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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 April 2013 (11.04.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/051019 A1

(51) **International Patent Classification**:
G07C 9/00 (2006.01) *G06Q 20/00* (2012.01)
G06K 19/00 (2006.01)

(21) **International Application Number**:
PCT/IN2012/000433

(22) **International Filing Date**:
18 June 2012 (18.06.2012)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
1763/MUM/2011 17 June 2011 (17.06.2011) IN

(72) **Inventor; and**
(71) **Applicant** : **GHATALIA, Jinav Sandeep** [IN/IN]; 205, The Blossom Chs Ltd., Adarsh Dugdhalaya Lane, Marve Road, Malad (West), Mumbai 400064, Maharashtra (IN).

(72) **Inventors**: **GHATALIA, Sandeep Harshad**; 205, The Blossom Chs Ltd., Adarsh Dugdhalaya Lane, Marve Road, Malad (West), Mumbai 400064, Maharashtra (IN). **DESAI, Neetin Shivajirao**; B-19, Flat No: 6, Kendriya Vihar, Sector 11, Kharghar, Navi Mumbai 410210, Maharashtra (IN). **THAKAR, Devang Kaushik**; 5/52, Om Sai Pratibha Chs, Gawde Nagar, Rawalpada, Dahisar (East), Mumbai 400068, Maharashtra (IN).

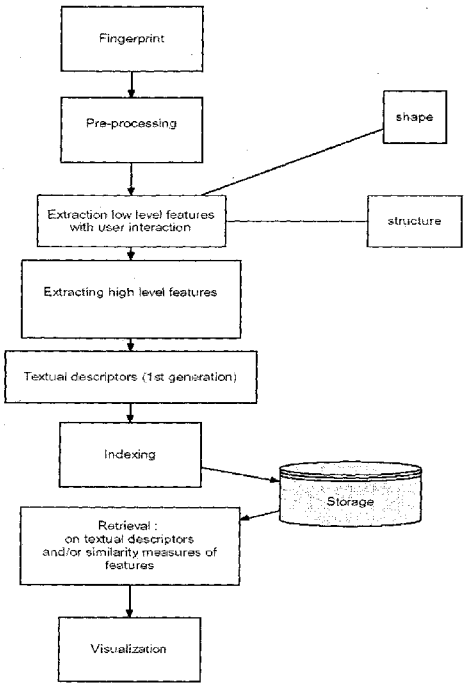
(74) **Agent**: **POONAM, Dhake Kolhe**; 7/5/6 Hill Crest Society, Bhavani Nagar, Near Vijay Nagar, Marol Maroshi Road, Andheri East, Mumbai 400059 (IN).

(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, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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,

[Continued on next page]

(54) **Title**: EVOLVED BIOMETRIC SYSTEM WITH ENHANCED FEATURE AND METHOD FOR THE SAME



(57) **Abstract**: Thus according to the basic aspect of the present invention there is provided an evolved biometric authentication system providing more than 99% accuracy and is precise as it uses multiple biometrics to identify and authenticate a live individual. This evolved biometric system provides real time verification and authentication. The biometrics characteristic data obtained from the individual at the time of identification and authentication is compared with the previously registered biometrics characteristic data at the time of user registration, said system comprises of multiple biometric instruments, a processing unit, a database, and means of access (output), and the method of biometric identification using multimodal biometric authentication device for authenticating a user enrolled/captured biometric and its means of access (output) with more than 99% accuracy, where initially characteristics image of a biometric feature an individual are captured, then the captured image/information undergoes process of converting, encrypting, and storing the above images in a computer/central processing unit with the help of software program in an integrated method which avoids overlapping of the multiple images an Individual as well as different individuals enabling easy, concise and fast retrieval of the desired biometric data pertaining to an individual. Further this captured data/image/information is matched or compared and verified with the enrolled data to identify or authenticate his or her identification. Then the means of access (output) is used as application in various field as token based identification system or knowledge based identification system.

WO 2013/051019 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TITLE OF THE INVENTION: "EVOLVED BIOMETRIC SYSTEM WITH ENHANCED FEATURE AND METHOD FOR THE SAME"

FIELD OF THE INVENTION:

The present invention relates to an evolved biometrics system with enhanced feature and method for the same. In particularly it relates to the authentication and verification of the identity of users in real time with live biometrics using one or more biometric modalities with maximum accuracy and precision. The data transfer is secured using different encryption techniques.

BACKGROUND OF INVENTION:

This invention relates generally to authenticating individuals and more particularly to a method and system for biometric authentication. Generally biometric authentication systems are used to identify and verify the identity of individuals and are used in many different contexts such as verifying the identity of individuals entering a country using electronic passports. Biometric authentication systelms have also been known to verify the identity of individuals and have now been deployed in various commercial, civilian, & forensic set-ups as a means of establishing & confirming identity like using driver's licenses, traveler's tokens, employee identity cards and banking cards.

In recent years, biometric authentication using biometric information is widely used as means for authenticating. Biometric are generally classified as stable and unstable biometric. Biometric which remain stable for longer time and do not vary occasionally are considered as stable biometric not limiting to for e.g. Fingerprints Scan, Palm, Retina, Iris Patterns, Signature, DNA Sequence, face, lips etc. Whereas in case of unstable biometric they frequently vary depending on emotion and surrounding/environment for example not limiting to Voice, Gait, Foot Pressure, Weight, Bodypressure, Heart beat scan, Nail, perspiration and dental pattern etc. Known biometric authentication system search engines generally identify individuals using biometric feature templates derived from raw biometric data captured from individuals. Biometric systems has the means to access control (output) include token-based identification systems such as driver's license or passport and knowledge-based identification systems such as password or personal identification number. Examples of available biometric

information include capture – image information obtained by capturing images of body parts, such as Fingerprints Scanner, Palm, Retina & Iris Patterns, Digital Signature, DNA Sequence and Voice print information obtained by recording voice.

Specifically a biometric feature template derived from biometric data captured from an individual during authentication is compared against a database of previously derived biometric feature templates and the identity of the individual is verified upon determining a match between one of the stored biometric feature templates and the biometric feature template derived during authentication However comparing biometric feature templates against a database biometric feature templates may place substantial demands on computer system memory and processing which may result in unacceptably long authentication periods. Moreover such known biometric authentication works in a multi-stages process that consists of the following steps: Enrollment, Processing, Extraction, Comparison and Matching data.

Most biometric systems deployed in real-world applications are unimodal, i.e. they rely on the evidence of a single source of information eg. single or multiple fingerprints or face or iris or retina or palm. But the 'unimodal' or 'single mode' biometric solutions have limitations in terms of accuracy and susceptibility to spoofing. For example according to the National Institute of Standards and Technology (NIST/USA) approximately two percent of the population does not have a legible fingerprint and therefore can't be enrolled into a finger print biometric system. Multiple problems such as noisy data, intra-class variations, interclass similarities, non-universality and spoofing leads to considerably high False Acceptance Rates (FAR) and low False Rejection Rates (FRR), limited indiscrimination capabilities, and lack of desired performances. In Indian patent No IN236304 by Multimedia Glory describe a method of identifying an individual using biometric data selected from one or more of the following; finger print, palm print, iris or any or any other biometric data. The relativity of each significant feature in relation to other feature is computed. The relativity is combined to obtain a classification code. The classification code and the biometric data obtained are encrypted. Then the encrypted data is stored. The biometrics data is verified against the earlier stored biometrics data of the same individual.

WO2008121730 discloses a method and/or system for identity management and authentication of examination candidates by, for example, capturing biometric data and identification information from an examination candidate and storing the data and information in a database. The method and/or system includes, for example, capturing biometric data from an individual at a later time for comparison with data stored in the database, and which allows authentication of the individual after determining that the biometric data matches the previously stored data and the individual matches the previously stored information.

Multimodal biometrics uses a combination of recognition technologies to compare the identity of an individual. If one of the technologies fails for any reason, the system can still use another one or more of them to provide accurate identification of an individual. Better accuracy can be naturally obtained by having a large number of biometric scanning systems. Additions of methods like DNA Sequencing, though it is time consuming would offer additional benefits. However it has been observed that integrating a large number of independent biometric systems offer certain technological challenges and hence are rarely attempted to integrate them.

WO2005008210 discloses a system and method for performing security access control based on modified biometric data. Here enhanced security and accuracy is obtained through recognition of one or more distorted biometrics. The method includes detecting a distorted biometric , comparing the distorted biometric, to one or more distortion patterns in storage unit, and controlling access to a restricted item based on results of the comparison. The biometric may be an eye pattern, a fingerprint or palm print, a voice print, a handwriting sample, a DNA sample, a facial image, or any other type of characteristic or behavioral attribute of a person. The biometric may be distorted in any one of a variety of ways for comparison to previously enrolled biometrics which have been distorted using the same or similar element. A system and program embodied within a computer-readable medium performs the steps of the method.

With the existing multimodal biometric system there is a requirement of system which could provide a real analysis and live biometric. There is a need of a system which could transfer data with high security avoiding data theft, plodder, and mutilate. There is a need of system which could authenticate the status of identified individual whether dead or alive. Time consumption is more in conventionally know biometric system to achieve the accuracy, hence there is a need of an system which could provide high accuracy as that of more than 99% in very less time with less noise. As there is large number of data need to be stored, hence a system that could store large number of data in considerable small space is required. Not limiting the above requirement/embodiment there is a need of a system which could overcome all the above drawbacks. Considering the above drawbacks, a biometric system and method for the same is evolved to overcome the same not limiting to the below mentioned embodiments.

OBJECTIVES OF THE INVENTION

A primary object of the present invention is to develop multimodal biometric device with high accuracy and precise result.

Another object of the invention is to provide a highest level security system.

Another object of the invention is to provide an integrated or synchronized biometric system.

Another object of the present invention is to develop the multimodal biometric which captures various / multiple biometric with in fraction of seconds / less time and less sensor noise.

Yet another object of the invention is to provide a multimodal biometric which is easy to operate and yet economic.

A further object of the present invention is to provide a multimodal biometric device which could save the collected data in compact space (fewer MB) in lesser time.

Another object of the invention is to provide a multimodal biometric device which can reduce identity theft.

Another object of the invention is to provide a multimodal biometric device which has user friendly application.

Another object of the invention is to provide a multimodal biometric device which has highest level of security for the stored /enrolled data.

Another object of the invention is to provide a multimodal biometric device which could provide access to secured enrolled data across the globe.

Yet another object of the invention is to provide an evolved biometric system which does not interfere with the other working software in a computer/server system.

It is yet another object of the invention to provide an intelligent biometric system in which the capturing device is a programmable device with embedded software for enrolling and identifying the individual with available protocols and encoding and decoding data encapsulated within them.

SUMMARY OF THE INVENTION

Thus according to the basic aspect of the present invention there is provided an evolved biometric authentication system providing more than 99% accuracy and is precise as it uses multiple biometrics to identify and authenticate a live individual. This evolved biometric system provides real time verification and authentication. The biometrics characteristic data obtained from the individual at the time of identification and authentication is compared with the previously registered biometrics characteristic data at the time of user registration, said system comprises of multiple biometric instruments, a processing unit, a database, and means of access (output), and the method of biometric identification using multimodal biometric authentication device for authenticating a user enrolled/captured biometric and its means of access (output) with more than 99% accuracy, where initially characteristics image of a biometric feature an individual are captured, then the captured image/information undergoes process of converting, encrypting, and storing the above images in a computer/central processing unit with the help of software program in an integrated method which avoids overlapping of the multiple images an Individual as well as different individuals enabling easy, concise and fast retrieval of the desired biometric data pertaining to an individual. Further this captured data/image/information is matched or compared and verified with the enrolled data to identify or authenticate his or her identification. Then the means of access (output) is used as application in various field as token based identification system or knowledge based identification system.

BRIEF DRESCEIPTION OF DIGRAM:

The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate various exemplary embodiments of the present invention and together with the description , further serve to explain various principles and to enable a person skilled in the pertinent art to make and use the invention.

FIGURE 1 is a flow chart showing an exemplary embodiment of a working of the Multimodal Biometric.

FIGURE 2 is the flowchart showing of an exemplary embodiment of working of the finger scanner.

FIGURE 3 is the flowchart showing of an exemplary embodiment of a working of iris scanner.

FIGURE 4 is the flowchart showing of an exemplary embodiment of a working of the palm scanner.

FIGURE 5 is the flowchart showing of an exemplary embodiment of a working of face camera.

FIGURE 6 is the flowchart showing of an exemplary embodiment of a circuit used in multimodal biometric system.

DETAIL DESCRIPTION OF THE DIAGRAM:

FIGURE 1 is the working of multimodal biometric.

The biometric of an individual are captured using multiple biometric device. The said biometric are either captured simultaneously or are captured one after another. The multiple scanning instruments are used in combination or simultaneously are the biometric device used to capture biometric of individual are palm scanner, iris scanner, face scanner, voice scanner, figure scanner, DNA scanner, signature scanner. The captured data/image /information is then transferred to processing unit which is the hardware within a computer system which carries out the instructions of a computer program by performing the basic arithmetical, logical, and input/output operations of the system it is with a software component either as embedded in hardware or running thereon. The processed data is then stored in database which is an organized collection of data in digital form that supports processes requires running the information as required/commanded. The means of access (output) is token-based identification systems such as passport, driving license and/or knowledge-based identification systems such as password or personal identification number. Generally the means of access is an application used in day to day practice where identification is very important and avoids identity theft, where the application are not limited to examples like immigration industry, Identity or identification access to confidential

area/restricted area, insurance sector including both health and life insurance, Financial security includes online like trading site, banking site etc and offline both like credit card, debit card etc.

FIGURE 2 is the flowchart for working of the finger scanner.

The Finger Scanner a component of our Integrated or Synchronized system works as follows. The instrument consists of three parts: 1. The Instrument comprising of Light Emitting Sensor (LES), 2. Data Cables to connect as well as to transfer data / to or from the instrument to / from hardware 3. Software Programmer

Data cable is connected to finger scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software program and finger scanner are synchronized and integrated with each other so that they are compatible with each other.

The finger scanner is ready to capture images of fingers by a special camera, which provides required magnification and Light Emitting Sensor (LES). Finger of individual is rested on the scanner. The images of the ridges of the finger are captured. The captured images are stored in storage device in milliseconds. The Software converts the scanned image in to a big contour map or a coordinate system. The process of converting the image into a big contour map or a coordinate system, and the output generated is known as Templates. There are many Templates of an individual. All those Templates which belong to an individual are assigned a unique code either manually or automatically.

FIGURE 3 describes the working of iris scanner.

The Iris scanner as a component of our Integrated or Synchronized system works as follows.

1. The instrument comprising of a camera, 2. Data Cable to connect as well as to transfer data / to or from the instrument to / from hardware, 3. Software Programmer.

Data cable is connected to iris scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software

program and iris scanner are synchronized and integrated with each other so that they are compatible with each other. The iris scanner is ready to capture images of iris. To capture iris image it utilizes high resolution camera which provides required magnification. The images of eye iris are captured. The captured iris image is processed and stored in a storage device by Software. The iris images of both irises are stored in the database in the form of binary data with which a Unique Code (for left and right irises of an individual) is also assigned either manually or automatically.

FIGURE 4 describes the working of the palm scanner.

The Palm scanner as a component of our Integrated or Synchronized system works as follows. The instrument consists of three parts:

1. The Instrument comprising of Infra Red Sensor, 2. Data cable to connect as well as to transfer data / to or from the instrument to / from hardware, 3. Software Programmer.

Data cable is connected to palm scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software program and palm scanner are synchronized and integrated with each other so that they are compatible with each other.

The palm scanner is ready to capture images of left and right Palms. To capture image it utilizes a pattern image while radiating it with near-infrared rays. The deoxidized hemoglobin in the palm vein absorbs these rays, thereby reducing the reflection rate and causing the veins to appear as a black pattern. An individual will rests his or her palm on the scanner. The images of the veins of the palm are captured. The captured images are stored in storage device. software convert the scanned image and stores it in the database in the form of binary data with which a unique code is also assigned either manually or automatically.

FIGURE 5 describes the working of face camera.

The Face scanner as a component of our Integrated or Synchronized system works as follows. The instrument consists of three parts:

1. The instrument comprising of a camera, 2. Data Cable to connect as well as to transfer data / to or from the instrument to / from hardware, 3. Software Programmer.

Data cable is connected to face scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software program and face scanner are synchronized and integrated with each other so that they are compatible with each other.

The Face camera is ready to capture images of Face. To capture face image it utilizes web or normal resolution camera which provides required magnification. An individual is present in front of face camera. The two dimensional (henceforth referred as 2-D) image of face are captured. The captured images are stored in storage device. software convert the scanned image and stores it in the database in the form of binary data with which a unique code is also assigned either manually or automatically.

FIGURE 6 is the circuit used in multimodal biometric system.

The circuit comprises of IC's, resistors, capacitors.

DETAILED DESCRIPTION OF THE INVENTION:

The Evolved Multimodal biometrics technology utilizes a process for enrollment with the help of one or more biometric instruments either simultaneously or one after another which are:

1. Finger scanner, 2. Iris scanner, 3. Face Camera, 4. Palm scanner, 5. Signature recognizer etc

1. Working of the Finger Scanner

The Finger Scanner a component of our Integrated or Synchronized system works as follows. The instrument consists of three parts: 1. The Instrument comprising of Light Emitting Sensor (LES), 2. Data Cables to connect as well as to transfer data / to or from the instrument to / from hardware 3. Software Programmer

Data cable is connected to finger scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software program and finger scanner are synchronized and integrated with each other so that they are compatible with each other.

The finger scanner is ready to capture images of fingers by a special camera, which provides required magnification and Light Emitting Sensor (LES). Finger of individual is rested on the scanner. The images of the ridges of the finger are captured. The captured images are stored in storage device in milliseconds. The Software converts the scanned image in to a big contour map or a coordinate system. The process of converting the image into a big contour map or a coordinate system, and the output generated is known as Templates. There are many Templates of an individual. All those Templates which belong to an individual are assigned a unique code either manually or automatically.

Finger Scanner has two major functions:

1. Enrollment:- Collecting Biometric Data by capturing the biometric Feature (two thumbs and eight fingers) of an individual for enrollment.
2. Identification:- Verifying or Matching or Comparing the recently or newly collected biometric data by capturing the biometric feature (thumb or finger) of an individual with the stored Templates in the computers.

This finger scanner is based on a principle that is needs to complete its circuit. In this scanner electrons emitting from finger tips completes the circuit cycle, as the electrode is based on this principle. With this unique feature a dead person's finger cannot be identified as a dead human/animal finger does not contain set of electrons to complete the circuit where as in case of a live human, blood is continuously flowing and replenishment of electrons is continuously there hence the circuit is completed and the individual can be identified. Also fingerprints with contaminants like dust, grease, oil, water and other contaminants can be easily identified using this scanner. Bruised or injured finger, blood stained or dye stained finger can be identified easily.

2. Working of Iris Scanner:

The Iris scanner as a component of our Integrated or Synchronized system works as follows.

1. The instrument comprising of a camera, 2. Data Cable to connect as well as to transfer data / to or from the instrument to / from hardware, 3. Software Programmer Developed by us

Data cable is connected to iris scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software program and iris scanner are synchronized and integrated with each other so that they are compatible with each other. The iris scanner is ready to capture images of iris. To capture iris image it utilizes high resolution camera which provides required magnification. The images of eye iris are captured. The captured iris image is processed and stored in a storage device by Software. The iris images of both irises are stored in the database in the form of binary data with which a Unique Code (for left and right irises of an individual) is also assigned either manually or automatically. The storage process is being defined in Software.

Iris Scanner has two major functions:

1. Enrollment:- Collecting biometric data by capturing the biometric feature (left and right irises) of an individual for enrollment.
2. Identification:- Verifying or Matching or Comparing the recently or newly collected biometric data by capturing the biometric feature (either left or right iris) of an individual with the binary data stored in the database.

This iris scanner is able to capture iris through contact lens, coloured contact lens, spectacles and glares. The unique feature of this scanner is autodetection of the iris and automatic capture of the iris.

3. Working of Face:

The Face scanner as a component of our Integrated or Synchronized system works as follows. The instrument consists of three parts: 1. The instrument comprising of a camera, 2. Data cable to connect as well as to transfer data / to or from the instrument to / from hardware, 3. Software Programmer.

Data cable is connected to face scanner at one end and to hardware at other end. By using

graphical user interface enrollment and identification is done. The computer system, software program and face scanner are synchronized and integrated with each other so that they are compatible with each other.

The Face camera is ready to capture images of Face. To capture face image it utilizes web or normal resolution camera which provides required magnification. An individual is present in front of face camera. The two dimensional (henceforth referred as 2-D) image of face are captured. The captured images are stored in storage device. software convert the scanned image and stores it in the database in the form of binary data with which a unique code is also assigned either manually or automatically.

Face camera has two major functions:

1. Enrollment:- Collecting biometric data by capturing the biometric features (face) of an individual for enrollment.
2. Identification:- Verifying or Matching or Comparing the recently or newly collected biometric data by capturing the biometric feature (face) of an individual with the binary data stored in the database.

This face scanner has an auto-detection and lag detection property which will continuously scan the face either it is identified or unidentified. This face scanner detects face only if the eyes of the individual are available during scanning, this avoids the fraud causes by cheat using a similar look mask or by doing a plastic surgery resembling same individual face, as this scan requires eyes for scanning. Another unique feature of this scanner is it doesn't recognize 2-D 3-D virtual sized photographs of the same individual placed in if front of the camera.

4. Working of Palm Scanner:

The Palm scanner as a component of our Integrated or Synchronized system works as follows. The instrument consists of three parts:

1. The Instrument comprising of Infra Red Sensors, 2. Data cable to connect as well as to transfer data / to or from the instrument to / from hardware, 3. Software Programmer.

Data cable is connected to palm scanner at one end and to hardware at other end. By using graphical user interface enrollment and identification is done. The computer system, software program and palm scanner are synchronized and integrated with each other so that they are compatible with each other.

The palm scanner is ready to capture images of left and right Palms. To capture image it utilizes a pattern image while radiating it with near-infrared rays. The deoxidized hemoglobin in the palm vein absorbs these rays, thereby reducing the reflection rate and causing the veins to appear as a black pattern. An individual will rests his or her palm on the scanner. The images of the veins of the palm are captured. The captured images are stored in storage device. software convert the scanned image and stores it in the database in the form of binary data with which a unique code is also assigned either manually or automatically.

Palm scanner has two major functions:

1. Enrollment:- Collecting biometric data by capturing the biometric feature (left and right palms) of an individual for enrollment.

2. Identification:- Verifying or Matching or Comparing the recently or newly collected biometric data by capturing the biometric feature (either left or right palm) of an individual with the stored binary data in the database.

The unique feature of this scanner is it identifies only alive individual, a dead individual cannot be identified because deoxygenated blood present both in veins and arteries which will differ from the previously recorded pattern and hence it will not identify.

5. DNA SEQUENCING:

For DNA sequencing following steps are followed:

A. Collection of Blood Samples

B. Isolation of Genomic DNA from Blood

C. Primer design and PCR

1. Primer sequence

2. Standardization of PCR conditions using gradient PCR

PCR cleanup:

The amplified PCR products were eluted and were further used for sequencing.

3. Cycle sequencing:

a. Protocol for Cleanup of PCR Product

b. Cycle sequencing components

c. Clean up after Cycle Sequencing

As described above all the four instruments function independently and store the data in their respective software development kit. Then program takes this input from the software and transfers all this data into the storage place created by program. Program does not allow overlapping of these images to happen as used tools to make our data tables so strong that this confusion is avoided.

After the enrollment process by the instruments is complete the individual will come to the port where his / her blood sample will be collected for DNA sequencing. This process takes a minimum of 48 hours. The sequence is 1400 bases long and it is taken only from the X or Y chromosome respectively. This sequence of 1400 bases is then entered into our program and then stored at the appropriate place.

The crux of our invention lies in integrating all the biometric instruments i.e. finger scanner, iris scanner, face scanner, palm scanner, digital signature with the DNA sequences in the same computer application.

We tried to solve many of the problems associated with the use multiple biometric devices which includes the issues related to accuracy of the instruments or biometric devices For example: the finger scanner can't take very sharp images every time so there is a possibility that the computer system misinterprets and shows us a wrong match for the same person. This can be overcome by

using several biometrics of the same person to identify him / her. In case of the iris scanner, there is a peculiar problem i.e. if the distance from the camera is not appropriate the scanner gives a distorted image and that can lead to misinterpretation leading to a wrong match. The problem is again solved by using other biometric data of the same person. Our biometric system can assure a result of more than 99% matching as we are using multiple biometrics of the same individual to identify him or her.

No biometric data may be available of an individual particularly in an accident or a crime scene where only some traces of blood or hair or saliva etc. related to that individual could be obtained. In such cases DNA sequencing helps in identification by checking in our database. Inclusion of DNA sequencing in our system thus becomes invaluable.

EXAMPLE 2

In another embodiment of the invention, at least 4 biometric scanning devices are arranged in an unique way with a single usb hub connecting the same to the computer (Fig.8).

The hardware consists of two additional devices for connecting the usb of the devices as seen on the blue print of the device. The first device is a usb hub which consists of four ports to fit in the usb drive of our instruments like finger scanner, iris scanner, palm scanner and face scanner. The function of the device is to connect all the devices with the computer via the single usb cable. The instrument is just like a bridge to connect the data transfer of the image between the computer and the scanners. The microprocessor chip of the usb is designed in such a way that it connects all the instruments to the computer still keeping their individual data transfer different from each other so that they do not combine with each other or they do not send the data of that instrument into the wrong field in the computer database which can lead to a confusion and ultimately lead to a collapse of the database. The problem which we have solved by installing this system is that most of the laptops currently available in the world have space only for three usb port whereas our program requires four usb ports to connect all the hardware. Hence by this system we are saving space of two usb ports which can be utilized for others purposes such as inserting a pen drive or another type of hardware. Also it takes away 90-95% load put on computer by attaching only one usb hub instead of attaching all the instruments. The greatest advantage of all is that the conventional usb wires are only a meter long while attaching this usb hub we can make the wire at least of 5 meters (as tried and tested by us) and the data transfer

speed remaining the same. The circuit consists of four hubs connected in a series connection as per ohms law. It is made unique by connecting by connecting two instruments directly with the printed circuit board will the other two by normal usb connection .What this type of connection does is that it gives us opportunity to run all the instruments simultaneously which currently no one in the world can provide with all these instruments.

Also the changes made in the printed circuit board of the multiple usb are for getting higher number of voltage from the main supply. Basically we have increased the capacity of the multiple usb hub by increasing the numbers of IC's, Capacitors, and the number of resistors has been decreased by a certain amount. This has increased the overall capacity while making the instruments consume fewer amounts of energy but making them work efficiently.

This image represents the structure for a multiple usb hub. (Fig.6)

In this modifications have been made to remove the ports while to replace with direct connections.

Now about the second hardware that is the charger system or the adapter system for our set of instruments. Actually our instruments do not consume that much power but to capture iris with high resolution we need power input of about 2-2.5 volts. So we have developed a charger cum adapter system for it even though the light is cut off it can power the instruments for a few minutes. Figure 7 depicts the figure of adapter which is powering our hardware model currently.

The design of the circuit is indigenous because we have made a unique arrangement for the data transfer of the data from the instruments to the computer. The role the hardware is transferring of data without overlapping of data between the instruments and the computer.

It is designed specifically to transfer data in a proper channel and it is done by using data cables which are retrofitted in the printed circuit board. The working mechanism is that it does not depend on the connection pins of the USB Slots of the computer as well as the device. Our circuit is planned in a very unique fashion consisting of IC's, resistors, capacitors and a microprocessor.

The data cable contains four Wires with colours White, Black, Green and Red. White and black wires of the cable are for the power supply to the instruments and Green and Red wires of the cable are for data transfer and instructions transfer from device to computer and vice versa.

Any data transfer process is a power consuming process so it needs help of capacitors. The function of capacitor is generally to store charge in the form of electric current. Each capacitor is having maximum capacity of 10 microfarad for charge accumulation and maximum capacity of 5 volts for potential difference. 10 (TEN) such capacitors are installed in the circuit. The reason for installing so many capacitors is to match the requirements of total charge and potential difference of all these instruments. The number of resistors has been significantly decreased so as to provide us the boost in storing the charge in the capacitors. 3 resistors with their minimum capacity have been installed in the circuit.

The data cables are embedded in the circuit. Four separate IC's are connected to each of the four data cables. The function of IC's with the microprocessor is to control timing and the data transfer without the confusion or overlapping within the hardware or in the computer. The IC's used in the circuit are 8085, 8081 and 7805. The coding of the particular IC's is done using a language known as computer language "C" which is an universal language of programming for the IC's. Also there are middle level programming languages and assembly level languages for the programming of IC's.

The examples mentioned below are not limited to the below mentioned:

Examples:

The biometric of individuals are captured using figure scan, iris scan, face scanner, palm scanner, signature scanner and DNA scanner. This data is transfer to a processing unit where the information is processed and segregated so that no agglomeration is there in the database. The information is then passed from the processing unit to database where it is stored systematically where time of retrieval is very quick. The mode of access (output) or application can be various depending on requirement not limited to mention below:

1. **Wireless Access Control**

This system is a very robust system which is built to give authorized user access to restricted areas. This is a system wherein the biometrics is collected and the verified with the already enrolled data and the access is given to only verified person. This system is kept wireless so that the range of the access control system can be extended from just a few feet to kilometers. It utilizes a specially designed circuit which gives wireless access.

2. Immigration

Elimination of fake passport can be achieved with this application in aviation industry for immigration. If an individual is issued a passport from a particular county and he moves to another country and then applies for fake passport from other country, in such case when biometric are in record he tries to enroll for the identification. At such point of time such a fraud of passport duplication could be stopped.

3. Insurance

Identity theft today is the biggest threat to insurance industry. Where insurance industry cater to health and life insurance. The enrolled biometric could help to detect the health status of such individual, also to issue an life-insurance the identity of an individual. This can be stopped by enforcing biometrics which will reveal the identity of the particular individual and hence the fraud can be stopped.

For the accuracy, precision and time point of view we had used Wireless Access Control system for 10 people with different age group. There biometric were enrolled and then was identified, authenticated, and verified as mentioned below:

Table 1: Figure enrollment data:

No of People	Time for finger enrollment (second)	Time for finger data to be stored in database (microseconds)	Identification time (microseconds)
1.	6	1	2
2.	7	1	2
3.	5.5	1	2
4.	4.5	1	2
5.	9	1	2
6.	7.5	1	2
7.	6.5	1	2
8.	6	1	2
9.	5	1	2
10.	6	1	2

Table 2:Palm enrollment data:

No of People	Time for palm enrollment Seconds	Time for palm data to be stored in database microseconds	Identification time microseconds
1.	5	2	1.7
2.	4.5	2	1.7
3.	6.5	2	1.7
4.	7	2	1.7
5.	5.5	2	1.7
6.	3.5	2	1.7
7.	6	2	1.7
8.	9	2	1.7
9.	5.5	2	1.7
10.	3.5	2	1.7

Table 3: Face enrollment data:

No of People	Time for face enrollment	Time for face data to be stored in database nanoseconds	Identification time nanoseconds
1.	3	10	10
2.	4	10	10
3.	5	10	10
4.	2	10	10
5.	3	10	10
6.	4	10	10
7.	2	10	10
8.	3	10	10

9.	4	10	10
10.	5	10	10

Table 4: Iris enrollment data:

No of People	Time for iris enrollment seconds	Time for iris data to be stored in database nanoseconds	Identification time nanoseconds
1.	5	10	5
2.	6	10	5
3.	7	10	5
4.	5	10	5
5.	6	10	5
6.	5.5	10	5
7.	9	10	5
8.	8	10	5
9.	7	10	5
10.	5.5	10	5

Table 5: Data and time:

No of People	total time for enrollment (Seconds)	total space required for data storage(MB)
1.	19	0.9
2.	21.5	0.9
3.	23	0.9
4.	16	0.9
5.	23.5	0.9
6.	20.5	0.9
7.	23.5	0.9
8.	26	0.9

9.	21	0.9
10.	19	0.9

Although illustrative embodiments have been described herein in detail, it should be noted and understood that the descriptions and drawings have been provided for purposes of illustration only and that other variations both in form and detail can be added thereupon without departing from the spirit and scope of the invention. The terms and expressions have been used as terms of description and not terms of limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents. The terms or expressions herein should not be interpreted to exclude any equivalents of features shown and described or portions thereof.

We claim:

1. An evolved biometric authentication system comprising of comprises of multiple biometric, a processing unit a database and output.

2. An evolved biometric authentication system claimed in claim 1 providing high precision and more than 99% accuracy using multiple biometrics to identify and authenticate an individual by verifying biometrics characteristic data obtained from the individual at the time of identification and authentication by comparing with the previously registered biometrics characteristic data at the time of user registration, said system comprises: multiple biometric instruments, a processing unit, a database, and means of access (output).

3. A biometric authentication system/device as claimed in claim 1 wherein multiple biometric instruments are used for collection of biometrics stable or unstable/scanner for stable biometric and unstable biometric.

4. A biometric authentication system/device claimed in claim 1 wherein the processing unit is the hardware within a computer system which carries out the instructions of a computer program by performing the basic arithmetical, logical, and input/output operations of the system it is with a software component either as embedded in hardware or running thereon.

5. A biometric authentication system/device claimed in claim 1 & 4 wherein the software component is being configured to code, encrypt and store the images obtained from the scanning instruments in such a manner to avoid overlapping of multiple biometric images of various individuals enabling easy, concise, and fast retrieval of desired biometric data pertaining to an individual to compare with the images obtained afresh to authenticate the identification.

6. A biometric authentication system claimed in claim 1 is an efficient and comprehensive authentication system.

7. A biometric authentication system/device claimed in claim 1 & 3 wherein the multiple scanning instruments are used in combination or simultaneously are the biometric device used to capture biometric of individual are palm scanner, iris scanner, face scanner, voice scanner, figure scanner, DNA scanner, signature scanner.

8. A biometric authentication system/device claimed in claim 1wherein the database is an organized collection of data in digital form that supports processes requires running the information as required/commanded.

9. A biometric authentication system claimed in claim 1 wherein the means of access (output) is token-based identification and/or knowledge-based identification systems.

10. A biometric authentication system claimed in claim 1 wherein the said multimodal biometric device can be operated online giving its access globally.

11. A biometric authentication system claimed in claim 1 & 5 wherein the software component configuration for storing the images comprises of:

    i) creating storage place using tools stand alone application, client server application and web application
    ii) Creating database in many platform and tools like SQL server or Oracle systems and many more.

12. The method of biometric identification using multimodal biometric authentication device for authenticating a user enrolled/captured biometric and its output with more than 99% accuracy, comprising the steps of ;

    i) capturing the characteristics image of a biometric feature an individual.

ii) process of converting, encrypting, and storing the above images in a computer/central processing unit with the help of software program in an integrated method which avoids overlapping of the multiple images an Individual as well as different individuals enabling easy, concise and fast retrieval of the desired biometric data pertaining to an individual

iii) matching, comparing and verifying the same enrolled data with the images recently or newly obtained (with one or more available scanner) to identify or authenticate his or her identification.

iv) using it with applications as output

13. The method of biometric identification of individuals according to claim 11 wherein images of face, finger pattern, iris pattern, signature, voice, and palm pattern are obtained by face camera, finger scanner, iris scanner, signature scanner, voice scanner and palm scanner respectively.

14. The method of biometric identification of individuals according to claim 11 wherein the integrated method of storing the data comprises of

i) computer programming languages and web development languages which works on all operating system platforms like Microsoft Windows, Linux / Unix, Apple's MAC OS etc.

ii) assigning unique code to all the captured characteristics image of a biometric feature images and

iii) Creating database tables in SQL Server, Oracle, MySQL, DB2, XML and Microsoft Access etc.

15. A method of biometric identification of individuals as claimed in claim 11comprising the steps of:

i) capturing the characteristics image of a biometric feature image of the face or finger pattern or iris pattern or palm pattern with a respective camera or scanner

ii) process of converting, encrypting, and storing the above images in a computer with the help of our software program in an integrated method which avoids

overlapping of the multiple images an individual as well as different individuals enabling easy, concise and fast retrieval of the desired biometric data pertaining to an individual

iii) matching, comparing and verifying the same enrolled data with the images recently or newly obtained (with one or more available scanner) to identify or authenticate his or her identification.

16. The method of biometric identification of individuals according to claim 11 wherein the integrated method of storing the data comprises of :

i) computer programming languages and web development languages which works on all operating system platforms like Microsoft Windows, Linux / Unix, Apple's MAC OS etc.

ii) assigning unique code to all the captured characteristics image of a biometric feature images and

iii) creating database tables in SQL Server, Oracle, MySQL, DB2, XML and Microsoft Access etc.

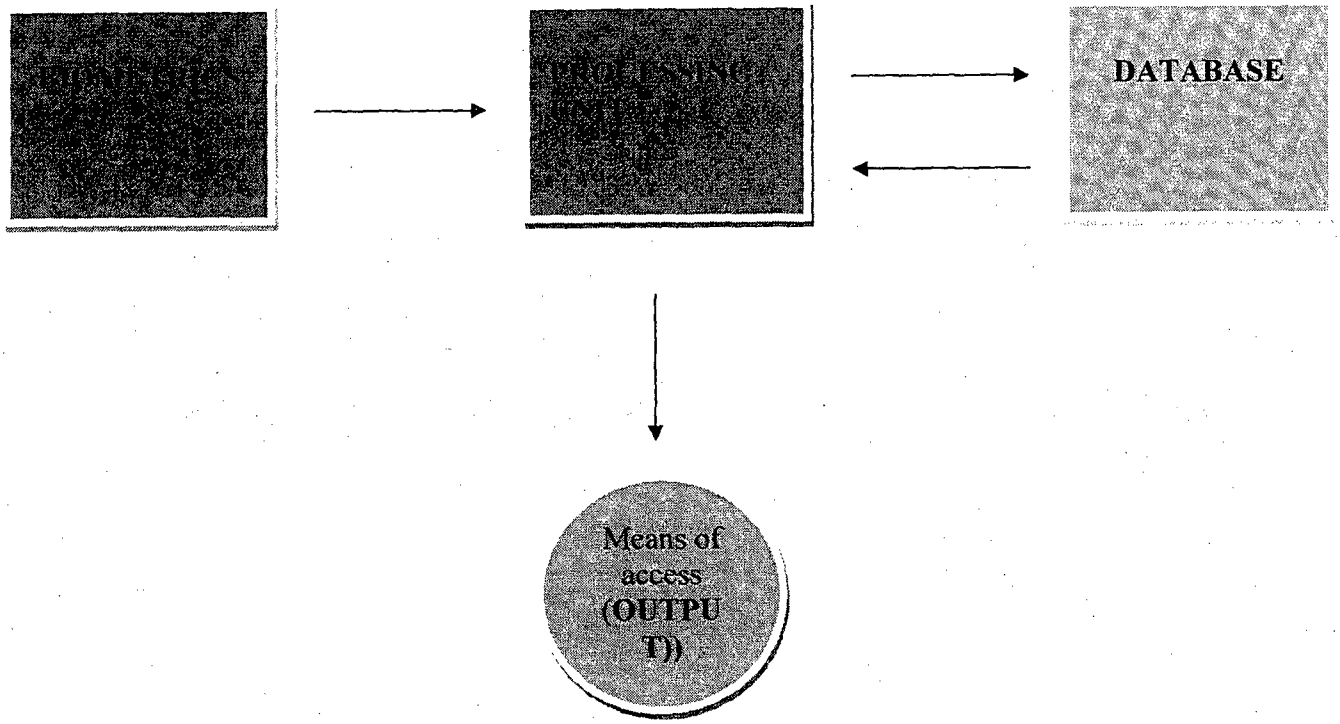


FIGURE 1

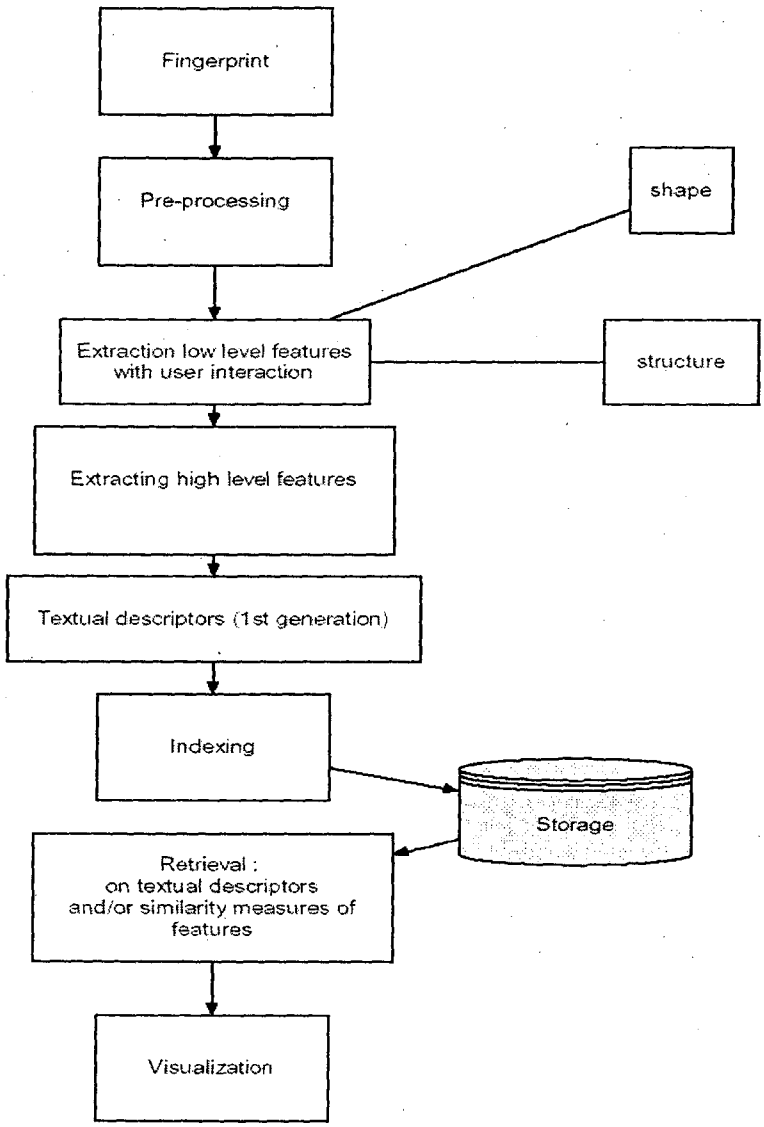
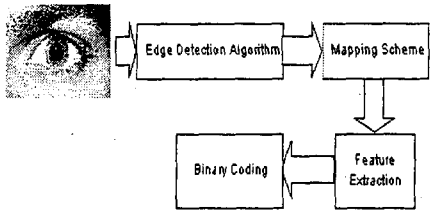

Fingerprint
Pre-processing
shape
Extraction low level features with user interaction
structure
Extracting high level features
Textual descriptors (1st generation)
Indexing
Storage
Retrieval : on textual descriptors and/or similarity measures of features
Visualization

FIGURE 2



Flow Chart of Iris Recogniton

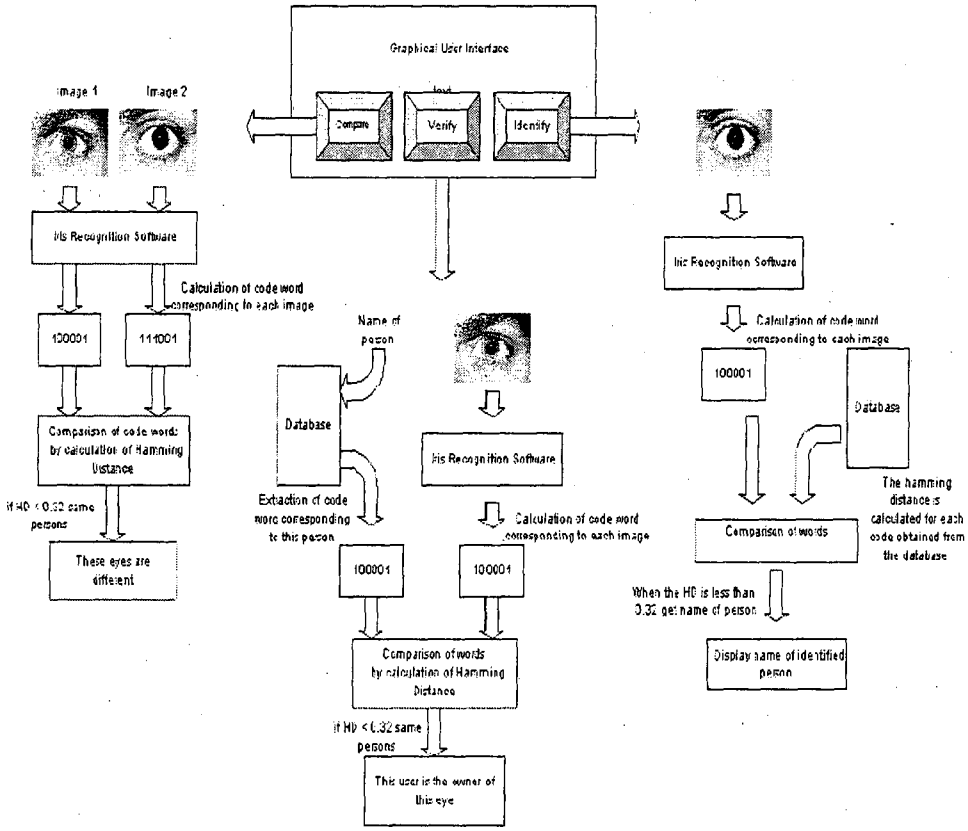


FIGURE 3

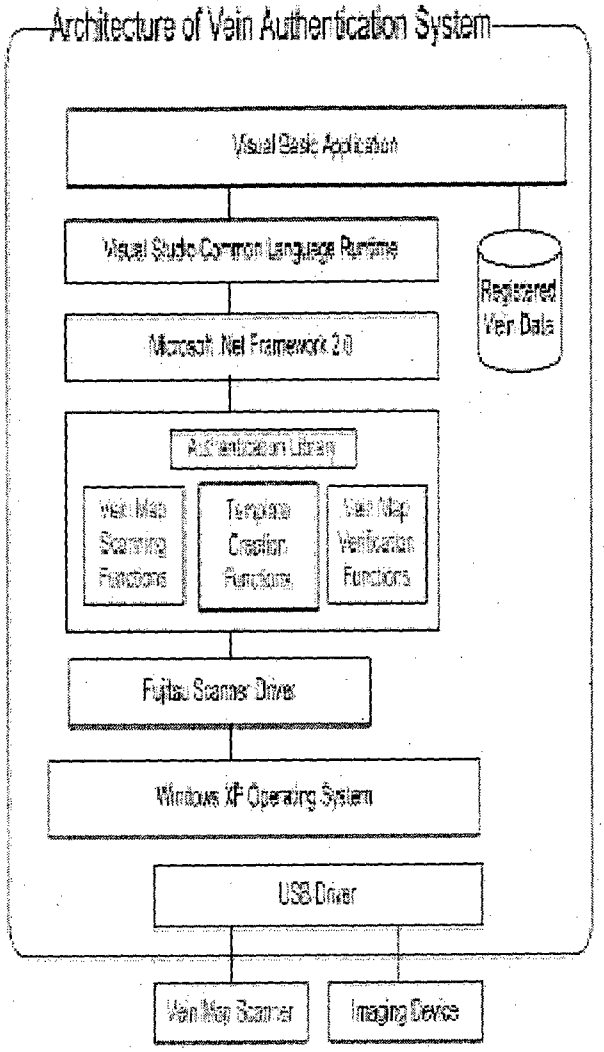

Architecture of Vein Authentication System
Visual Basic Application
Visual Studio Common Language Runtime
Microsoft .Net Framework 2.0
Registered Vein Data
Vein Map Scanning Functions
Template Creation Functions
Vein Map Verification Functions
Fujitsu Scanner Driver
Windows XP Operating System
USB Driver
Vein Map Scanner
Imaging Device

FIGURE 4

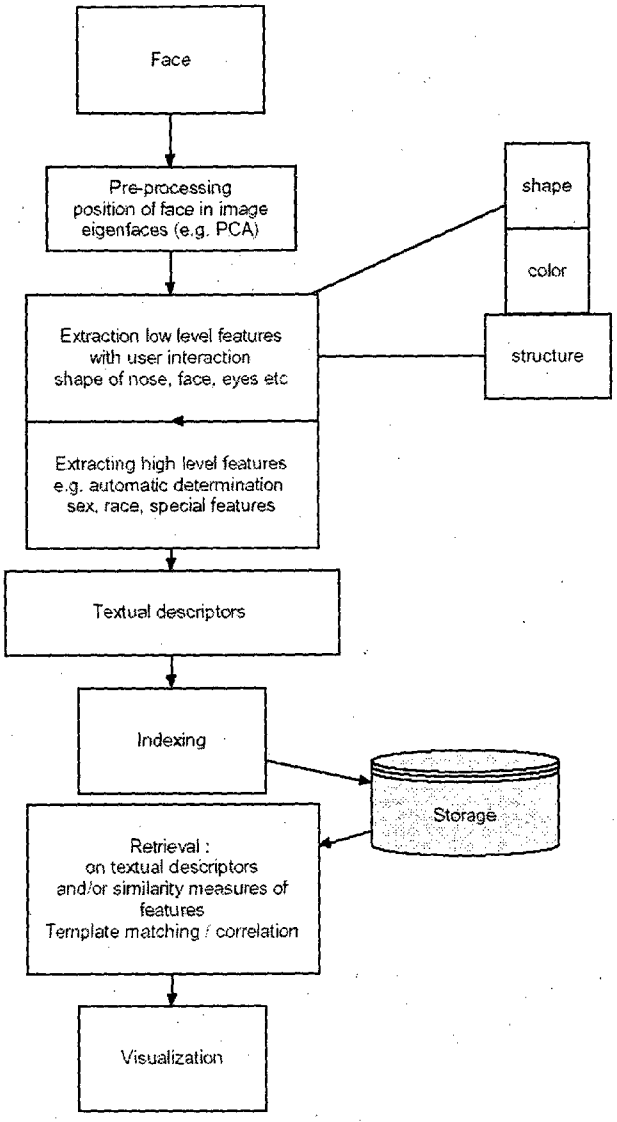

Face
Pre-processing
position of face in image
eigenfaces (e.g. PCA)
shape
color
structure
Extraction low level features
with user interaction
shape of nose, face, eyes etc
Extracting high level features
e.g. automatic determination
sex, race, special features
Textual descriptors
Indexing
Storage
Retrieval :
on textual descriptors
and/or similarity measures of
features
Template matching / correlation
Visualization

FIGURE 5

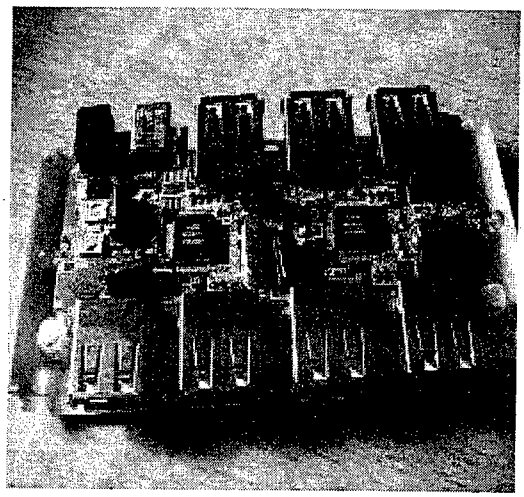


FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/IN2012/000433

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 G06K19/00 G06Q20/00
ADD.

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)
G07C G06K G06Q G06F H04L

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)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/055575 A2 (IMAGEWARE SYSTEMS INC [US]; WILLIS WILLIAM FREDERIC [US]; MILLER JAMES) 26 May 2006 (2006-05-26) abstract; claims; figures the whole document	1-16
X	EP 2 065 823 A1 (BIOMETRY COM AG [CH]) 3 June 2009 (2009-06-03) abstract; claims; figures paragraphs [0001], [0023], [0025] - [0041], [0043] - [0061]	1-16
A	US 7 882 032 B1 (HOFFMAN NED [US]) 1 February 2011 (2011-02-01) abstract; claim 1; figures paragraphs [0001], [0025] - [0041], [0043] - [0068]	1-16

☐ Further documents are listed in the continuation of Box C.

☒ 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
27 February 2013	05/03/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Rother, Stefan

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IN2012/000433

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006055575 A2	26-05-2006	AR 051670 A1	31-01-2007
		AU 2005307863 A1	26-05-2006
		CA 2588078 A1	26-05-2006
		EP 1817716 A2	15-08-2007
		WO 2006055575 A2	26-05-2006
EP 2065823 A1	03-06-2009	EP 2065798 A1	03-06-2009
		EP 2065823 A1	03-06-2009
		US 2009138405 A1	28-05-2009
US 7882032 B1	01-02-2011	AU 8501401 A	25-02-2002
		US 7882032 B1	01-02-2011
		WO 0214984 A2	21-02-2002