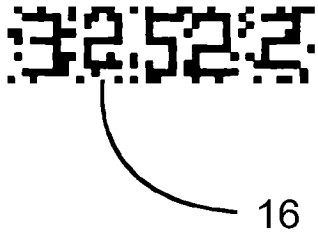


FIG.3A



[Fig. 4]

FIG.4

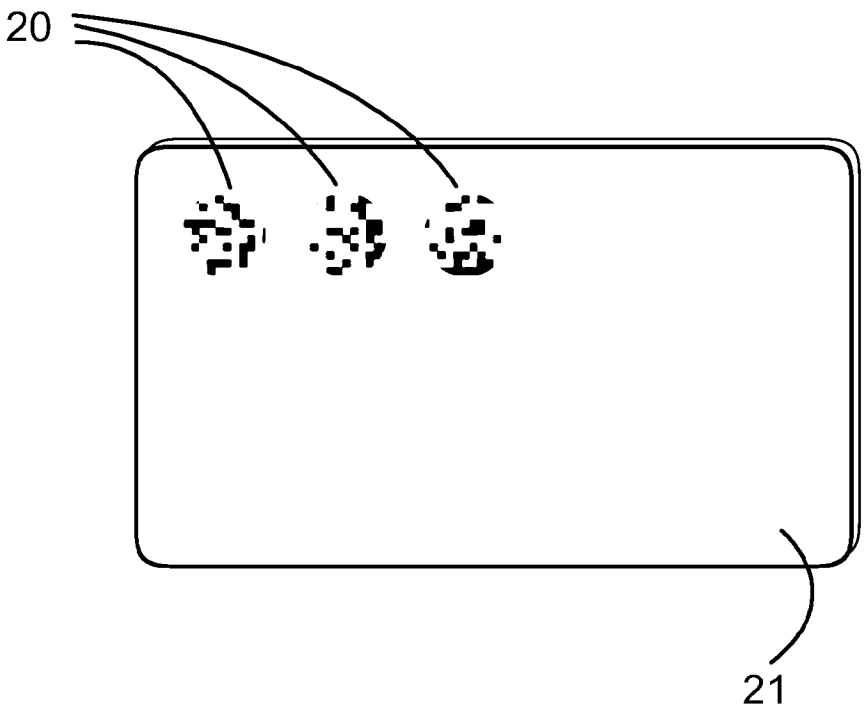


FIG.5

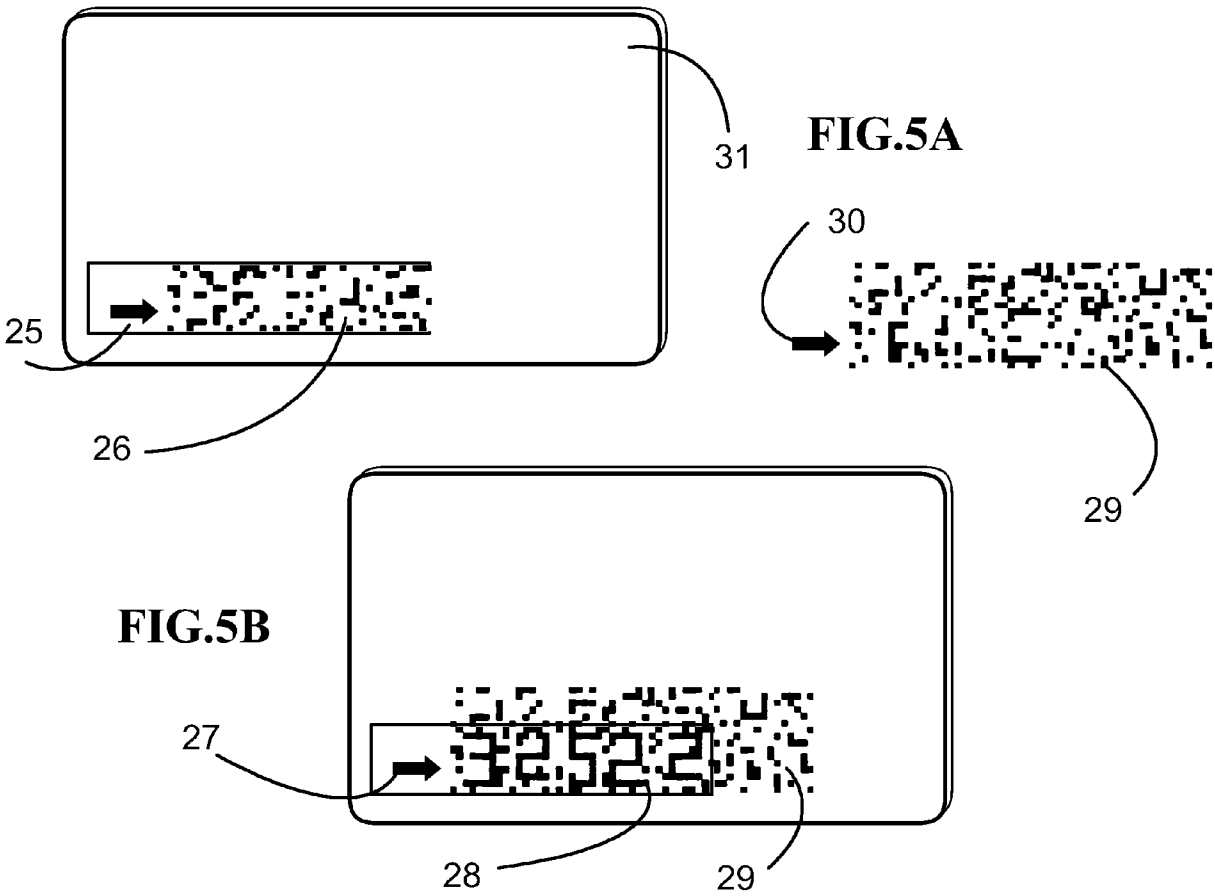


FIG.5A

FIG.5B

FIG.6

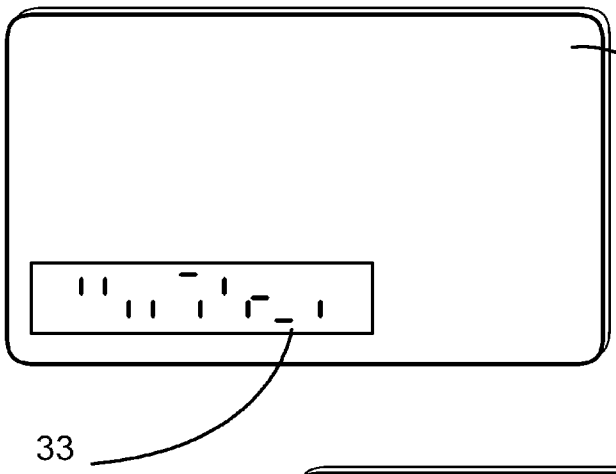


FIG.6A

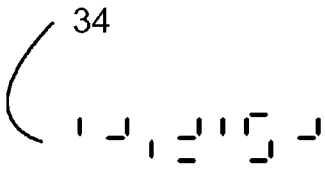


FIG.6B

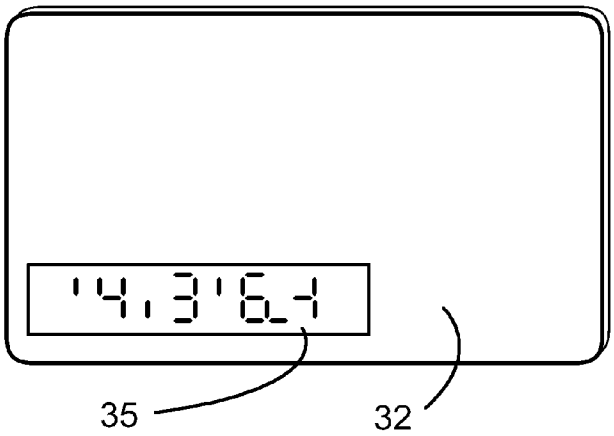


FIG.7

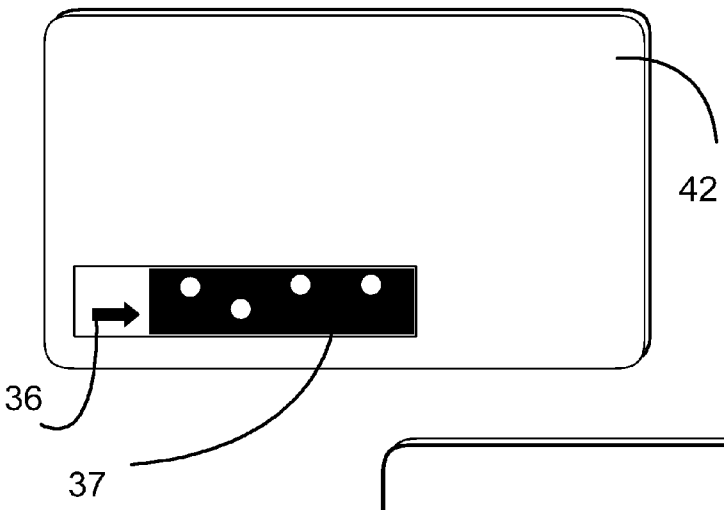


FIG.7A

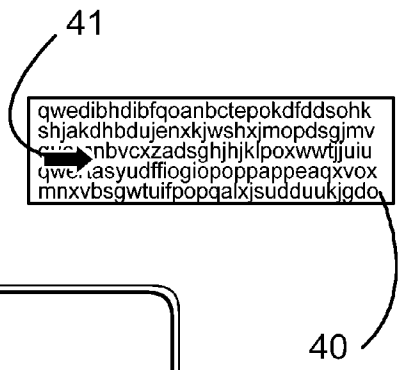


FIG.7B

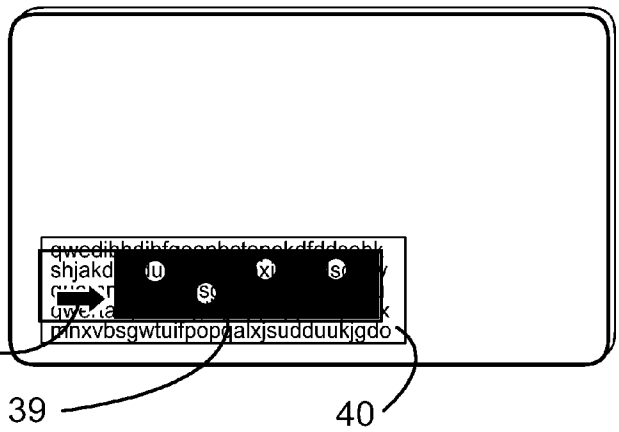


FIG.8

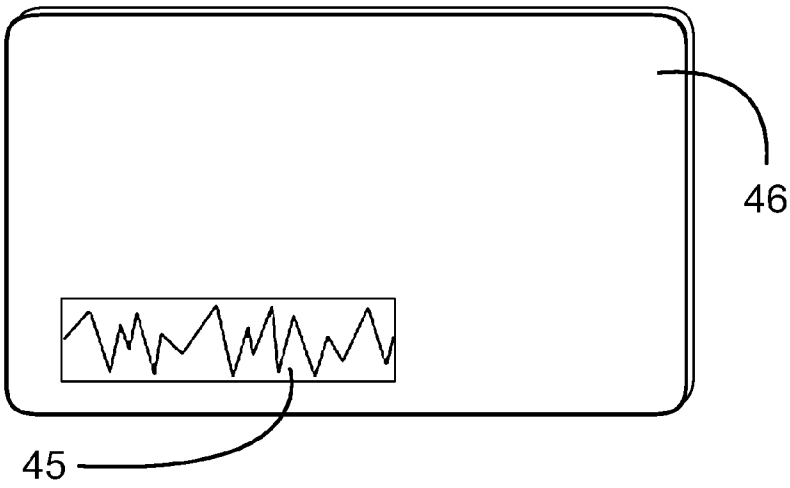


FIG.8A

FIG.8B

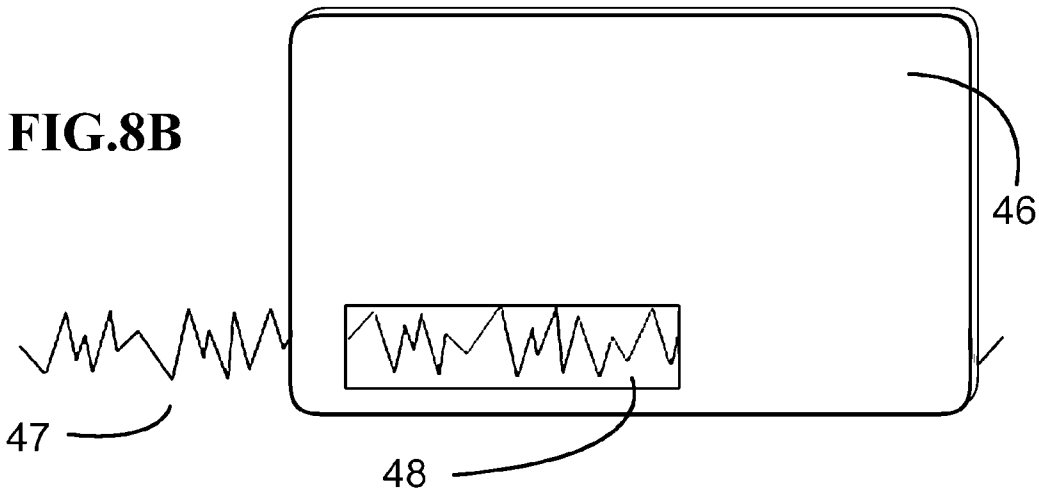


FIG.9

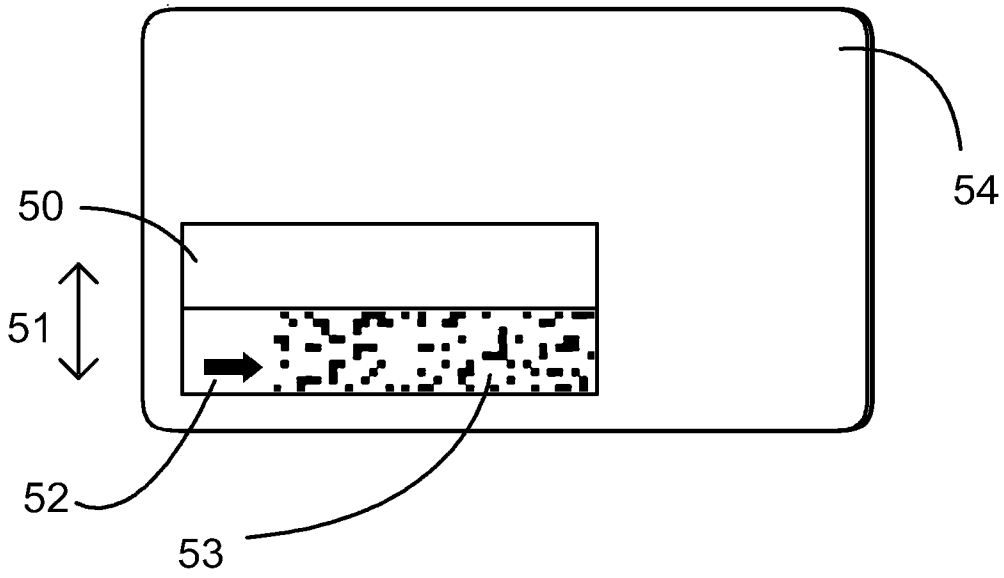


FIG.10

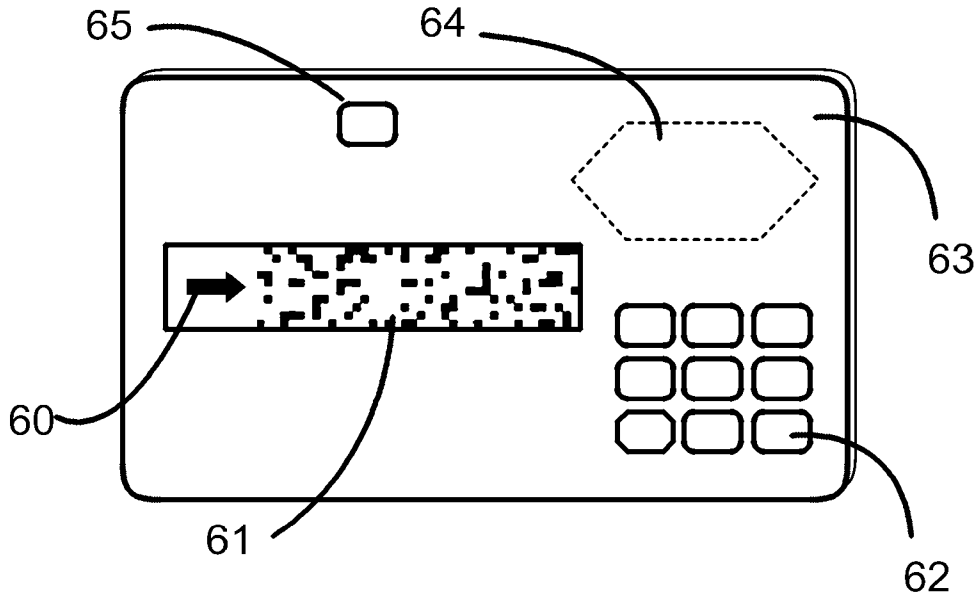
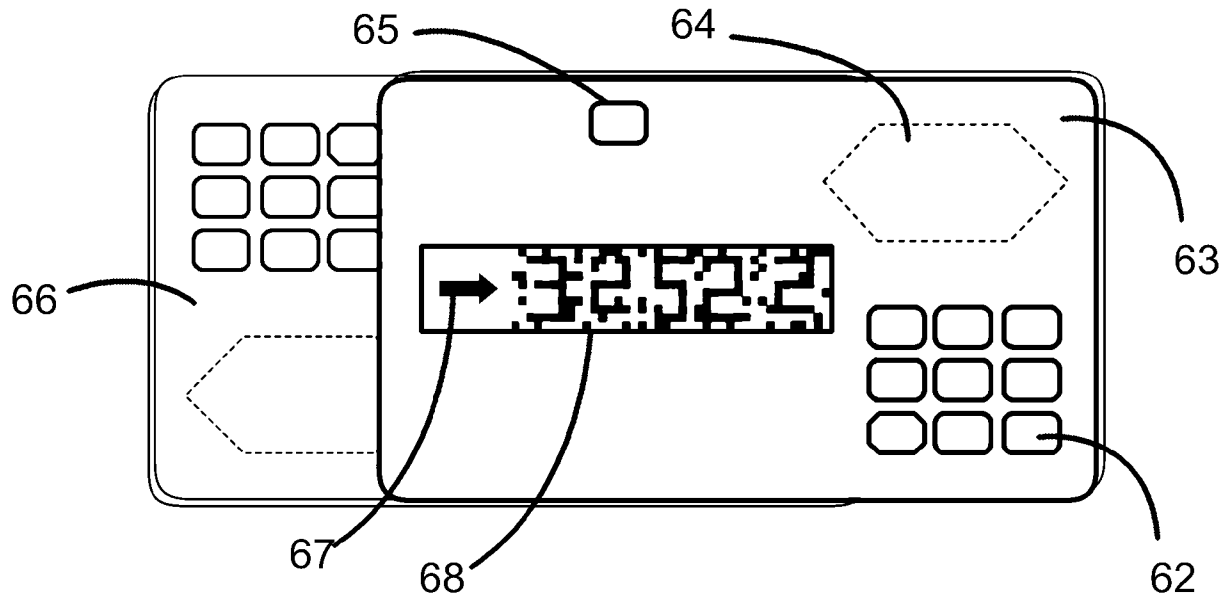


FIG.11



INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2006/002013

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G07D 7/12 (2006.01) ***G06K 9/00*** (2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Derwent WPAT, Espacenet: verification, authorisation, check, trust, identification, authentication, security, pattern, code, mark, mask, template, transparent, align, match, superimpose and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10260124 A1 (GIESECKE & DEVRIENT GmbH) 1 July 2004 whole document	1-45, 47-48
X	WO 2001/011591 A1 (EPIGEM LIMITED) 15 February 2001 whole document	1-45, 47-48
X	GB 1434907 A (DEEP PRINT PROJECTS LIMITED) 12 May 1976 whole document	1-45, 47-48
X	AU 746473 B2 (BUNDESDRUCKEREI GmbH) 2 May 2002 whole document	1-45, 47-48

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 March 2007	09 MAR 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **Mani Ramachandran** Telephone No : (02) 6283 2233

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2006/002013

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6249588 B1 (AMIDROR et al) 19 June 2001 whole document	1-45, 47-48
X	WO 1999/026793 A1 (SECURENCY PTY LTD) 3 June 1999 whole document	1-45, 47-48
X	US 4921278 A (SHIANG et al) 1 May 1990 whole document	1-45, 47-48
X	US 4991205 A (LEMELSON) 5 February 1991 whole document	1-45, 47-48

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2006/002013

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
DE	10260124	AU	2003293901	EP	1588332	WO	2004056582
WO	0111591	AU	63056/00	EP	1206767		
GB	1434907						
AU	746473	DE	19729918	CA	2294755	EP	0993379
		EP	1127712	HU	0100039	NZ	502142
		PL	337943	WO	9901291		
US	6249588	EP	1554699	US	5995638	US	6819775
		US	2002012447	WO	02101669		
WO	9926793	AU	12197/99				
US	4921278	CN	85100700	DE	3610445	JP	63158297
US	4991205	US	2959636	US	3003109	US	3051777
		US	3081379	US	3084213	US	3106612
		US	3227012	US	3313014	US	3372568
		US	3434130	US	3499650	US	3511940
		US	3555245	US	3559256	US	3559257
		US	3587856	US	3646258	US	3693983
		US	3699266	US	3705953	US	3735350
		US	3751583	US	3803350	US	3812287
		US	3818500	US	3842432	US	3842433
		US	3854889	US	3872462	US	3881053
		US	3918029	US	3925815	US	3943563
		US	3970775	US	4084198	US	4087839
		US	4107741	US	4110801	US	4118730
		US	4121249	US	4148061	US	4212037
		US	4213163	US	4338626	US	4342549
		US	4398223	US	4511918	US	4511930
		US	4636137	US	4646172	US	4660086
		US	4675498	US	4773815	US	4965829
		US	4969038	US	4979029	US	4984073
		US	5017084	US	5023714	US	5067012
		US	5119190	US	5119205	US	5128753
		US	5144421	US	5177645	US	5202929

US	5228112	US	5249045	US	5281079
US	5283641	US	5351078	US	5408536
US	5491591	US	5548660	US	5570992
US	5672044	US	5966457	US	6169840
US	6708385	US	7065856		

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX