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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 June 2011 (30.06.2011)

PCT

(10) International Publication Number
WO 2011/077459 A2

(51) **International Patent Classification:**
G06K 9/20 (2006.01)

(21) **International Application Number:**
PCT/IN20 10/000846

(22) **International Filing Date:**
23 December 2010 (23.12.2010)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
2976/MUM72009 23 December 2009 (23. 12.2009) IN

(71) **Applicant** *(for all designated States except US):* **ALEX¬ IA TECHNOLOGIES PRIVATE LIMITED** [IN/IN]; 2, Crescent Chambers, 4th Floor, Tamarind Lane, Fort, Mumbai 400 023 (IN).

(72) **Inventor; and**

(75) **Inventor/Applicant** *(for US only):* **KUMAR, C , Kushal** [US/IN]; Alexia Technologies Private Limited, 2, Crescent Chambers, 4th Floor, Tamarind Lane, Fort, Mumbai 400 023 (IN).

(74) **Agent: OBHAN, Essenese;** Obhan & Associates, 501/7, Lane W 21A, Western Avenue, Sainik Farm, New Delhi 110 062 (IN).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, 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, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

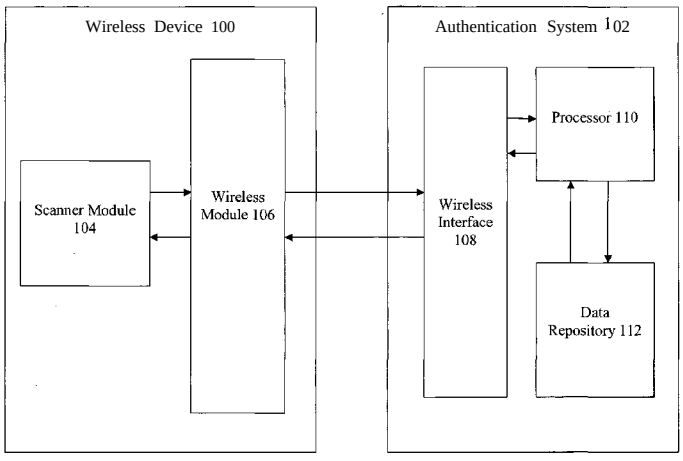
(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: A METHOD OF EXTRACTING NATURALLY ENCRYPTED FEATURES FROM A NATURAL SURFACE OF A PRODUCT

Figure 1



(57) Abstract: An authentication system for authenticating a product is disclosed. The authentication system comprises of an interface that is configured to receive a microscopic image of a specific area on the surface of the product including a naturally encrypted feature set of the product. The authentication system also comprises of a data repository that is configured to store the reference mathematical feature set and the identification key and a processor operatively communicating with the interface. The processor is configured to translate the naturally encrypted feature set received by the interface into a sample mathematical feature set. The processor further configured to compare the sample mathematical feature set with the reference mathematical feature set for the product stored in the data repository and authenticates the product on a successful match.

WO 2011/077459 A2

A METHOD OF EXTRACTING NATURALLY ENCRYPTED FEATURES FROM A NATURAL SURFACE OF A PRODUCT

FIELD OF THE INVENTION

The invention relates to a method of generating an identifier for any subject including a product, or an object, or a document, or a label or anything having unique microscopic imperfection present on its surface.

BACKGROUND

In today's commercial world, consumers, businesses, government bodies, etc. require information relating to the origin, and/or authenticity of a large variety of goods, properties and also identify people using the documents they carry. Consumers, manufacturers, suppliers, distributors, retailers, and others in the supply chain of goods can benefit from irrefutable assurances that the goods are genuine, and has not been introduced from illegitimate channels and/or adulterated or diverted from legitimate points in supply chain. Uniquely and positively identifying documents, identity cards, commercial products, etc has become very important.

In the present scenario, counterfeit goods are manufactured, distributed, and sold in direct competition with the authentic goods. Counterfeiting, has reached pandemic proportions worldwide, particularly in the area of consumer goods including goods made from fabric, plastic, leather, metal, ceramic, and other goods. In the banking world, counterfeiting of financial instruments such as currency notes, credit/ debit cards, bank drafts, money orders, etc have also spread to a large extent. It is common for the counterfeit goods to be of high quality and closely resemble the genuine or authentic goods such that the consumers readily confuse the counterfeit goods with the genuine or authentic goods. Moreover, fake identities and identity theft also is becoming a menace to our society today.

Counterfeiters every year sneak high value fake goods onto the store shelves. Despite the use of barcodes, holograms and watermarks and other externally applied features on the product, any object or document to verify the product, any object identity or authenticity, counterfeiters still manage to copy and replicate the marks or symbols on the fake products or packaging.

Recently, several Material Surface Authentication techniques have been developed by some companies as a means of detecting counterfeit products and tracing the origin of these goods. However, most of these surface authentication techniques require new equipments and products which employ non-standard methods which failed in the market place because of the process complexity and cost of implementation. Techniques which required adding taggants or expensive chemical or magnetic encoding also failed to succeed because of changes required in product packaging lines and prohibitive cost of authenticating devices. Some Surface authentication techniques use laser to scan the surface of a product to record a unique signature.

A line scanner is used in this kind of surface authentication used laser LEDs to scan a product using line scan to determine the authenticity of the product. The line scanners are stationary in nature, so moving a bulky product to the line scanner may be a tedious task. The scanner requires the product to have a flat surface to be able to scan. So, the line scanner is not able to scan a product without a flat surface. Moreover, the line scanner will scan the entire product having a flat surface line by line to trace the signature, which may be time consuming.

Furthermore, when large number of signatures are stored on a database, to trace and track one signature from millions of stored signature becomes a computing challenge and does not scale up in large commercial implementations.

SUMMARY

An authentication system for authenticating a product is disclosed. The product comprises of an identification key marked thereon and has a linked reference mathematical feature set. The reference mathematical feature set is obtained by capturing a microscopic image of a specific area on the surface of the product identifying surface imperfections present on the surface of the product. The surface imperfections forms a naturally encrypted feature set for the product that is translated into the reference mathematical feature set serving as an electronic signature for the product. The authentication system comprises of an interface that is configured to receive a microscopic image of a specific area on the surface of the product including a naturally encrypted feature set of the product. The authentication system also comprises of a data repository that is configured to store the reference mathematical feature set and the identification key and a processor operatively communicating with the interface. The processor is configured to translate the naturally encrypted feature set received by the interface into a sample mathematical feature set. The processor further configured to compare the sample mathematical feature set with the reference mathematical feature set for the product stored in the data repository and authenticates the product on a successful match.

A method of generating an identifier for a product is also disclosed. The method comprises of marking the product with an identification key and capturing a microscopic image of a specific area on the surface of the product. The microscopic image identifies surface imperfections present on the surface of the product. The surface imperfections forms a naturally encrypted feature set for the product. The method further comprises of translating the naturally encrypted feature set into a reference mathematical feature set serving as an electronic signature for the product and linking the reference mathematical feature set to the identification key of the product.

A method of authenticating a product is also disclosed. The product comprises of an identification key marked thereon and has a linked reference mathematical feature set. The reference mathematical feature set is obtained by capturing a microscopic image of a specific area on the surface of the product identifying surface imperfections present on the surface of the product. The surface imperfections forms a naturally encrypted feature set for the product that is translated into the reference mathematical feature set serving as an electronic signature for the product. The method comprises of scanning the specific area on the surface of the product and capturing a sample microscopic image of the specific area. The microscopic image identifying surface imperfections present on the surface of the product. The method further comprises of identifying the naturally encrypted feature set for the product from the microscopic image and translating the naturally encrypted feature set into a sample mathematical feature set. The method further comprises of comparing the sample mathematical feature set with the reference mathematical feature set for the product and authenticating the product on a successful match.

BREIF DISCRIPTION OF DRAWINGS

The following is a brief description of the preferred embodiments with reference to the accompanying drawings. It is to be understood that the features illustrated in and described with reference to the drawings are not to be construed as limiting of the scope of the invention. In the accompanying drawings

Figure 1 illustrates a schematic diagram of a wireless device in communication with an authentication system in accordance with an embodiment of the invention.

DETAIL DESCRIPTION OF THE INVENTION

It will be understood by those skilled in the art that the foregoing objects and the following description of the nature of invention are exemplary and explanatory of the invention and are not intended to be restrictive thereof.

For the purpose of promoting an understanding of the principles of the invention, reference will now be made to various alternative embodiments and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended, such alterations and further modifications in the illustrated method, and such further applications of the principles of the invention as illustrated therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

It will be understood by those skilled in the art that the following description is exemplary and explanatory of the invention and are not intended to be restrictive thereof.

Many of the functional units described in this specification have been labelled as modules, in order to more particularly emphasize their implementation independence. For example, a module may be implemented as a hardware circuit comprising custom very large scale integration circuits or gate arrays, off-the-shelf semiconductors such as logic, chips, transistors, or the other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices or the like.

Modules may also be implemented in software for execution by various types of processors. An identified module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions which may, for instance, be organised as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations

which, when joined together, comprise the module and achieve the started purpose for the module.

Indeed, a module of executable code could be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices. Similarly, operational data may be identified and illustrated herein within modules, and may be embodied in any suitable form and organised within any suitable type of data structure. The operational data maybe collected as a single data set, or may be distributed over different locations including over different member disks, and may exist, at least partially, merely as electronic signals on a system or network.

Reference throughout this specification to "one embodiment" "an embodiment" or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrase "in one embodiment", "in an embodiment" and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

In the context of specification:

A barcode is an optical machine-readable representation of data on a product.

ID barcode represents data in the form of parallel lines and the spacing between the parallel lines.

2D barcode represents data in the form of an image containing squares, dots, hexagons and other geometric patterns within the image.

Holograms refers to commercial available 2D and 3D black and white and color holograms and optically programmed sensors which can change optical and visual properties based on light, moisture, or other chemicals coming in contact with this sensor

RFID (Radio Frequency Identification) refers to tags incorporated in a product to identify and trace the product using radio waves.

NFC (Near Field Communication) is a short-range high frequency wireless communication technology which enables the exchange of information between devices within a small area.

The invention relates to a method of generating an identifier for any subject including a product, or an object, or a document, or a label or anything having unique microscopic imperfection present on its surface.

The invention also relates to a method of authenticating any subject based on its unique microscopic imperfection present on its surface including any product or any object or any document by scanning a specific marked area on a surface to verify the authenticity of the product or object or document's identity by extracting what is called the naturally encrypted feature set based thereon and carrying out the said positive authentication based thereon.

According to an aspect of the invention, the product or object includes a self-identifying feature set capable of uniquely identifying the product. The self-identifying feature set includes an identification key. According to a specific example of the invention, the self-identifying feature set is a barcode and the identification key is a barcode number.

More specifically, the method of generating an identifier for a product or object comprises of extracting a naturally encrypted feature set from a specific marked area of the subject surface which can be the said specific marked area of the product, object, document or packaging of the product. The specifically marked area can be created by printing, coating, painting or any other surface treatments used in the packaging or manufacturing industry.

According to an aspect of the invention, the method of generating an identifier for a product or object is based on its unique and distinctive surface material matrix that comprises of selecting a specific marked area on the said subject surface comprising of the microscopic

imperfections and capturing a high resolution microscopic image of the specific marked area. A naturally encrypted feature set is extracted from the microscopic image of the product, object or document surface. Further, the naturally encrypted feature set is translated into an electronic signature comprising of a reference mathematical feature set. The reference mathematical feature set is linked to the identification key and the reference mathematical feature set and the identification key are stored into a data repository.

According to an embodiment of the invention, the naturally encrypted feature set is translated into a reference mathematical feature set by representing the naturally encrypted feature set by its mathematical coefficients.

According to an embodiment of the invention, the naturally encrypted feature set is translated into a reference mathematical feature by modifying the mathematical coefficients representing the naturally encrypted feature set with a unique code, i.e., an algorithm.

According to an embodiment of the invention, mathematical feature sets can be defined based on the microscopic image extracted from the product. Standard and non standard pattern recognition algorithms, identified geometric objects like lines, curves, polygons, their polynomial equations, coefficients, eigen values, vectors, matrix representations, various mathematical transformations performed on the data, image processing and other image transformation functions, etc can be performed on extracted image which can create a superset mathematical model or a mathematic equivalent of the image. This mathematical model can also be a used optionally to recreate the image using reverse transformation methods. The objective of creating this mathematic feature set is to reduce the amount of data or data objects transmitted in business transactions using the identifier or secured element for any commercial or business application software. As these mathematic feature set or data is created from natural material matrix patterns encapsulating natural disorders, there are no logical correlations or patterns to be

identified by anyone recording or studying this data in transit on the internet or intranet. For this reason, this data can be considered a natural encrypted data set, which cannot be deciphered for recognizing or duplicating commercial authentication or verification done through any open network communication channels. This naturally encrypted feature set can only be recognized by the authorized feature recognition software created by an authorized legal entity. Moreover, all natural patterns are very random and based on the numerous mathematical feature sets available to be utilized, it is virtually impossible to duplicate or mimic an identifier or secured element or its mathematic equivalent created here.

According to an embodiment of the invention, the reference mathematical feature set uniquely identifies the naturally encrypted set from the microscopic image.

According to another aspect of the invention, the method of authenticating a product or object comprises of scanning the specified marked area on the surface again and capturing a sample microscopic image of the selected marked area. A set of naturally encrypted feature set is extracted from the sample microscopic image. The naturally encrypted feature set is translated into an electronic signature that comprises of a sample mathematical feature set.

Further, the reference mathematical feature set (which was already stored in the data repository) is extracted from the data repository and matched with the sample mathematical feature set (which is just generated) and on a successful match the product or object is authenticated.

The identification key linked to a reference mathematical feature sets may be electronically catalogued for easy searches in the data repository.

According to an embodiment of the invention, the naturally encrypted feature set created algorithmically on the wireless scanning device or PDA or computer is naturally protected from anybody intercepting this data as without clear knowledge of the algorithms used, and this data

has no meaning for anyone. In the event that algorithm is known or data set is duplicated the so created identity will not match the naturally encrypted feature set extracted from the natural surface due to inherent disorder in a composite material.

Preferably for the purpose of such authentication the microscopic image thus obtained of the specific area may be recorded in a data repository such as those residing on the scanner, PDA or computer or server.

According to an embodiment of the invention, each naturally encrypted feature set is unique, even for the individual products from the same production line, due to the unique microscopic random patterns formed during manufacturing the product.

According to an embodiment of the invention, the specific marked area may be on the product, object or document surface or on the label attached to the product, any object or document or on any of the packaging of the product.

According to an embodiment of the invention, the identification key for the reference mathematical feature set may include a serial number. The serial number may be stored in the data repository or physically printed on the product, object, document or label affixed on it

According to an embodiment of the invention, the method relates to capturing the natural encrypted feature set from a microscopic image of the specific marked area on the product, any object or document surface without applying any external material identifiers. The products being protected by the proposed method do not need any alteration or additional holograms, or electronic chips or exotic ink or specialized printing process for identification.

Figure 1 illustrates a Wireless Device 100 and an Authentication System 102 in accordance with an embodiment of the invention. The Wireless device 100 includes a Scanner Module 104 and a Wireless Module 106. The authentication system 102 includes a wireless

Interface 108, a Processor 110 and a Data Repository 112. The scanner Module 104 of the wireless device 100 may be directly connected to the Authentication system 102.

The scanner Module 104 is configured to capture a microscopic image of a selected marked area and is further configured to extract a naturally encrypted feature set from the microscopic image. In addition, the scanner module 104 may also extract any identification key from the product.

The wireless communication Module 106 is configured to transmit the naturally encrypted feature set and the identification key to an authentication system 102 over a wireless medium. The wireless communication Module 106 also configured to receive signals from the authentication system 102 and transmit to scanner Module 104.

The wireless interface 108 of the authentication system 102 is configured to communicate with the wireless device 100 and further configured to receive information from the wireless device like naturally encrypted feature set and identification key.

The processor 110 of the authentication system 102 is configured to translate the naturally encrypted feature set into an electronic signature comprising a sample mathematical feature set. The processor further configured to retrieve the reference mathematical feature set from a data repository and matching the reference mathematical feature set with the sample mathematical feature set. The processor is further configured to transmit an encrypted signal to the wireless device for authentication of the product on a successful match.

The data repository 112 is configured to store the reference mathematical feature set and the identification key. The data repository is further configured to locate the reference mathematical feature set with the identification key.

According to a specific example of the invention, a barcode is placed by the manufacturer on the product, any object or document while packaging of the product or printing labels for the

product. The barcode may be a ID barcode or a 2D barcode. Typically, 2D barcode is preferred over a ID barcode as there are clearly marked areas within the 2D barcode to capture the material matrix image. Here, barcode is the self-identifying feature set and the barcode number is the identification key.

Further, a wireless device 100 is used to scan the surface of the barcode positioned on the product, any object or document surface. Every barcode or product or product packaging will encompass several random microscopic imperfections or patterns present on the surface or just below the surface of the barcode. A specific marked area on the barcode (generally, but not limited to, up to or more than 2 mm * 2 mm = 4 sq mm in size) is selected. The specific marked area is zoomed using the scanning Module 104 present on the wireless device 100 and a microscopic image is taken. The scanning Module 104 may have a microscopic camera irradiated by laser or ultraviolet light or other approved radiations at a high resolution level. This scanner Module 104 has the capability of zooming into extracted features and particles size from about 50 to 4000 nanometre in the surface of the product, any object or document. The scanner Module 104 extracts a naturally encrypting feature set from the image.

Further, the wireless communication Module 106 transmits the naturally encrypted feature set and the identification key to an Authentication System 102 over a wireless medium. The interface 108 of the authentication system 102 receives the information from the wireless device i.e., naturally encrypted feature set and identification key and passed to the processor for further processing.

The processor 110 translates the naturally encrypted feature set into an electronic signature comprising a reference mathematical feature set. The processor 110 links the reference mathematical feature set with the identification key and stores them in the data repository 112.

According to an aspect of the invention, for authentication of a product, the processor 110 receives another set of naturally encrypted feature set of the specific market area from a user and translates it to acquire a sample mathematical feature set. The processor 110 further retrieves the reference mathematical feature set from the data repository 112 and matches that with the sample mathematical feature set just acquired. The processor 110 further transmits an encrypted signal to the wireless device for authentication the product if a successful match is obtained.

According to an embodiment of the invention, the reference mathematical feature set may be recorded on the data repository 112 of the Authentication System 102 for all future authentication of this signature and positively establishing the identify of any object or product.

Advantageously, according to an embodiment of the invention, when the microscopic image is captured from within the barcode then it is unique even from the similar barcodes being manufactured on the same production line, due to the random microscopic imperfections or patterns or disorders formed are completely different for each of the barcode, holograms, RFID or NFC tags or labels during the manufacturing process.

According to an embodiment, an algorithm may be used for matching the sample mathematical feature set with a previously stored reference mathematical feature set on the Authentication System 102. The algorithm may further reduce the size of the natural encrypted feature set from several hundred KB to up to (but not limited to) 2 KB or the less than 2KB for easy communication over a network and other purposes.

According to an embodiment, the above method of scanning the surface and recoding a microscopic image to verify the authenticity of a product, any object or document can also be implemented on existing object identifiers such as a RFID tag, NFC tag or holograms or any other tags or labels for identifying products.

According to an embodiment, the wireless device 100 is in the form of a mobile/fixed device that works as a barcode reader with the built in capability to capture the microscopic image and extract the natural encrypted feature set. The wireless device 100 may have a built in barcode sensors as well as surface matrix signature sensors capturing an image from the unique location embedded in the barcode itself. The wireless device 100 may comprise of a processor or processors to translate the image into the natural encrypted mathematical-- feature sets which is unique to that particular barcode on the product. The material matrix scanner is configured to have a magnification range of (but not limited to) lOOx to lOOOOx. Additionally the material matrix scanner is configured with all the capabilities of a standard mobile device like GSM, GPRS, GPS, Wi-Fi, Blue Tooth, USB, etc.

According to an alternative embodiment of the invention, the wireless device 100 may comprise of a processor or processors to translate the natural encrypted mathematical feature sets into electronic signature comprising of a reference mathematical feature set which is unique to that particular barcode on the product. The wireless device 100 may also comprise of a data repository that may store the reference mathematical feature set.

SPECIFIC EMBODIMENTS ARE DESCRIBED BELOW

A method of generating an identifier for a product comprising marking the product with an identification key, capturing a microscopic image of a specific area on the surface of the product, the microscopic image identifying surface imperfections present on the surface of the product, the surface imperfections forming a naturally encrypted feature set for the product, translating the naturally encrypted feature set into a reference mathematical feature set serving as an electronic signature for the product and linking the reference mathematical feature set to the identification key of the product.

Such method(s), wherein storing the reference mathematical feature set and the identification key into a data repository.

Such method(s), wherein translating the naturally encrypted feature set includes representing the naturally encrypted feature set by its mathematical coefficients.

Such method(s), wherein translating the naturally encrypted feature set further comprises modifying the mathematical coefficients with a unique code.

Such method(s), wherein the identification key is a barcode or a serial number.

Such method(s), wherein the specific area is marked on the product.

Such method(s), wherein the specific area is the area of the identification key marked on the product.

FURTHER SPECIFIC EMBODIMENTS ARE DESCRIBED BELOW

A method of authenticating a product, the product comprising an identification key marked thereon and having a linked reference mathematical feature set, the reference mathematical feature set obtained by capturing a microscopic image of a specific area on the surface of the product identifying surface imperfections present on the surface of the product, the surface imperfections forming a naturally encrypted feature set for the product that is translated into the reference mathematical feature set serving as an electronic signature for the product; the method comprising scanning the specific area on the surface of the product and capturing a sample microscopic image of the specific area; the microscopic image identifying surface imperfections present on the surface of the product, identifying the naturally encrypted feature set for the product from the microscopic image and translating the naturally encrypted feature set into a sample mathematical feature set, comparing the sample mathematical feature set with the

reference mathematical feature set for the product and authenticating the product on a successful match.

Such method(s), wherein the reference mathematical feature is stored in a data repository and comparing the sample mathematical feature set with the reference mathematical feature set for the product includes retrieving the reference mathematical feature from the data repository.

Such method(s), wherein the reference mathematical feature is retrieved from the data repository by its identification key.

FURTHER SPECIFIC EMBODIMENTS ARE DESCRIBED BELOW

An authentication system for authenticating a product, the product comprising an identification key marked thereon and having a linked reference mathematical feature set, the reference mathematical feature set obtained by capturing a microscopic image of a specific area on the surface of the product identifying surface imperfections present on the surface of the product, the surface imperfections forming a naturally encrypted feature set for the product that is translated into the reference mathematical feature set serving as an electronic signature for the product, the authentication system comprising an interface configured to receive a microscopic image of a specific area on the surface of the product including a naturally encrypted feature set of the product or a naturally encrypted feature set of the product, a data repository configured to store the reference mathematical feature set and the identification key and a processor operatively communicating with the interface and configured to translate the naturally encrypted feature set received by the interface into a sample mathematical feature set; the processor further configured to compare the sample mathematical feature set with the reference mathematical feature set for the product stored in the data repository and authenticate the product on a successful match.

Such authentication system(s), wherein the interface includes a wireless interface configured to communicate with a wireless device and receive the naturally encrypted feature set from the wireless device.

Such authentication system(s), wherein the processor is further configured to transmit an encrypted signal for authentication of the product after a successful match.

Such authentication system(s), further configured to generate an identifier for a product having an identification key marked thereon by translating a naturally encrypted feature set into a reference mathematical feature set serving as an electronic signature for the product; and linking the reference mathematical feature set to the identification key of the product.

Such authentication system(s), further configured to store the reference mathematical feature set and the identification key in the data repository.

INDUSTRIAL APPLICABILITY

The disclosed method provides high level of security and stringent requirements for products, objects or documents with an authenticity assurance without the expense of altering the manufacturing process or product packaging. The method works at the microscopic level and is robust enough to deal with rough everyday handling of the product.

There is no way of duplicating the surface material matrix structure i.e., the unique microscopic imperfections present on the surface of the product and the image captured of the surface. Even repetitive manufacturing process will produce a different result every time due to the random surface patterns formed during manufacturing on the subject such as any product, object or document and the material matrix image taken of the specific marked area of the subject such as the product; object or document cannot be duplicated or matched with any existing images

The invention may be used in existing manufacturing processes without issuing or changing the manufacturing or packaging process.

It would be thus possible by way of the present invention to provide a method for positive identification and authentication of any subject such as any product, object or documents securely without the possibility of duplication or counterfeiting by any unauthorized person at any point in the supply chain so that the as made quality/value of original brand is ensured to the end user. The method can be implemented involving simple and user friendly gadgets. Importantly, the method of the invention is capable of establishing and authorizing each and every product utilizing the same microscopic random imperfection or disorder since the manufacturing process itself provides such unique features to the surface of products or documents. The method is applicable for a wide range of materials and everything from metals, ceramics, plastic, paper, etc. with equal accuracy and security for authentication purpose. Advantageously, the method of the invention is adapted to provide high level of security and authenticity assurance for any subject involving a material matrix without the expense of altering the manufacturing process or product packaging and including providing means for authentication of any financial instruments, fully secured against any counterfeit/duplication to thereby ensuring large scale commercial application of the method of authentication of any subject based on its unique and distinctive surface material matrix for a number of application in industry/commercial house or banking/financial sector, favoring substantial savings on losses both financial and reputation due to counterfeit and spurious products.

While specific language has been used to describe the invention, any limitations arising on account of the same are not intended. As would be apparent to a person in the art, various working modifications may be made to the method in order to implement the inventive concept as taught herein.

We claim:

1. A method of generating an identifier for a product comprising:
   - marking the product with an identification key;
   - capturing a microscopic image of a specific area on the surface of the product, the microscopic image identifying surface imperfections present on the surface of the product, the surface imperfections forming a naturally encrypted feature set for the product;
   - translating the naturally encrypted feature set into a reference mathematical feature set serving as an electronic signature for the product; and
   - linking the reference mathematical feature set to the identification key of the product.

2. A method of generating an identifier for a product as claimed in claim 1 wherein storing the reference mathematical feature set and the identification key into a data repository.

3. A method of generating an identifier for a product as claimed in claim 1 wherein translating the naturally encrypted feature set includes representing the naturally encrypted feature set by its mathematical coefficients.

4. A method of generating an identifier for a product as claimed in claim 3 wherein translating the naturally encrypted feature set further comprises modifying the mathematical coefficients with a unique code.

5. A method of generating an identifier for a product as claimed in claim 1 wherein the identification key is a barcode or a serial number.

6. A method of generating an identifier for a product as claimed in claim 1 wherein the specific area is marked on the product.

7. A method of generating an identifier for a product as claimed in claim 5 wherein the specific area is the area of the identification key marked on the product.

8. A method of authenticating a product, the product comprising an identification key marked thereon and having a linked reference mathematical feature set, the reference mathematical feature set obtained by capturing a microscopic image of a specific area on the surface of the product identifying surface imperfections present on the surface of the product, the surface imperfections forming a naturally encrypted feature set for the product that is translated into the reference mathematical feature set serving as an electronic signature for the product; the method comprising:

scanning the specific area on the surface of the product and capturing a sample microscopic image of the specific area; the microscopic image identifying surface imperfections present on the surface of the product;

identifying the naturally encrypted feature set for the product from the microscopic image and translating the naturally encrypted feature set into a sample mathematical feature set;

comparing the sample mathematical feature set with the reference mathematical feature set for the product; and

authenticating the product on a successful match.

9. A method of authenticating a product as claimed in claim 8 wherein the reference mathematical feature is stored in a data repository and comparing the sample mathematical feature set with the reference mathematical feature set for the product includes retrieving the reference mathematical feature from the data repository.

10. A method of authenticating a product as claimed in claim 9 wherein the reference mathematical feature is retrieved from the data repository by its identification key.

11. An authentication system for authenticating a product, the product comprising an identification key marked thereon and having a linked reference mathematical feature set, the reference mathematical feature set obtained by capturing a microscopic image of a specific area on the surface of the product identifying surface imperfections present on the surface of the product, the surface imperfections forming a naturally encrypted feature set for the product that is translated into the reference mathematical feature set serving as an electronic signature for the product, the authentication system comprising:

- an interface configured to receive a microscopic image of a specific area on the surface of the product including a naturally encrypted feature set of the product or a naturally encrypted feature set of the product;
- a data repository configured to store the reference mathematical feature set and the identification key; and

- a processor operatively communicating with the interface and configured to translate the naturally encrypted feature set received by the interface into a sample mathematical feature set; the processor further configured to compare the sample mathematical feature set with the reference mathematical feature set for the product stored in the data repository and authenticate the product on a successful match.

12. An authentication system as claimed in claim 11 wherein the interface includes a wireless interface configured to communicate with a wireless device and receive the naturally encrypted feature set from the wireless device.

13. An authentication system as claimed in claim 11 wherein the processor is further configured to transmit an encrypted signal for authentication of the product after a successful match.

14. An authentication system as claimed in claim 11 further configured to generate an identifier for a product having an identification key marked thereon by translating a naturally encrypted feature set into a reference mathematical feature set serving as an electronic signature for the product; and linking the reference mathematical feature set to the identification key of the product.

15. An authentication system as claimed in claim 14 further configured to store the reference mathematical feature set and the identification key in the data repository.

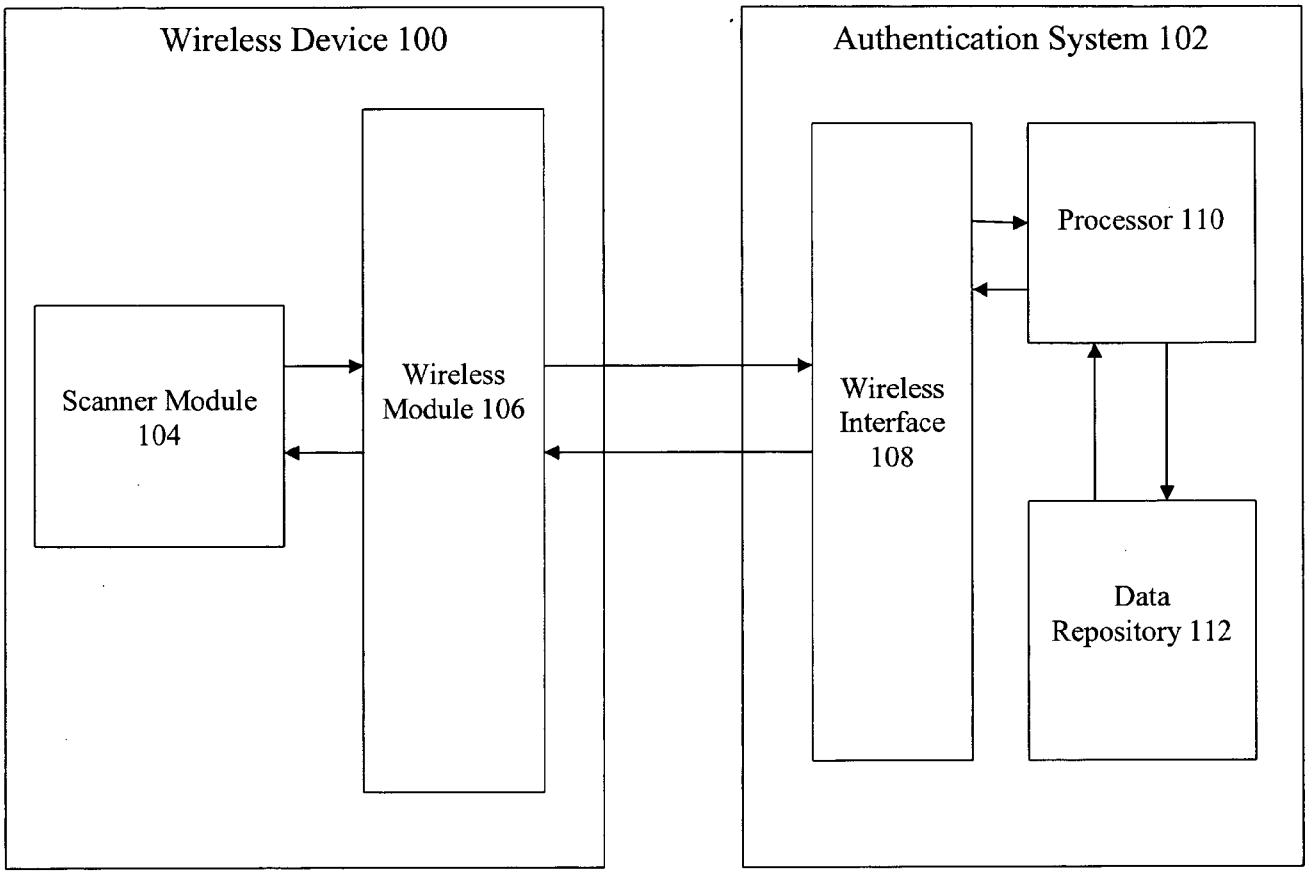

Wireless Device 100
Authentication System 102
Scanner Module 104
Wireless Module 106
Wireless Interface 108
Processor 110
Data Repository 112

Figure 1