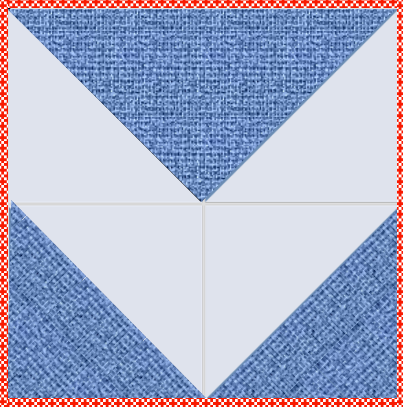
# PATENT PORTFOLIO OF VERITEC INC.

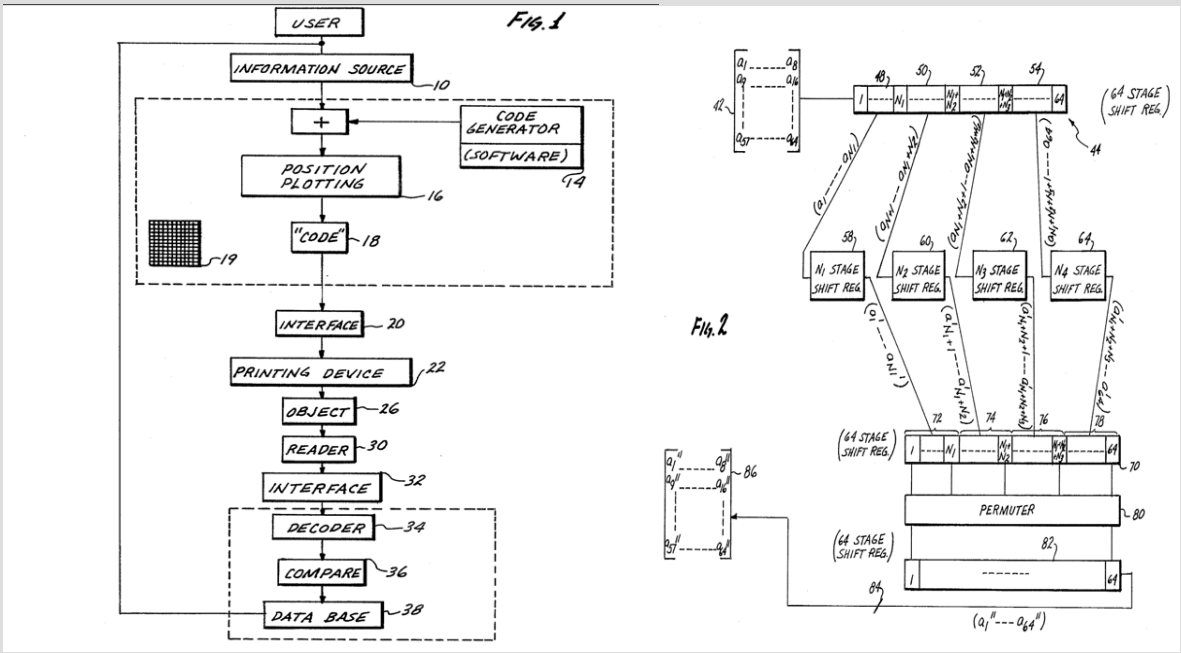
*Summaries & Potential Infringers*



AARON HAGSTROM - VERITEC INC. – 13 May 2023

## Table of Contents

NICKNAME: "2-CODE ENCRYPTION"
PATENT #: 4972475
TITLE: Authenticating Pseudo-Random Code and Apparatus
AUTHOR: C. Sant' Anselmo
PATENT FAMILY: Encoding/Decoding
ISSUE DATE: 1990 NOV. 20




*"Security against deciphering or 'cracking' the code is provided by the fact that the effects of the permutation … and of the non-linear shift register logics … present a numerically insurmountable hurdle to 'reverse' deciphering."* **– C. Sant' Anselmo**

Summary: This invention spruces up Dr. Solomon Golomb's shift-registers idea with a 2-code method and describes its use in an apparatus of detectors and readers to encrypt and decrypt information in a smaller space than normally used for barcodes.

The information source is digitized into binary bit form and processed by a software algorithm to generate a matrix code through a nonlinear feedback algorithm implemented through a 64-stage shift register that generates "pseudo-random" numbers for encryption. The software then feeds this first code to generate a second code by means of a permuter into a matrix array form and physically plot the results by means of a printing device. The nonlinear feedback algorithm was originally developed by Dr. Golomb to create sequences with random properties (an invention for which he was awarded the US National Medal of Science). Golomb wrote a book entitled "Shift Register Sequences: Secure and Limited-Access Code Generators, Efficiency Code Generators, Prescribed Property Generators, Mathematical Models" in 1967.

Sant' Anselmo improves on Golomb's idea by using a permuter in conjunction with the shift-registers to make the code extra secure. Sant 'Anselmo notes in his patent:

"From the foregoing, it can be appreciated that security against deciphering or "cracking" the code is provided by the fact that the effects of the permutation of permuter and of the non-linear shift register logics or algorithms of shift registers mask each other, as well as providing for an unusually large number of logical code generations from the original information source, so as to present a numerically insurmountable hurdle to "reverse" deciphering."

As an example of implementation, Sant' Anselmo suggests that a code reader – a photo-optical detector and photo source – reads the encrypted code and feeds it thorough a modem interface to a decoder that reverses the algorithm to produce the original code. The deciphered code is compared with the original in the "comparator."

Potential Infringement: Infringers could be anyone who uses Golomb's shift-register idea in conjunction with a "permuter" to encrypt and decrypt information, which allows codes to be reduced in size. Anywhere where there is a need for random number generation, whether that be in electronics, cryptography, error detecting and correcting codes, and synchronization pattern generation (i.e. fast access to data).

At the time of invention, barcodes used Golomb's shift register for encryption and the registers are also common components of RFIDs, which were "officially" invented in 1983 but in use since the 1940s and used to track assets, manage stock, and to control quality. Nonlinear shift-registers were proposed in one 2010 academic paper for use in Very Large-Scale Integration (VLSI), which millions or billions or transistors are combined onto a single chip for the purpose of high-speed cryptography.

Claim #1: A method for encrypting a code in a matrix array, comprising the steps of:

(a) Generating a first code having a series of signals;

(b) Permuting said signals to form a second code in a pseudo-random scheme including nonlinear feedback permutations and producing a representation of a two-dimensional spatial matrix pattern of the second code having a plurality of signal locations in a first Cartesian direction and a plurality of locations in a second Cartesian direction; and

(c) Printing, from the representation, a two-dimensional spatial matrix pattern of light reflective and non-light reflective portions arranged according to said permutations on a surface of a substrate.

NICKNAME: “PHONE-SCREEN CODE”

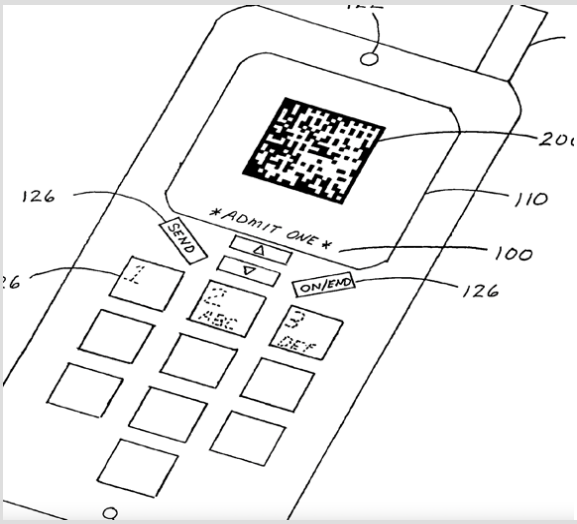
PATENT #: 8002175 B2

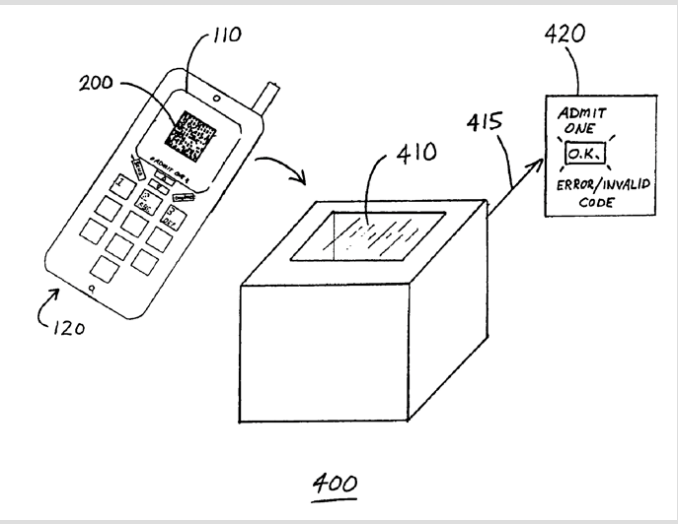
TITLE: System and Method for Utilizing a Highly-Secure 2-Dimensional Matrix Code on a Mobile Communications Display

AUTHOR: M. Kuriyama

PATENT FAMILY: Encoding/Decoding

ISSUE DATE: 2011 AUG. 23




*“There exists a need for a highly secure 2D matrix code on a mobile communications display which provides increased security and convenience and which overcomes the drawbacks of the known systems and methods.”* **-M. Kuriyama**

Summary: This patent describes the means, by which a highly-secure 2D matrix code can be transmitted to a “mobile communications device” and displayed on the LCD screen in a transaction between a “user” and “recipient.” This is vital to prevent the risk of identity theft when using a credit card. The patent includes the right to generating the code, transmitting the code to a phone, and reading the code off the phone.

At the time of the invention, point of sale solutions for businesses in the form of magnetic stripe reader devices that connected to cell phones were in existence. NTT DoCoMo had developed a system for displaying a 2D code on a phone screen. An example of use would be buying a virtual

ticket (i.e. code) to get into a concert. However, these codes are generally not secure and not information dense. A recommendation for making the process more secure is for the use of a "highly-secure 2D code" which includes VeriCode and VSCode, and checking the validity of the code through use of an access code.

Potential Infringement: Infringers might be anyone who uses a "highly-secure 2D code" in some kind of transaction on a mobile communications device. A mobile communications device could be a cellphone, pager, PC, or integrated wireless communicator. The question is what defines a highly-secure 2D matrix code. The patent is meant to include VeriCode and VSCode but what else?

Claim #1: 1. A method for providing and permitting use of a secure two-dimensional matrix code on a mobile communications display for the purpose of facilitating a selected transaction between a user and a recipient, said method comprising steps of:

> electromagnetically receiving a request from a user as part of a transaction between the user and a recipient;
>
> generating a secure two-dimensional matrix code comprising data including at least a verification of the transaction and further selected data directed to at least account numbers of the user related to a financial aspect of the transaction, and goods and services information related to the transaction, said code including such data in order to facilitate the transaction as such data is coded within the two-dimensional matrix and as authorized by the recipient;
>
> transmitting image data of the secure two-dimensional matrix code to a mobile communications device so that the secure two-dimensional matrix code can be created on a display of the mobile communications device;
>
> reading the two-dimensional matrix code off the display of the mobile communications device by a remote reader, wherein the reader includes a touch screen for display, and displaying at least portions of the financial account numbers of the user as determined from the two-dimensional barcode on the touch screen, and receiving an election by the user of a chosen financial account of the user for completing the transaction;
>
> upon electromagnetically reading of the two-dimensional matrix code, receiving a signal from the remote reader including transactional use data regarding the transaction and the further selected data between the user and recipient, and as a result of such transactional use data and the further selected data, checking the validity for use of the secure two-dimensional matrix code as a part of the transaction between the user and the recipient; and
>
> electromagnetically transmitting data regarding acceptability of the use of the secure two-dimensional matrix code to at least one of the recipient, the user and the reader, wherein acceptability of the use of the secure two-dimensional matrix code results permits completion of the transaction between the user and the recipient.

NICKNAME: “FINGERPRINT READING METHOD”

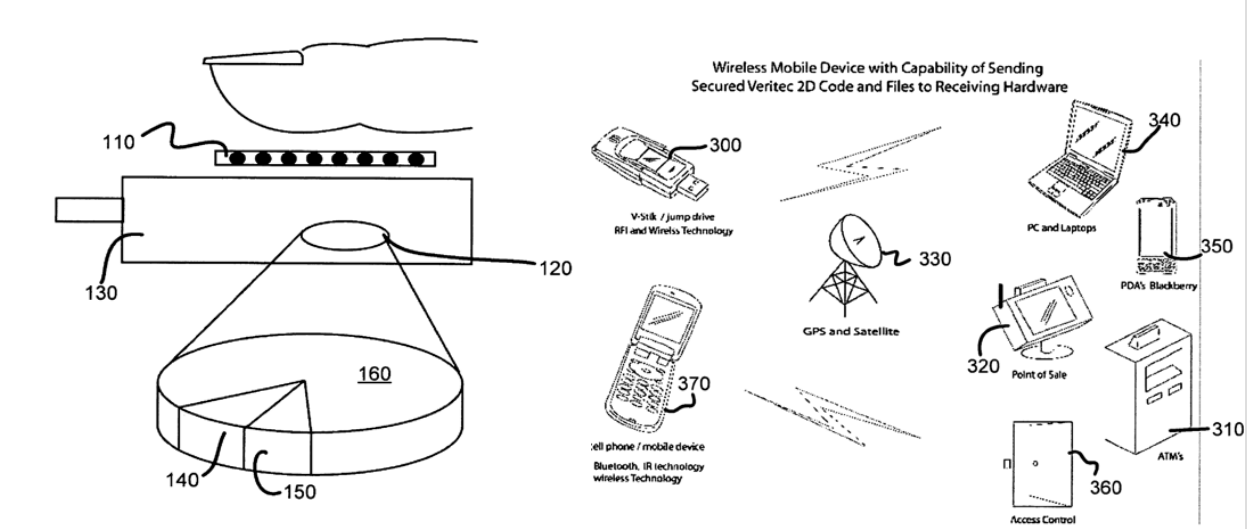
PATENT #: 7614551 B2

TITLE: Method and System for Securely Encoding and Decoding Biometric Data into a Memory Device Using a Two-Dimensional Symbol

AUTHOR: J. Kingsley-Hefty

PATENT FAMILY: Encoding/Decoding

ISSUE DATE: 2009 NOV. 10




*“Often it may be desirable to have security on a portable memory device. Further, it may be desirable to have a fingerprint reader or other biometric device coupled to a memory device that stores a template or a fingerprint or other biometric identifier in a data representation that may be converted to a two-dimensional array symbol.”* **– J. Kingsley-Hefty**

Summary: This is a patent for converting biometric data gathered from an optical finger-print sensor or iris scanner (for instance) into a 2D symbol and also for decoding said 2D symbol back to biometric form. A user might access secure files on a computer by placing his finger on a USB-attached fingerprint sensor. The encoding and decoding process will be done partially on a flash drive and partially on a computer. For security purposes, some of the encoding and decoding software is stored on the flash drive and some software on the actual computer. This

software makes the 2D code which can then be compared with a template of the fingerprint on the flashdrive. If user is authenticated, he can see the information associated with that code, whether medical records, demographic info or something else.

Potential Infringement: Infringers are those who use 2D codes to encode and decode biometric data. Facial biometrics have been encoded into colored barcodes, for instance, through a software called FaceCerts developed by Microsoft Research around 2003. So, we could be infringing their patent, potentially.

Claim #1: A method of storing information on a memory device comprising:

> setting up a user to be associated with the memory device, in order to selectively control access to stored information on the memory device, the step of setting up a user including a step of obtaining biometric information from a biometric reader;
>
> coding at least a portion of the biometric information before storage in the memory device, wherein the coding comprises a bar coding process so that biometric information will be stored as a representation of a bar code symbology;
>
> storing the representation of the bar code symbology within memory of the memory device;
>
> storing at least one additional file on the memory device; and
>
> protecting the at least one additional file with the biometric information stored in the representation of the bar code symbology wherein protecting the at least one additional file includes encoding the at least one additional file with the biometric information stored in the representation of the bar code symbology.

NICKNAME: "GHOST ENCODER"

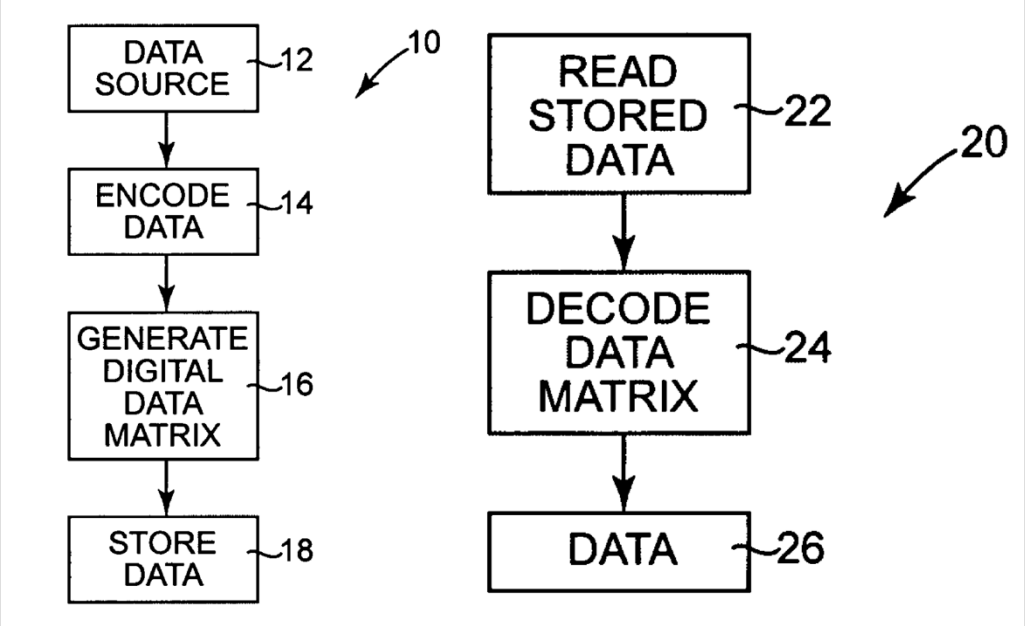
PATENT #: 7516904 B2

TITLE: Methods for Encoding and Decoding Information

AUTHOR: D. Wood

Patent Family: Encoding/Decoding

ISSUE DATE: 2009 April 14




*"The present invention provides methods for securing data by using a data-encoding technique of a symbology, such as a one or two-dimensional symbology to provide secure data without the need to convert the data into a graphical symbol."*

***- D. Wood***

Summary: This invention allows for the encoding, decoding, and storing of a 2D matrix code electronically. That is, there is no need for an actual physical symbol, thus the "ghost" nickname. The processing is all done electronically.

Generally, 2D matrix codes are encoded into Reed-Solomon blocks and then converted to a bitmap image, which can be printed on labels. The code is then decoded with an optical imaging system.

An implementation of Reed-Solomon is used for encryption in this patent. Several suggestions for how to store the code efficiently are mentioned in the patent: compression by data cells, compression by row, stringing together data matrices, bit-packing.

Potential Infringement: If this patent covers anyone who decides to store a code on a memory device, it could be very lucrative patent.

Claim #1: 1. A method of encoding and electronically storing at least one of personal, biometric or financial information within an electronic storage device so as to facilitate the use of the stored information from the storage device as part of an activity that utilizes at least some of the stored information, the method comprising the steps of:

> providing at least one of personal, biometric or financial information to be encoded;
>
> encoding the information into digital data;
>
> generating a two-dimensional matrix of digital data cells from the encoded information; and
>
> electronically storing the two-dimensional matrix of encoded information by electronically writing the two-dimensional matrix of encoded information to an electronic memory storage device as a data file usable for printing a two-dimensional bar code symbol and allowing access to the two-dimensional matrix data file to permit decoding of the two-dimensional matrix data file and information decoding for use in an activity without utilizing either of optical scanning and image capturing of a printed bar code symbol.

NICKNAME: “CODE FIXER”

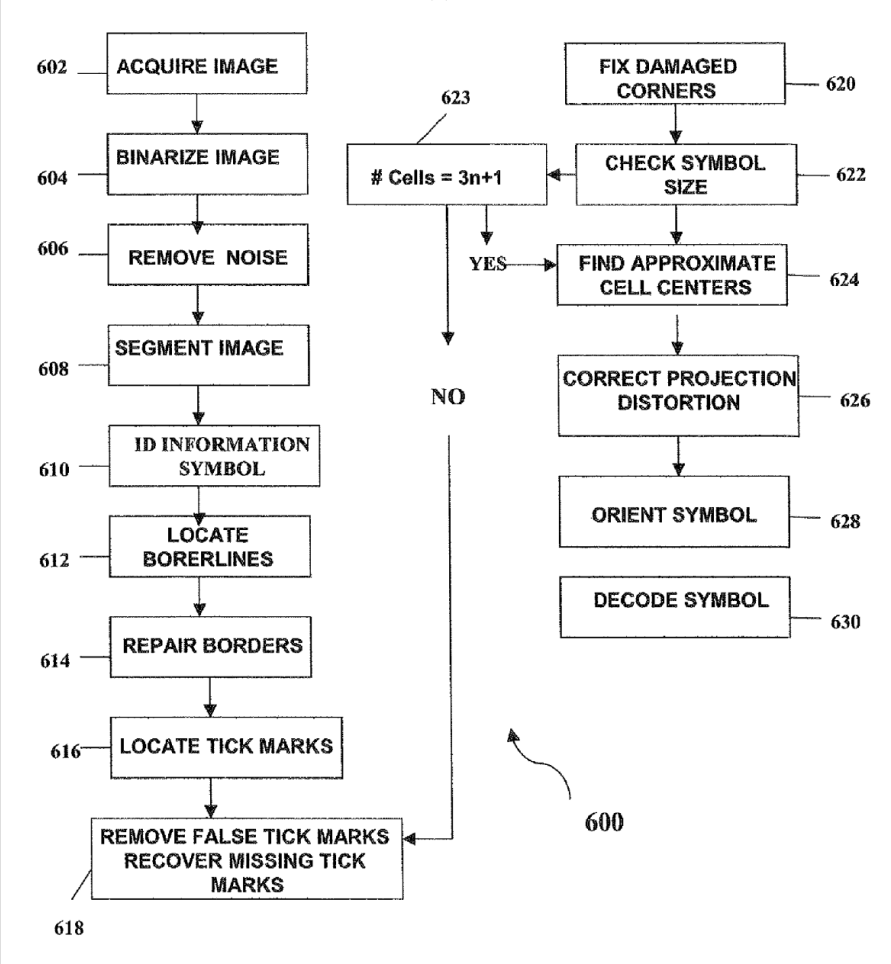
PATENT #: 8746566 B2 / 8152070

TITLE: Two-Dimensional Symbol and Method for Reading Same.

AUTHOR: H. Al-Hussein

PATENT FAMILY: Encoding/Decoding

ISSUE DATE: 2014 June 10 | 2012 April 10



*"Both the 2D symbologies and the methods used in such applications need to be able to accommodate noise and distortion and correct for poor lighting or missing sections of a symbol to accurately and efficiently decode such symbols."*
***-H. Al-Hussein***

Summary**:** This invention describes 2D code that can be read regardless of the noise or distortion or missing parts of the symbol. This is accomplished by means of the code having four solid borders to locate the code easier and tick marks throughout the code to help repair it. Before the code is repaired, it needs to be binarized and this is done by means of tiling the image and generating a greyscale histogram for the data cells in each tile; the histogram is then smoothed. Once this is complete, noise can be removed from the image of the code. Specifically, the image in segments to locate pieces of the symbol. Other more intricate steps are taken to find the solid sides of the symbol, fill in missing sections of the borderlines, fix damaged corners and correct image projection distortion.

Potential Infringement**:** This is a complex algorithm for removing noise from codes, so to know whether someone is infringing might be pretty difficult because they would have to share their algorithm and it would need to be analyzed in detail.

Claim #1 2014 Patent (8746566 B2**):**
A method of reading an information symbol having: four borders defining an interior region; and data cells within the interior region comprising a plurality of first shade tick marks and plurality of second shade tick marks, the method including:

acquiring an image of the information symbol;

identifying plural borderlines in the image of the information symbol;

determining location information for a plurality of data cells;

reducing projection distortion in the image o the information symbol;

modifying the location information of the image as a result of the reduction of projection distortion; and

decoding data in the data cells of the image of the information symbol.

Claim #1 2012 Patent (8152070):

A two-dimensional symbol comprising:

four solid borders defining an interior region;

a plurality of first shade tick marks and a plurality of second shade tick marks arranged in an alternating pattern at the interior region of the four solid borders and adjacent to the four solid borders; and

data cells in the interior of the plurality of first shade and plurality of second shade tick marks, wherein each of the four solid borders are made up of constituent cells; at least a first solid border is reconstructed; at least a second solid border is not reconstructed; and the at least first solid border is reconstructed based on the length of the at least second solid border.

NICKNAME: “CLOSED & OPEN-LOOP MONEY SAVER”

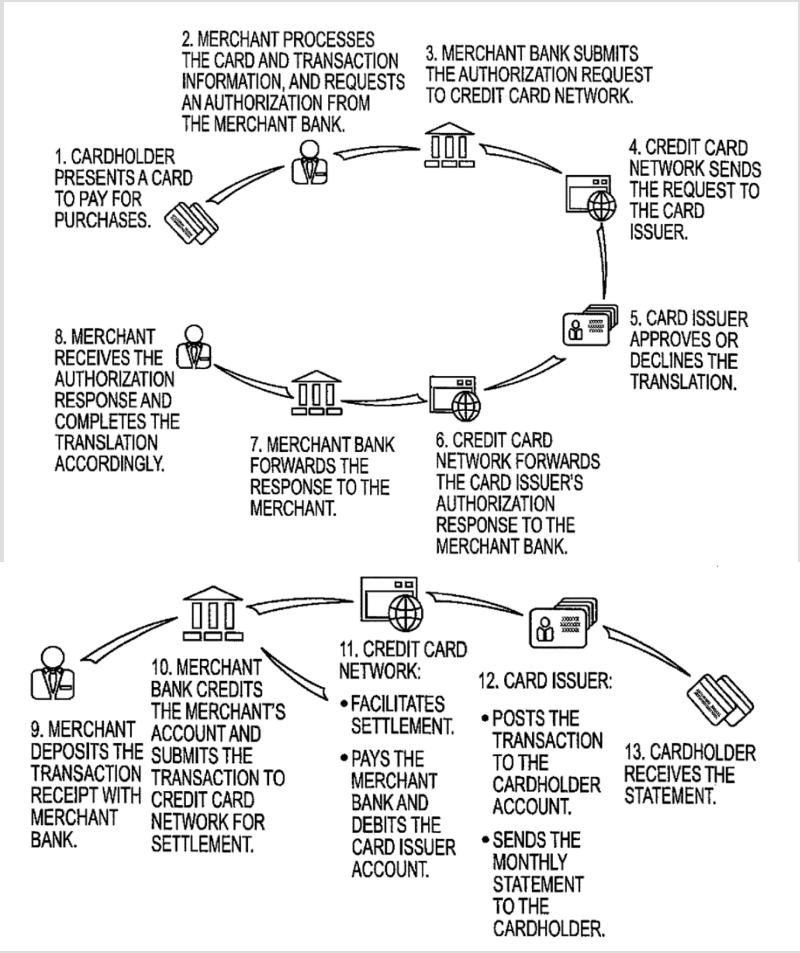
PATENT 10360556 B2 / 20140025518

TITLE: Financial Card Transaction Security and Processing Methods

AUTHOR: T. Look

PATENT FAMILY: Encoding/Decoding

ISSUE DATE: 2019 July 23 & 2014 Jan 23




“The present invention is directed to methods and systems for reducing fraudulent transactions and for avoiding high interchange fees that are associated with open-loop transactional networks.”

**– T. Look**

Summary: This patent describes a method and system for a secure financial transaction that can be processed through either open loop or closed loop networks. There are problems associated with traditional methods of completing a financial transaction in the credit or debit card industries: the first problem is that the banks, card processor, and merchants are taking on all the financial risk and the second problem is the cost of using an open-loop financial network from the main service providers.

A solution to these problems is to first have the user prove his right to ownership of the card using digital secured data or biometric data, and second, to avoid fees by bypassing the open-loop network in favor of a closed-loop network. Software can turn the user's card off, forcing the card-holder to identify himself.

Potential Infringement: A potential infringer would be anyone who combines a closed-loop system with an authentication system.

Claim #1 2019 Patent (10360556 B2):

A method of authorizing a financial card transaction at a merchant point of sale system, comprising:

accepting, by a merchant point of sale system, a presentation of a financial card of a financial card user, the financial card having data stored within a financial card data storage component;

reading the data from the storage component of the financial card by a reader that is operatively connected with the merchant point of sale system and thereby receiving data within the merchant point of sale system from the data that is stored within the storage component of the financial card related to a financial card transaction, the data received including at least one character that indicates the usage of a closed loop network to process financial aspects of the transaction;

receiving additional data from the data that is read from the storage component of the financial card by the merchant point of sale system for payment of a transaction, the received additional data being sufficient to conduct a financial transaction including the usage of an open loop network to process financial aspects of the transaction;

utilizing software or firmware coded within the merchant point of sale system for determining from the received data to process the financial transaction by way of the closed loop network instead of the open loop network based upon the receipt of the at least one character that indicates the usage of the closed loop network;

as a result of the step of reading the data, changing a status of the financial card from an on position, based upon the financial card status at a time of reading the data, to an off position utilizing the merchant point of sale system and the software or firmware coded within the merchant point of sale system, and then requiring a verification input at the merchant point of sale system from the financial card user; and

after the verification input is received from the financial card user at the merchant point of sale system, changing the status of the financial card to an on position followed by a processing of the financial transaction by way of the closed loop network.

Claim #1 2014 Patent (20140025518):

A method of conducting a financial card transaction for the payment of goods or services from a merchant comprising:

Receiving data from data that is provided to a financial card for payment of a transaction, the data received including at least once character that indicates the usage of a private network to process financial aspects of the transaction; and

Receiving data from data that is provided to the financial card for payment of a transaction, the data received including at least one character that facilitates the usage of an open network to process financial aspects of the transaction; and

Determining from the received data whether to process the financial transaction by way of the private network or the open network.

NICKNAME: "LIGHT-WINDOW READER"

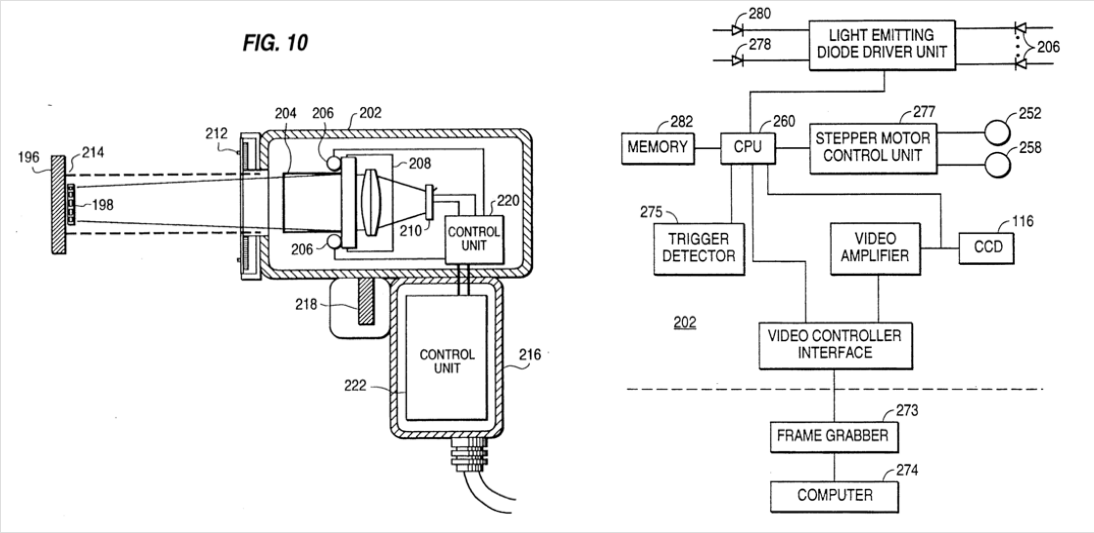
PATENT #: 5331176

TITLE: Hand-Held Two-Dimensional Symbol Reader with a Symbol Illumination Window

AUTHOR: C. Sant' Anselmo

PATENT FAMILIES: Readers

ISSUE DATE: 1994 July 19




*"Positioning the sensor so that all of the symbol is in the field of view of the sensor can be a problem. What is needed is a capture system that allows the user to position the field of view of the sensor to cover the symbol being captured."* **– C. Sant' Anselmo**

Summary: This patent describes a symbol reader that projects a "window" of light to more easily read the symbol than with current technology. The light might be projected only on the edges or on both the edges and the interior of the symbol. The window can be different shapes and sizes depending on the code being read. There is an automatic zoom control implemented with a CPU and stepper motor unit but can be implemented with an integrated circuit as well. A CCD array captures the entire symbol and then this signal is converted into an RS-170 video signal by a

video signal controller and interface. The user pulls a trigger to project a light window onto the symbol. When the image is in focus, the captured data is fed to the “frame grabber” and enters a decoding loop, described in more detail in the patent.

Potential Infringement: Cognex creates a lot of 2D barcode readers and they have a full page on website devoted to lighting of 2D codes, which could potentially infringe.

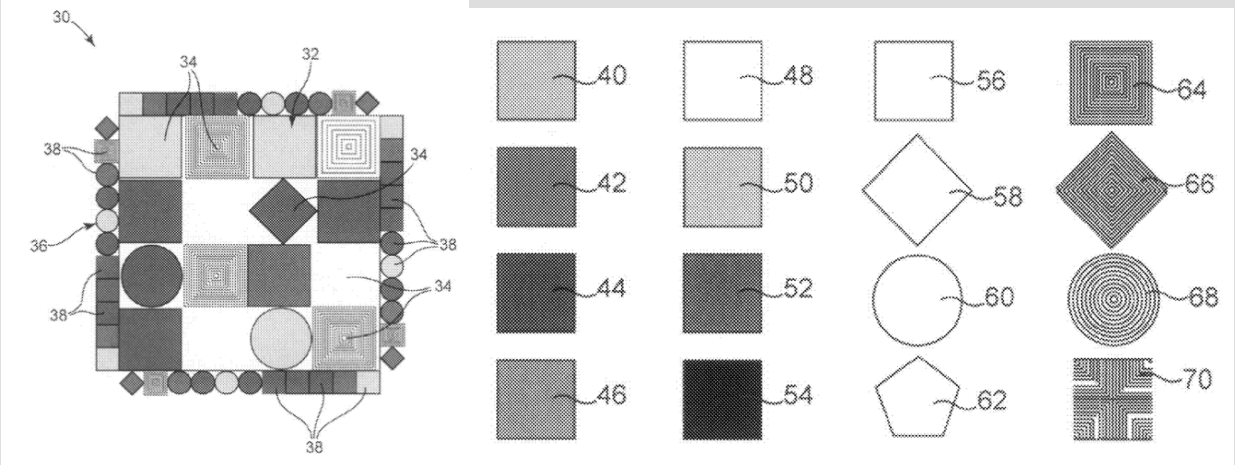
---

Claim #1:

A symbol illuminator and capture system, comprising:

> a two-dimensional sensor for viewing a two-dimensional symbol, having a viewing window and capturing an entire symbol image; and
>
> projection means, associated with said sensor, for projecting two-dimensional illumination window for illuminating the entire symbol, the illumination window being equal to or larger in size than and aligned with the viewing window.

NICKNAME: “SMORGASBORG CODE”
PATENT #: 7510125
TITLE: Multi-Dimensional Symbologies and Related Methods
AUTHOR: T. Look
PATENT FAMILY: Symbologies
ISSUE DATE: 2009 March 31




*“The present invention provides the ability to realize increasing data bits from a single cell by creating the cell from differing optically readable designs and colors or combinations thereof in any combination or array that provides more than two data bits per cell.”*
**-T. Look**

Summary: This patent describes a code that increases storage capacity by utilizing colors, grey-scale levels, various cell shapes or geometric patterns within the code. This may allow the ability for a camera to extract more data from a cell without extra cost or camera complexity.

Again, a symbology is a mapping between messages and barcodes.

Linear symbologies usually are read with a laser scanner that uses a polygonal mirror or galvanometer-mounted mirror. On the other hand, 2D codes cannot be scanned by a sweep pattern and therefore scanners are usually cameras that have light-sensitive elements organized in an array.

Potential Infringement: There might be a code that combines different methods to store data, for instance a combination of color and geometric patterns. However, I can't find any that use such techniques.

---

Claim #1:
A multi-dimensional matrix symbol comprising a first plurality of data cells wherein at least one data cell of the first plurality of data cells comprises plural characteristic features and each characteristic feature represents an encoded data bit wherein the first plurality of data cells are arranged in an internal data field and the symbol further comprises a data cell border comprising a second plurality of data cells surrounding the internal data field, the second plurality of data cells including at least one binary data cell.

NICKNAME: “EASY-SCAN CODE”

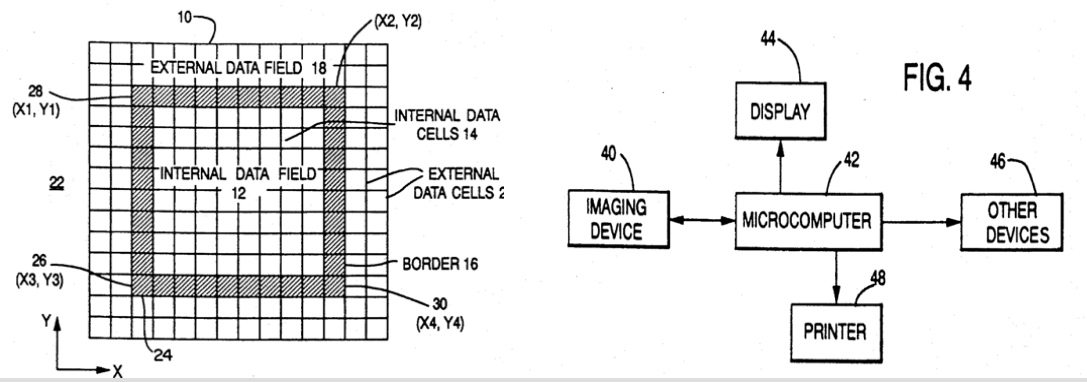
PATENT #: 5612524

TITLE: Identification Symbol System and Method with Orientation Mechanism

AUTHOR: C. Sant’ Anselmo

PATENT FAMILY: Symbologies

ISSUE DATE: 1997 March 18




*“Because of the need to scan the conventional symbols in a preferred direction and because many items that include such symbols are randomly oriented when they arrive at a symbol reader, a need has arisen for a symbol that contains high-data density and which oriented in any direction can still be cost-effectively machine-readable.”* – **C. Sant’ Anselmo**

Summary: The goal of this invention is a data matrix symbol that is more easily scannable.

This invention is a symbol including a square array of data cells surrounded by a border of orientation and timing cells. This border can in turn be surrounded by an external data field that also includes information data cells or can be a quiet zone. Also included with the invention is a system of capturing an image of the symbol, determining its orientation, decoding the symbol and outputting the results to a display or a label. The border is usually formed by cells that are light-absorbing or light-reflecting. The 3D orientation of the symbol is determined with rotational decomposition algorithms common in the graphics industry. More information on the rotational decomposition can be found in a 1986 article entitled “Graphing Quadric Surfaces” by

G. Haroney. The data cells can be encoded in color or gray-scale or alphanumeric information or morse-code, as example. A machine using magnetic ink character recognition or s optical recognition system can read a symbol containing alpha-numeric or Morse code. The code can be used for a film hologram, in which different symbols are laid out at different depths and viewed with a camera with controllable depth of field and focus.

There are many 2D Matrix symbologies: QR, ShotCode, DotCode, Grid Matrix, Aztec Rune, Aztec Code, Code One, Han Xin Code, iQR code, Micro QR code, Data Matrix, VeriCode, VSCode (derived from VeriCode but with higher information density), Maxicode. Most were invented in 80s and 90s but also in early 2000s. These codes have the general structure of data regions containing square modules in an array, alignment patterns, finder patterns, and a quiet-zone border. The symbology supports all 256 ASCII characters, ISO characters, and Extended Binary Coded Decimal Interchange Code. They are divided into codes that use the Reed-Solomon algorithm for error detection and correction and those that use convolutional error correction. The size of the codes can vary from 7 *x 7* to *144 x 144.*

Potential Infringement:

This is another difficult patent to prove infringement on because one needs to have a detailed knowledge of the algorithm used and get access to a competitor's algorithm. The one that is being used seems to be using other methods in common use.

Claim #1:

An identification symbol system for an object, comprising:

an identification symbol, comprising:

a substrate associated with the object;

a computer readable data matrix data field formed on said substrate and providing symbol information for uniquely identifying the symbol; and

computer readable orientation means, formed on said substrate and positioned adjacent said field on at least one side, for providing orientation information from a substantially omni-directional three-dimensional orientation of capture; and

a device for capturing the symbol, identifying the object from the symbol information.

---

NICKNAME: “LCD-SCREEN CODE”

PATENT #: 7159780

TITLE: Method for Reading a Symbol having Encoded Information

AUTHOR: M. Christian

PATENT FAMILY: Symbologies

ISSUE DATE: 2007 Jan. 9

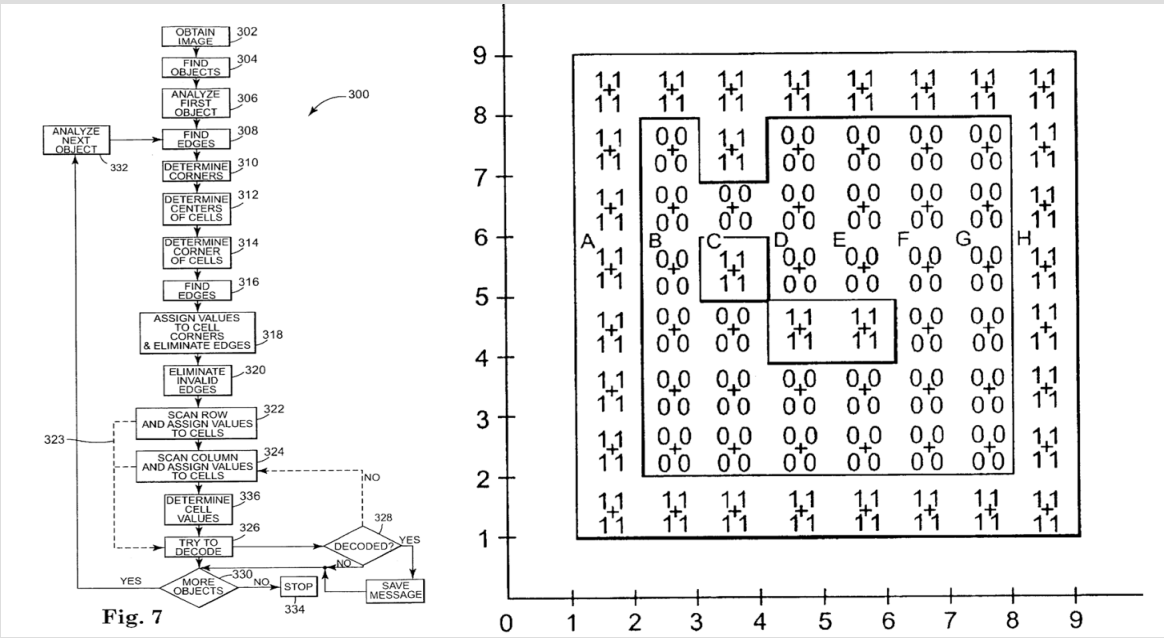


Fig. 7

*“A significant drawback of [symbols etched on LCD screens] is they have little or no light reflecting contrast, and as a result can be very difficult to image …. However, generally, an edge analysis can determine the symbol image.”* **– M. Christian**

Summary: This patent gives methods and apparatus for imaging and decoding symbols that are formed in relief or within the surface of an object.

Generally. when a reader scans a symbol, the different light reflective properties of the lines and spaces are analyzed and decoded into an alphanumeric representation of the symbol. As an alternative, the code can be raised or set in relief on the surface of the object (i.e. stamped, engraved, etched, milled, or molded into the surface). The codes set in relief are more durable and may be less expensive. They, however, may be particularly difficult to read since the high and low areas reflect the scanning beam fairly equally. A particular application of such a code are on certain microelectronic devices such as LCD screens. The codes are also useful in

manufacturing where there is a need to store large amounts of information such as serial numbers, lot numbers, batch numbers, model numbers, and customer codes. Such codes may also protect against forgery since engraved into the surface.

The problem with LCD displays is that they are usually covered with a thin-film coating of chromium, a highly reflective metal which buries the code, when it is etched. So color differences between the code and substrate are hard to discern. The patent can be applied not only to linear or stacked symbologies but also to 2D symbologies. A multi-step edge analysis is applied to eliminate invalid edges and to assign binary values to the data cells. The imaging device might be a Charge-Coupled Device (CCD), which comprises a one or two-dimensional array of adjacent photodiodes, where each photodiode defines a distinct pixel.

Potential Infringement: Besides the microelectronic industry, the automotive industry is one big user of 2D laser marking QR codes where traceability, quality control, manufacturing instructions, and general product data are important to store compactly and permanently on the car. There is a particular need to track defective products. Also relevant in the gun industry where traceability and storing large amounts of vital data. Companies that seem relevant are Keyence, Datalogic, Microscan, Honeywell, and Zebra Technologies, all of which have readers for 2D barcodes on various surfaces.

Claim #1: A method of determining features of a symbol based on a relief pattern having a two-dimensional matrix of data cells representing encoded information, the method comprising the steps of:

> determining the presence of discernible edges of the relief pattern and compiling information representative of an edge image at least partially representative of the two-dimensional matrix of data cells and including the discernible edges;
>
> validating the edge image by performing an edge analysis of at least one of the discernable edges; and
>
> determining data cells of the symbol from the edge image so that the symbol can be decoded to provide the information encoded within the relief pattern of the symbol.

NICKNAME: “2-CARDS-IN-ONE”
PATENT #: 2022-0129720 A1 / 11222250 B2 / 2019-0272455 A1 / 2013-0248591
TITLE: Combined Event Driver and Financial Card
AUTHOR: T. Look
PATENT FAMILY: Financial Cards
ISSUE DATES: 2022 Apr. 28 | 2022 Jan. 11 | 2019 Sept. 5 | 2013 Sept. 26

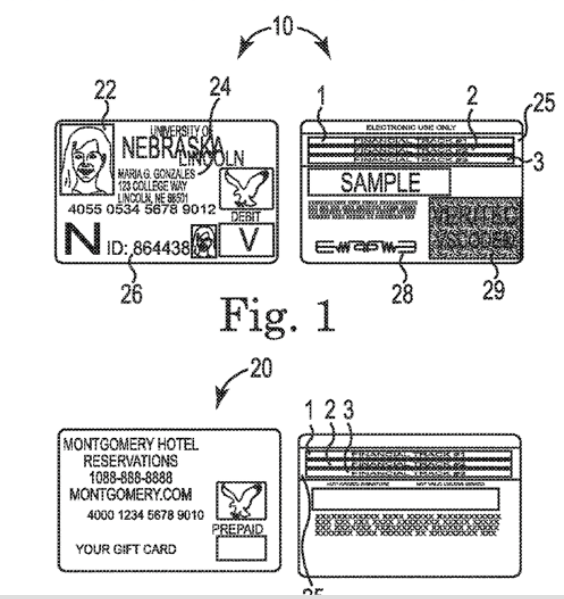


Fig. 1

*“It is a goal of the present invention to reduce the potential for fraud and theft …. Cards and methods of the present invention can also add value to certain types of cards so as to increase a user’s standard of care to such cards.”* **- T. Look**

Summary: This patent describes a financial card that can also store a secondary type of information.

Combining multiple functions into one card reduces the potential for fraud or theft that comes with carrying around multiple cards. Some potential financial use of the card are as gift-cards, prepaid, debit, or credit cards. Some potential secondary uses are for buying school lunches, for loyalty and membership uses, for a hotel room key, for keyless electronic door opener, or for paying tolls. An example of such a card might have financial information on two magnetic stripe and non-financial information on a third magnetic stripe. Data on the RFID transponder could serve as an electronic key for entering a secure location. As another example, a secure Veritec Inc. code like VSCode might store biometric or demographic data. This patent has four different versions and the 2022 versions make it clear that the secondary data is "associated with an event other than a membership number, or other issuer, card sponsor or issuing bank data" and furthermore that there is an "access ability" on the card that does not utilize the financial account data.

Potential Infringement: Potential infringers are anyone who uses financial cards combined with a secondary use.

Claim #1 April 2022 Patent (2022-0129720 A1): A combined use transactional card including electronic readable means by which a financial transaction can be conducted, the card also comprising further electronically readable means that is also functionally part of the transactional card and that is encoded with data that when read by an electronic data reader for the source of electronically readable data services an event that is not associated with the financial account.

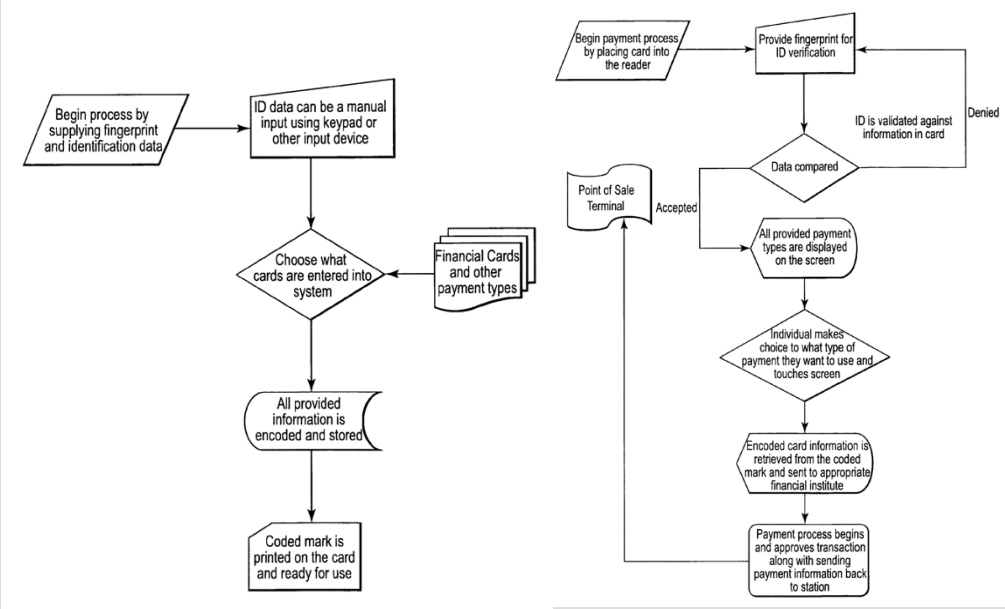
Claim #1 Jan. 2022 Patent (11222250 B2): A combined use financial transactional card including first electronically readable means that is encoded with financial account data by which a financial transaction is to be conducted from a financial account along with graphics on a face of the card that depict information about at least one of a card issuer, a card sponsor, and an issuing bank, and a second electronically readable means of the transactional card that is encoded with access ability data that comprises at least one of cardholder identification or biometric data, demographic data of a cardholder, data associated with an event other than a membership number, or other issuer, card sponsor or issuing bank data, and that when read by an electronic data reader for the source of electronically readable data services an access ability for a card user, which access can be obtained based upon the access ability data without utilizing the financial account data or based upon data of any financial transaction.

Claim #1 2019 Patent (2019-0272455 A1): A combined-use transactional card including first electronically readable means that is encoded with financial account data by which a financial transaction is to be conducted from a financial account, a second electronically readable means of the transactional card that is encoded with access ability data that when read by an electronic data reader for the source of electronically readable data services an access ability for a card user which access can be obtained based up on the access ability data without utilizing the financial account data or based upon data of any financial transaction.

Claim #1 2013 Patent (2013-0248591): A combined-use transactional card including electronically readable means by which a financial transaction can be conducted, the card also comprising further electronically readable means that is also functionally part of the transactional

card and that is encoded with data that when read by an electronic data reader for the source of electronically readable data services an event that is not associated with the financial account.

NICKNAME: "ALL-IN-ONE CARD"
PATENT #: 8152056 B2
TITLE: Secure Cards and Methods
AUTHOR: L. Johanns
PATENT FAMILY: Financial Cards
ISSUE DATE: 2012 Apr. 10




*"With the increase of fraud and identity theft, financial institutions and individuals are having to pay for losses because of such theft …. Managing the numerous financial transaction cards and the like can be cumbersome and increase the risk of theft or loss …. The present invention therefore provides the ability to provide the transactional capability of one or more cards in a single, secure, and useable format." – **L. Johanns***

Summary: This patent describes an invention that combines multiple cards -- whether financial, loyalty, phone, ID -- into one card. The key is to put the information of all these cards into a 2D matrix code. When using the card at a point of sale, a fingerprint scanner can validate the user.

Potential Infringement: Potential infringers could be anyone who uses a chip to combine information on multiple cards into one card.

Claim #1: A method of making a secure card, the method comprising the steps of:

obtaining information to be encoded including account information related to a first transaction account;

obtaining information to be encoded including account information related to a second transaction account;

encoding the account information of the first transaction account and the second transaction account;

generating a coded mark, the coded mark comprising a matrix of data cells that represent encoded information of the first and second transaction accounts; and

providing the coded mark of encoded information on a surface of a card so that by decoding the coded mark, a transaction can be conducted with respect to one of the first and second transaction accounts.