International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V9I3201909
Volume 9 Issue 3 September 2019

HUMAN IDENTIFICATION SYSTEM: A REVIEW

Oday A. Hassen[a], Nur Azman Abu[b], Z.Zainal Abidin[c]
[a,b,c]University Technical Malaysia Melaka,
Hang Taya, Melaka 76100, Malaysia.

[a]Odayali@uowasit.edu.iq
[b]nura@utem.edu.my
[c]Zaheera@utem.edu.iq

Abstract
Human Identification is directly associated with the approaches with the biometric detection and training of the datasets so that the analysis of particular person can be done for forensic applications. The investigating authorities use these approaches for criminal identification and overall analytics of the human traits. In this manuscript, the assorted dimensions and perspectives of the human traits in terms of biometric are specified with the depiction of the datasets including biological traits of EEG data. The biological traits can be used for the identification of human being including the brain waves. In addition, this manuscript points out the assorted points associated with the biometric applications. The biometric applications are having huge thrust of the human parameters whereby the human perspectives and traits are trained with higher degree of training and learning process in the model of the artificial intelligence and with these points the overall model is getting trained. The human identification system can be having any type of the human trait whether it is face, fingerprint, lips, iris, palm or any other and there may be some new aspects including tongue. Now days, the tongue based evaluations are also getting huge fame and this domain of tongue identification is still not used in the research perspectives. The tongue of every human being is quite unique and can be used the biometric applications based identification and recognition perspectives and it can be used as the higher degree of accuracy as the hybrid approach in integration with other aspects. This manuscript is having assorted and diversified points on the biometric applications and thereby the huge application areas in the detection of body points in the human traits and thereby the evaluation and overall performance in the traditional systems can be elevated to higher degree of accuracy and performance. The manuscript presents the multiple dimensions of the human features for the human identification with the accuracy levels.

Keywords: Human Biometric; Human Features; Biometric; Human Identification; Human Traits; Face Detection; Cloud Biometric; Cloud based; Human Identification; Face Data Mining; Face Biometric.

I. INTRODUCTION

Biometric refers to the analysis of the traits and features of a living creature whereby the assorted key points can be trained and further analyzed. Biometric applications are having number of perspectives which are used for the analytics of different features from human outlook or even inner segments [1, 2]. Biometrics is methods to automatically verify or identify individuals using their physiological orbehavioralcharacteristics. Biometric technologies include:, Face Recognition, Face Smile Detection, Voice Recognition, Hand Geometry Identification, Iris Identification, DNA Sequence Matching, Signature Recognition, Finger Print (dactylogram) Identification, Retina Identification [3, 4].

Countries which are integration biometrics in assorted segments includes the following:

Australia	Brazil
Canada	Cyprus
Greece	China
Gambia	Germany
India	Iraq
Israel	Italy
Malaysia	Netherlands
New Zealand	Nigeria
Norway	Pakistan
South Africa	Saudi Arabia
Tanzania	Ukraine
United Arab Emirates	UK
USA	Venezuela

Among low to middle income countries, roughly 1.2 billion people have already received identification through a biometric identification program.

There are also numerous countries applying biometrics for voter registration and similar electoral purposes [5, 6, 7]. As per the Database of Citizens for Elections, some of the countries using Biometric Voter Registration (BVR) are:

Armenia	Angola
Bangladesh	Bhutan
Bolivia	Brazil
Burkina Faso	Cambodia
Cameroon	Chad
Colombia	Comoros
Congo	Costa Rica
Ivory Coast	Dominican Republic
Fiji	Gambia
Ghana	Guatemala
India	Iraq
Kenya	Lesotho
Liberia	Malawi
Mali	Mauritania
Mexico	Morocco
Mozambique	Namibia
Nepal	Nicaragua
Nigeria	Panama
Peru	The Philippines
Senegal	Sierra Leone
Solomon	Somaliland
Islands	
Swaziland	Tanzania
Uganda	Uruguay
Venezuela	Yemen
Zambia	Zimbabwe

Features Recognition for Human Identification in Biometric input an image of the person in question inside the system and the system will first preprocess the image which will cause unwanted elements such as noise to be removed from the image [8, 9]. After that, the system will then classify the image based on its landmarks for example, the distance between the eyes, the length of the jaw line, etc. Then, the system executes a search through the database to find its perfect match and display the output. Current practice of thumbprint identification which is simple and easy to be implemented can be challenge by the use of latent thumbprint and sometimes cannot be acquired from the crime scene. The criminals have become cleverer and normally are very careful in leaving any thumbprint on the scene. This system encompassed face database and an image processing algorithm to match the face feed with faces stored in the database. There are two parts vital to the success of this system; detection and recognition. [10, 11]

A biometric detection is one of the most important steps in a recognition system and can be classified into four principle categories; knowledge based, feature invariant, template matching and appearance-based methods. In recognition, two stages are required; training process and evaluation process [12, 13]. In a training process, the algorithm is fed samples of the images to be learned and a distinct model for each image is determined while in an evaluation process, a model of a newly acquired test image is compared against all existing models in the database. Then the near corresponding model is acquired to determine whether the recognition is triggered. In this stage, a statistical procedure, the approach of simulated annealing is used to on a collection of face images to form a set of basis features, which is called a set of Eigen-objects. Any human face can be considered to be a combination of these standard faces [14, 15].

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V9I3201909
Volume 9 Issue 3 September 2019

Assorted Types of Biometric Traits.

A. Physiological

a. Face
b. Iris
c. Hand
d. Fingerprint
e. DNA

B. Behavioral

- Gait: Motion Detection
- Voice: Speech based Signals
- Sign: Texture
- Keystroke

C. Gait

- Floor Sensor Based
- Machine Vision Based
- Wearable Sensor Based

D. Machine Vision Based

- Appearance Based
- Model Based

E. Appearance Based

- State Space Methods
- Spatio-temporal Methods

Following is the depiction of the user authentication aspects associated with the biometric traits and thereby the way by which the different perspectives of the human biometric can be evaluated [16, 17]. Figure 1 & 2 & 3, explain this.

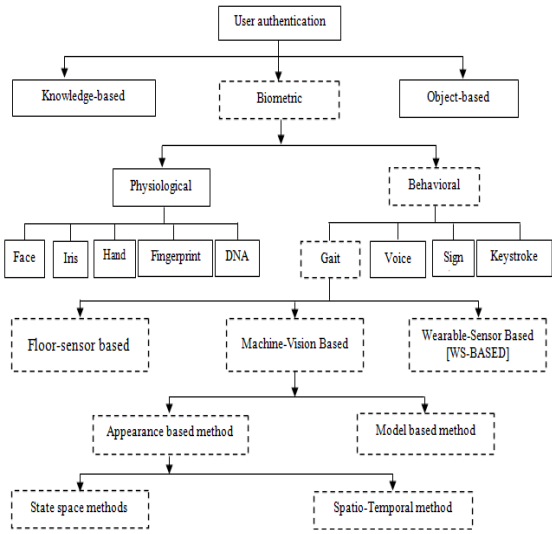


Figure 1: User Authentication Approaches.

Figure 2: Biometric Types.

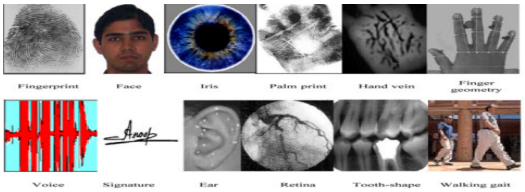


Figure 3: Assorted Human Traits for Recognition.

A. Tongue Biometric:-

The human tongue (fig.4) is having unique structure and its features can be used as the biometric object that is not widely used. Following is the depiction of the tongue based biometric identification in the human features.

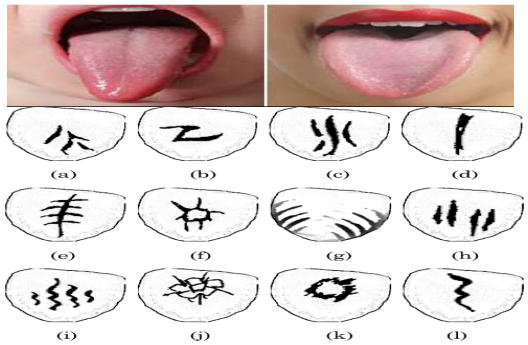


Figure 4: Tongue Biometric.

B. Facial Recognition

In figure 5. Face recognition refers to the identification of human face with respect to the different lines and the features associated with the face. Each face is having a specific and unique structure and these are training in the soft computing models [18, 19].

Figure 5: Facial Recognition

The face recognition techniques are enormous with the edge, corner and pixel evaluations and these can be evaluated while prediction of the face for different applications [20, 21].

C. Iris Recognition:-

The iris detection and further recognition refers to the identification of the features in the nerves of human eye with the deep analytics of the patterns in the iris [22, 23]. Figure 6 show this.

Figure 6: Iris Recognition.

Many countries are using iris recognition for the evaluation of human traits and citizen identification using this approach.

D. Voice Recognition:-

In figure 7. The approach of voice recognition is more diverted towards the signals analytics whereby the pitch and sound level of the speech is trained and then predicted [24, 25].

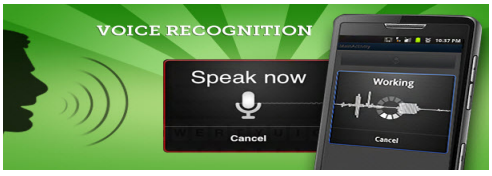


Figure 7: Voice Recognition.

This approach is widely used and integrated for the assorted applications of human traits detection and criminal investigation [26].

E. Fingerprint Recognition:-

In figure 8. Fingerprint training and analytics is one of the very popular and historical aspects in the biometric and it is used from the decades [27, 28].

Figure 8: Fingerprint Recognition

The feature points in the finger of every human being are unique and it is used for the identification and prediction of the criminals as well as different forensic applications [29, 30].

F. Signature Recognition:-

The approach of signature detection (figure 9) is classically used for the financial transactions for the validation of texture on the checks or the banking instrument [31, 32].

Figure 9: Handwritten Texture or Signature Recognition.

II. BIOMETRIC EVALUATION AND

A. IDENTIFICATION PROCESS:-

Recently, the field of human identification has become one of the broadest areas of research that the researchers have dealt with and reached very strong results, especially in the external aspects of man, namely iris of the eye and face, signature of the hand, fingerprint, etc. Therefore, there was a disparity between the accuracy of the results and the disparity and even the cost that became very necessary in the application at a time when it became a world focused on the material issues and cost. The following table 1 &diagram 10 explain illustrates the differences between human identifiers.

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V9I3201909
Volume 9 Issue 3 September 2019

Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
ADN	High	High	Test equipment	Low
Iris recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature recognition	Low	Medium	Optic pen, touch panel	High

Table 1: Accuracy, Cost and Other Factors with Assorted Biometrics.

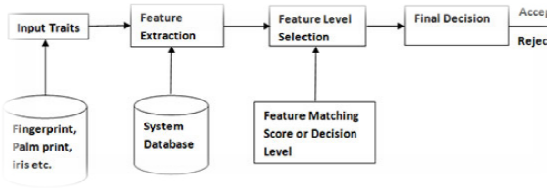


Figure 10: Evaluation and Prediction.

Also the Advantages of Biometric system includes Identification Accuracy, Reduces Administrative Cost, Convenience, Accountability, Difficult to forge, Return on Investments, Integration, Effectiveness, Security, Scalable and Profitability [33, 34, 35].

In some research literature, it is proposed to work on the detection on Biometric Traits to analyze the Features Detection using meta-heuristic approach which makes use of global optimization of results. In this area, the use of artificial neural networks or support vector machine can be used for classification of the Smile on Human Biometric Trait [36, 37]. Biometric Trait recognition or detection is a widely used technology which is undergoing constant development to improve its results [38, 39]. It is used in different environments such as in forensic science, medicine and surveillance or security systems. It is also a widely developed mobile application. There are many different kinds of Biometric Trait detection devices and many different algorithms operating these devices [40, 41, 42, 43]. Many researchers and scholars have been trying to implement the ideal case of Biometric Trait detection algorithm. Many algorithms were used to achieve this goal but not all constraints have been taken into consideration while developing this software [44, 45, 46]. Some of the known algorithms are: Principle Component Analysis using Eigen Biometric Traits, Linear Discriminate Analysis, Elastic Bunch Graph Matching using Fisher-Biometric Trait Algorithm, Content Based Image Retrieval (Jyoti Jain), the Hidden Markov and Dynamic Link Matching [47, 48, 49, 50]. The constraints taken while developing the software to yield accurate results are: position of the Biometric Trait, low lighting, and sufficient data in database and facial expressions [51, 52, 53].

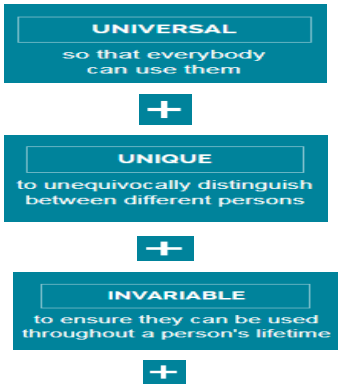
The performance of biometric system is evaluated from the following aspects;

a. False match rate (FMR, also called FAR = False Accept Rate).
b. False non-match rate (FNMR, also called FRR = False Reject Rate).
c. Receiver operating characteristic or relative operating characteristic (ROC).
d. Equal error rate or crossover error rate (EER or CER).
e. Failure to enroll rate (FTE or FER).
f. Failure to capture rate (FTC).
g. Template capacity.

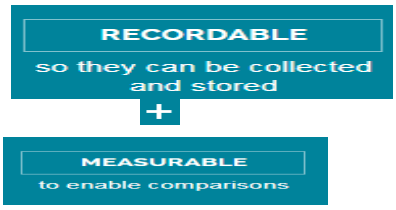
Types of biometric evaluations include biological, morphological and behavioral [54, 55, 56, 57]. Show figure 11.

Figure 11: Biometric Traits.

There is specific set of features that must be present in the biometric. This Diagram 12 explain this.



International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V9I3201909
Volume 9 Issue 3 September 2019



Figer12: features specific in biometric.

B. Biometric Functions and Architecture diagram:-

a. Verification
b. Identification
c. Matching with Security and Accuracy
d. Feature Extraction
e. Training the Dataset
f. Decision Making Module
g. Predictive Mining Module.

F. Components of Biometric System:-

Biometrics system is the science of the measurement of unique human characteristics, both physical and behavioral. Biometric technology refers to any technique that reliably uses measurable physiological or behavioral characteristics to distinguish one person from another. The roots of biometric technology go back a long way, about several thousandsof years. Therefore, the components of the biometric system vary from one type to another depending on the type of user and the nature of the challenges encountered to work. This figure 13, 14, 15, 16 illustrates this.

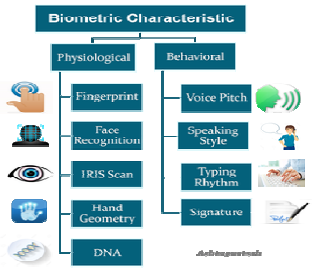


Figure 13: Biometric Components.

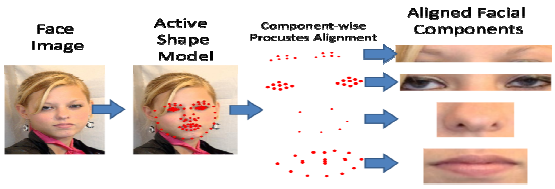


Figure 14: Biometric Components.

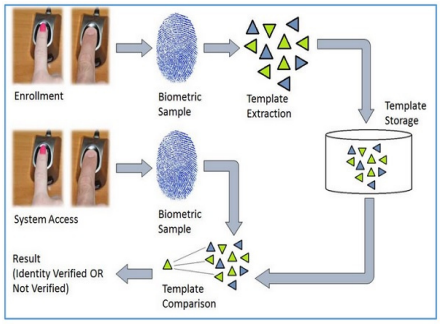


Figure 15: Biometric Components.

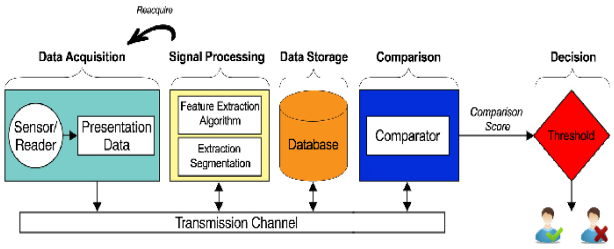


Figure 16: Biometric Components.

A. Advantages of Biometric:-

a. Identification Accuracy
b. Reduces Administrative Cost
c. Convenience
d. Accountability
e. Difficult to forge
f. Return on Investments
g. Integration
h. Effectiveness
i. Security
j. Scalable
k. Profitability
l.

G. Biometric Object Recognition:-

Biometric Object recognition refers to a process of identification of human Biometric Object or Biometric Objects similar to

human Biometric Object in a video or an image [58, 59, 60]. Sometimes it is also referred as the process of identifying images which are similar to each other, for example there is a database of 100 images of 10 individuals, each person can look up, down, sideways, can smile, can frown etc. [61, 62, 63, 64] Thus the designed system should be able to recognize a particular person having all the different expressions and also should be proficient in differentiating other person's Biometric Object [65, 66, 66, 67]. The Biometric Object recognition technology has improved over the years but still there are some drawbacks. This work focuses on the integration of dynamic data and real time webcam based implementation for the Biometric Object Detection so that a rich training of the model can be done with the higher degree of accuracy [68, 69, 70, 71]. The high level algorithm with the multilayered approaches for classification can be devised and implemented using big data based repository of the Biometric Object images so that the multiple dimensions and features can be extracted with the deep evaluation and matching for higher degree of accuracy and predictions in minimum error factor [72, 73].

H. **Technology of Biometric Object Recognition**:

A. Biometric Object Detection:

a. Biometric Object detection [74, 75]
b. Biometric Object located in image [76, 77].
c. Skin-tone, texture and Biometric Object pyramid used [78, 79, 80].

B. Biometric Object recognition:

C. Appearance and geometry of Biometric Object used [81, 82]

a. Geometry- difficult but robustness against disguising [83, 84].
b. appearance- easy but vulnerable [85, 86].
c. facial landmarks used.
d. A Biometric Object image is represented as a vector of intensities and this vector is then approximated as a sum of basis vectors [87, 88].

D. Matching:

a. Biometric Object templates used.
b. Similarity and dissimilarity decided based on threshold [89, 90].
c. Altering threshold- FA and FR.

III. APPLICATIONS:

A. Forensic science: The face of the dead/criminal is checked against the database to identify the face. Some software can identify the face similar to a given face even if the input is distorted, Lee Gomes.

B. Identification systems: This is an identification task, where any new applicant being enrolled must be compared against the entire database of previously enrolled claimants, to ensure that they are not claiming under more than one identity, Lee Gomes.

C. Surveillance: The application domain where most interest in face recognition is being shown is probably surveillance. Video is the medium of choice for surveillance because of its richness and type of information that it contains and naturally, for applications that require identification, face recognition is the best biometric for video data, Glenn Menin.

D. Pervasive Computing: Another domain where face recognition is expected to become very important, although it is not yet commercially feasible, is in the area of pervasive or ubiquitous computing.

Biometric applications are having number of perspectives which are used for the analytics of different features from human outlook or even inner segments. Biometrics is methods to automatically verify or identify individuals using their physiological or behavioral characteristics.

Biometric Technologies Include:

a. Face Recognition
b. Face Smile Detection
c. Voice Recognition
d. Hand Geometry Identification
e. Iris Identification
f. DNA Sequence Matching

g. Signature Recognition
h. Finger Print (dactylogram) Identification
i. Retina Identification

Biometric Object Detection is one the key domain of research in digital image as well as real time video processing. In Biometric Object analysis, there are assorted segments which are required to be investigated in terms of getting emotions and feelings of the person. These segments include Lips, Eyes, Cheeks, Ears, Eye Brows, Nose and many others. Lips Detection is used to analyze the emotions of the person in terms of Sadness, Happiness, Frustrations and many others. Using this research work, it is proposed to work on the Lips based Smile Detection on Biometric Objects to analyze the Smile Detection using fuzzy based soft computing approach which makes use of global optimization of results. In this area, the use of artificial neural networks or support vector machine can be used for classification of the Smile on Human Biometric Object. Biometric Object Detection, Recognition and Analytics are the key domains of research in the surge of electronic pictures in relationship with machine learning and discerning examination. This particular space is to an awesome degree supportive for the criminal examination on various regions including Airports and other open locales where the progression of guilty parties are standard. The key desire for confront assertion is to dismantle and engineer the improvements of a man on the Biometric Object and extraction of honest to goodness conclusions amidst the situation under scrutiny. The execution of critical learning based assembling and check approaches in relationship of meta-heuristic based joining is utilized for the more lifted measure obviously of activity to construct least goof factors. Biometric Object Detection is one the key space of research in motorized picture and also fearless video organizing. In stand up to examination, there are particular bits which are required to be investigated like getting estimations and suppositions of the individual. These parts lace Lips, Eyes, Cheeks, Ears, Eye Brows, Nose and differing others. Lips Detection is utilized to restrict the thoughts of the person regarding Sadness, Happiness, Frustrations and unmistakable others. Assembled typical enlivened procedures arranged so far for managing the building issues in composed spaces yet there is 'before a wide level of research in the bit. Nature gave us diverse approaches which can be utilized for the settling and besides managing the issues in various spaces including delineating and social perspectives.

IV. CRIMINAL RECOGNITION USING OPEN SOURCE TOOLS AND RELATED LIBRARIES

OpenCV is Intel open source computer vision library (Computer Version). It consists of a series of C functions and a few C ++ classes that implement many common algorithms for image processing and computer vision [91, 92]. OpenCV includes a plurality of 300 C functions have cross-platform, high-level API. It does not depend on other external libraries - although you can also use some external libraries. OpenCV for non-commercial use and commercial applications are free. Meanwhile OpenCV provides access to the hardware, you can directly access the camera, and opencv also provides a simple GUI (graphics user interface) system: high-up. We passed some of the ways to construct OpenCV provides the face detection (face detection) program [93, 94]. OpenCV itself is a C / C ++ to write, if you want to use in other languages, we can be packed to its dynamic link library files, fortunately, there are a lot of such packaging under Python, as used herein, is Cvtypes. In fact, in many Python packages are from third parties, such as PIL (Python Image Library) is a graphics package C language, are packed into the Python, these packages allow you to use Python's like inside built in the same function using these API [95, 96, 97].

Face detection is part of Target Detection (object detection), mainly related to two aspects:

a.The target object to be detected prior probability statistics, so they know to be some of the characteristics of the detection object, and establish target detection model.

b.Use the resulting model to match the input image, if there is a match, the output matching area, otherwise do nothing.

Computer vision system with the human eye is very different, but which also have similarities.

The human eye can see objects by light reflected from the object to stimulate the human eye's photoreceptor cells, then like objects form the optic nerve in the brain. Computer much simpler to see things through the camera, simply put, is a bunch of digits in the matrix. These figures show that the strength of the photosensitive element of the camera optical signals into objects emit light into a digital signal, which is quantified as a matrix [98].

How to be drawn from these figures: "This is a human face," the conclusion is a more complicated matter. The physical world is in color, in general, computer color pictures are cumulative out by a number of color channels, such as RGB mode image, a red channel (Red), the green channel (Green), and blue channels (Blue), these three channels are grayscale, such a point is represented by the eight, then one channel may represent $2^8 = 256$ gray levels. After three channels that can be superimposed Table 3 * 8 = 24 kinds of color, that is, we often say that 24-bit true color. For such pictures do deal with, no doubt, it is a very complicated matter, it is necessary to first color image into grayscale, so you can reduce the amount of data (such as RGB mode, the original image can be reduced to 1/3). At the same time we can remove some of the noise signal. First image is converted to grayscale, then this will increase the contrast of grayscale, so you can make pictures originally dark place darker, brighter place brighter. After this treatment, the more likely it is the algorithm set pictures do not come out. HAAR features cascadingtableOpenCV on object detection using a cascade of HAAR feature table, this table contains a cascade classifier boost. First, people use HAAR feature samples of classifier training, resulting in a cascade boost classifier [99, 100]. Training mode contains two aspects:

a. The positive samples that the target sample to be tested

b. Negative samples, any other pictures.

First, these images will be unified into the same size, this process is called normalization, and statistics. Once the classifier created, can be used to detect the input image of the region of interest, in general, the input image will be larger than the sample, so, you need to move the search window, in order to retrieve the target of different sizes, the classifier You can be scaled to change their size, so you may want to enter multiple image scanning. Cascade classifier is composed of several simple classification cascades into a big classifier, the detected window sequentially through each category, we can through the window to all categories judged as a target area. Meanwhile, in order to consider efficiency, it can be the most stringent classification on the top of the entire cascade classifier, so you can reduce the number of matches [101].

Basis HAAR classifiers to features as input to the output 0/1, 0 indicates no match, 1 match.

HAAR features on Face / Lip / Tongue and Other Human ObjectsBoundary characteristics, contains fourLinear features, including eight kindsCenters around a feature, comprising two to be detected at the time of scanning images to the boundary feature in (a), for example, as previously mentioned, the computer image is a matrix of numbers, the program first calculate the entire window in the gray value x, then Calculation rectangle of black gray value y, then calculate (x-2y) value, the value obtained is compared with x, and if this ratio is within a certain range, it means to be detected picture boundary characteristics in line with the current scan area (a), and then continue scanning [102].

A more detailed description of this algorithm is beyond the scope of this research, you can get more information in the reference resource. Non-fixed size target detection because it is based on the object detection video stream, we had less likely to know the size of the target to be detected, which requires us to cascade classifier table has proportionally increased (or reduced) capacity, so that when small windows mobile complete a picture to be detected when the target is not found, we can adjust the size of the classifier, and then continue to test until after the target to be detected or the window size of the picture is quite far.

Step one: image preprocessing.

Step Two: Detect and mark targets.

OpenCV, for face detection model has been established as an XML file, which contains the results of training the classifier HARR features mentioned above, we can load the file and omit the table to establish their own cascade process. With cascading table, we only need to be detected image and cascading table to pass along to OpenCV target detection algorithm to get a collection of the detected face.

Because the video stream is dynamic, so we can use an infinite loop at the entrance of the program, in the cycle, each from the video reads a frame, the frame transmission gives the current face detection module, the detection module on the frame After marking (if someone current face), and then return to the frame, the main program to get this frame, update the display window [103].

OpenCV function is very powerful, but also provides a large number of algorithms, text content related to only a small part of the computer vision. Readers can consider the collected human face identification, in order to achieve a specific person's face recognition. Or consider the human face detection ported to the network, enabling remote monitoring. Imagine, they had no life of the machine, we can, through their own thoughts, actions to make them appear to have thought the same, this in itself is very interesting [104].

Object Recognition for Criminal Identification is the face assertion structures in which the security expert data a photograph of the individual being insinuated inside the framework and the structure will first preprocess the photograph which will cause undesirable portions, for example, object to be removed from the photograph. Beginning now and into the not so distant, the structure will then sort out the photograph in context of its prominent concentrations for instance, the separation between the eyes, the length of the jaw line, and so forth. By at that point, the framework executes an enthusiasm through the database to locate its ideal match and exhibit the yield. This work is concentrating on executing the framework for criminal perceiving proof. Current routine as for thumbprint indisputable proof which is immediate and simple to be finished can be challenge by the utilization of lethargic thumbprint and now and again can't be anchored from the awful conduct scene. The guilty parties have pushed toward getting the chance to be cleverer and ordinarily particularly attentive in leaving any thumbprint on the scene. This framework solidified face database and a photograph arranging estimation to encourage the face feed with faces set away in the database. There are two territories pivotal to the accomplishment of this structure; territory and attestation. Face region is a champion among the most essential strolls in a face certification framework and can be sorted out into four oversee classes; learning based, join invariant, organize arranging and appearance-based procedures. In attestation, two phases are required; preparing framework and examination process [104].

In a course of action framework, the calculation is bolstered instances of the photographs to be scholastic and a certain model for every photograph is settled while in an evaluation procedure, a model of a starting late got test picture is considered against each present model in the database. By then the close-by relating model is anchored to pick if the confirmation is started. In this stage, a quantifiable framework, the approach of reenacted toughening is utilized to on a get-together of face pictures to shape a blueprint of introduction highlights, which is known as a strategy of eigen-objects. Any human face can be accepted to be a blend of these standard appearances [105]. Face Detection is one the key space of research in computerized picture and also constant video preparing. In confront examination, there are different sections which are required to be explored as far as getting feelings and sentiments of the individual. These portions incorporate Lips, Eyes, Cheeks, Ears, Eye Brows, Nose and numerous others. Lips Detection is utilized to break down the feelings of the individual regarding Sadness, Happiness, Frustrations and numerous others. Following are the locations using biometrics in their systems,

China, Brazil, Cyprus, Germany, Australia, Iraq, Canada, Gambia, India, Pakistan, Netherlands, Greece, Malaysia, Italy, Norway, Tanzania, New Zealand, South Africa, Ukraine, Saudi Arabia, Nigeria, UAE, UK, USA, Venezuela Among low to middle income countries, roughly 1.2 billion people have already received identification through a biometric identification program. There are also numerous countries applying biometrics for voter registration and similar electoral purposes. According to the International IDEA's ICTs in Elections Database, some of the countries using (2017) Biometric Voter Registration (BVR) are , Armenia, Bangladesh, Angola, Cambodia, Bolivia, Brazil, Burkina Faso, Cameroon, Congo (Democratic Republic of), Chad, Colombia, Comoros, Costa Rica, Ivory Coast, Bhutan, India, Dominican Republic, Gambia, Ghana, Guatemala, Fiji, Iraq, Kenya, Lesotho, Liberia, Malawi, Mali, Mauritania, Mexico, Morocco, Mozambique, Namibia, Nepal, Nicaragua, Solomon Islands, Nigeria, Panama, The Philippines, Senegal, Swaziland, Peru, Sierra Leone, Somaliland, Venezuela, Tanzania, Uganda, Uruguay, Zimbabwe, Yemen, Zambia. Face Detection, Recognition and Analytics are the key domains of research in the stream of digital images in association with machine learning and predictive analysis. This specific domain is very helpful for the criminal analysis on different locations including Airports and other public locations where the movement of criminals are expected. The key motive of face recognition is to analyze and classify the motions of a human being on the face and extraction of actual emotions during the scenario under investigation [106]. The implementation of deep learning based classification and prediction approaches in association of meta-heuristic based integration is used for the higher degree of classification to gain minimum error factors. Face Detection is one the key space of research in automated picture and furthermore steady video planning. In stand up to examination, there are distinctive segments which are required to be investigated similar to getting emotions and suppositions of the person. These segments fuse Lips, Eyes, Cheeks, Ears, Eye Brows, Nose and various others. Lips Detection is used to separate the sentiments of the individual with respect to Sadness, Happiness, Frustrations and various others. Assorted natural inspired approaches devised so far for solving the engineering problems in assorted domains but there is still a wide scope of research in the segment. Nature provided us a number of approaches which can be used for the resolving as well as solving the problems in different domains including engineering and social aspects. The recent Nature Inspired algorithms include Artificial Bee Colony Algorithm, Firefly Algorithm, Social Spider Algorithm, Bat Algorithm, Strawberry Algorithm, Plant Propagation Algorithm, Seed Based Plant Propagation Algorithm and many others. In this proposed research work, the novel and effective approaches for deep learning and classification of face smiles shall be used so that the face smile classification on multiple classes can be done with minimum error factor. Using nature inspired approaches in association with soft computing fuzzy techniques, the higher degree of accuracy and optimization can be achieved. The following depicts the process face smile detection using deep training of the model using embedded Hidden Markov Model (HMM) . The approach is quite effectual in getting the results with higher degree of accuracy and predictions. The approach of maximum likelihood training is traditionally implemented with the HMM so that the performance aware results can be obtained from the implementation and predictive analysis. The accuracy and output of Hidden Markov Models are highly successful in speech recognition which is further proposed to be implemented in Face Smile Detection for predictive analysis in assorted domains. The process of features extraction is depicted in Figure in which the face image having height H and width W is segmented into multiple overlapping blocks so that the unique features can be extracted and further analytics can be done [107].

Due to the dynamic nature of Biometric images, a Biometric recognition system encounters various problems during the recognition process. The problems may include variation in lighting conditions, pose, etc. One more problem that is usually encountered is high

dimensionality problem. The dimensions of an image are very large so it makes the calculation and thus the Biometric recognition system very complex. So, techniques are required that not only reduces the dimensions of the image but are also time efficient. The other problems of a robust Biometric recognition system are given below.

In Shift Invariance, the projected approach is required to be effective and performance with the variation in the shift of Biometric. The smile of any person should be invariant in the analysis from different angles of Biometric and it should be able to give accurate results with more optimization in the resources.

In Illumination Invariance, once the illumination or lighting effect is projected on the Biometric image with particular smile expression, the algorithm is always required to be presenting the output in same accuracy as without illumination effect. In precise, the lighting or illumination or false flash lights should be easy identified with the accurate Biometric detection.

In case of Skin Modeling and Biometric Analytics, for skin modeling a training set of skin images are used. These images were obtained by cropping off skin regions in images containing human subjects, downloaded from the web, manually. Similarly for the non-skin model, background regions from these web images are used. As discussed, the skin color is localized to a small region in the CbCr chrominance space as can be seen, where a projection of the histogram of the skin pixels in the database on the CbCr plane is shown. The histogram of the training skin pixels is shown. The non-skin database histogram projected onto the CbCr plane is shown the unimodal Gaussian density estimate for the skin pixel distribution. The unimodal Gaussian skin and non-skin models are used to calculate the skin probability image for an input test image. The skin probability image is analyzed using the set of connected operators described before, to detect and segment Biometric(s) present in the image. The thresholds for various connected operators have been arrived at, after testing a number of images containing Biometric(s).

Threshold values for the operators used:
Compactness threshold = 0.025
Solidity threshold = 0.5218
Orientation range = 0.9 to 2.1
The threshold for binary segmentation has been decided based on the results obtained using different values.
Binary segmentation threshold = 60

Also the structuring elements used, viz. 5-by-5 with a constant gray level of 25 for open operation, and 3-by-3 with a constant gray level of 15 for close operation, were obtained by observing the performance on a number of images [103, 104].

A sample input image has the skin probability image, using unimodal gaussian for skin color the corresponding opened/closed image is shown, and the thresholded image. Finally the result of segmentation is as shown. The segmentation results, using a unimodal Gaussian skin model, for a few test images are shown. The results of both true and false segmentation are shown. A false segmentation has occurred because the skin pixels of the left leg have been exposed and the resulting component from thresholding has a Biometric-like shape. The false segmentation because of the background containing many skin-colored regions and one of the components in the background having values for the operators within the range for a Biometric [105].

The term $P^{old}(j/c_n)$ is obtained by just accessing the element Prior_Prob(n,j) of the matrix Prior_Prob which is calculated once for a given set of GMM parameters and a given set of data. The term that appears in every iterative equation is obtained by summing all the terms along the j^{th} column of the Prior_Prob matrix. It can be calculated only once and used in the iterative equations for one update process. The sum **L** =, is used as the likelihood function for

the data set. It is obtained by just summing the elements of the Tot_Prob vector [106].

During every iteration of the EM algorithm, the updated parameters are obtained by passing the old parameters and the training data set to the calc_prob function and accessing the two output arrays in the iterative equations. This method saves computation because the prior probabilities $P(j/c_n)$ are calculated only once and the Tot_Prob vector is obtained from an intermediate step while computing the Prior_Prob matrix as follows:

First the conditional probability for each input data point is calculated for every j = 1 to N and a matrix Cond is obtained as follows:

Every column of the above matrix is multiplied by the prior probability of the corresponding component to obtain the matrix Weighted_Cond below:

Every element of Tot_Prob vector is obtained by summing all the elements of the corresponding row of the Weighted_Cond matrix. Next the Prior_Prob matrix is obtained by dividing elements of each row of the Weighted_Cond matrix by the element in the corresponding row of the Tot_Prob vector as follows where every term in the above matrix satisfies the equations. Thus the above described order of calculation of the Prior_Prob matrix results in fast updating of parameters in the EM algorithm.

EM is performed for every model order from M = 1 to 10 and the likelihood for the validation data is calculated each time. The available skin data is split into disjoint training and validation sets. The peak in the likelihood function gives the optimal model order. A third order model gave the peak likelihood for the validation data as evident in the plot of likelihood against model order. The mean points of the three component Gaussian model and the density functions of the three components. Note that the plots show scaled values for density functions.

This 3 component Gaussian mixture model (GMM) is used to obtain the skin probability image from an input color image. For the same test image, the corresponding skin probability image, calculated using the GMM, is shown show the same series of connected operators applied to the skin probability image obtained using GMM. The final result of segmentation. The segmentation results are also shown for the same test images as before, but using the GMM in obtaining the skin probability image. The false segmentation is because of a large skin colored background. The algorithm fails to detect one of the Biometrics due to the small size of the Biometric w.r.t the size of the largest Biometric detected (Normalized area operator). Also the middle Biometric, though segmented, has been merged with the skin colored background.

In general, false detection/segmentation can occur when there are large background regions whose color resembles that of skin. Also a true face may not be detected/segmented by the system when the face is merged with a background object having skin color. The use of the same structuring elements (in the open/close operations) irrespective of the size of face(s) in an input image may cause excessive erosion or dilation of the face component(s) in some cases. This may lead to the rejection of that particular component by one of the shape-based connected operators

It is observed that though the Gaussian mixture model provides a better approximation to skin color distribution than a unimodalgaussian, the results do not show an improvement in true segmentation performance. It is because the amount of skin data used for training both the models is small here. Hence the skin probability image obtained using the Gaussian mixture model does not show a significant improvement over that obtained using a unimodal Gaussian. But there is improvement in false segmentation rate. This may be because the mixture model is able to distinguish skin and non-skin colors which are close to each other in the chrominance space, better than the unimodal gaussian. Note that the skin probability image obtained using the mixture model is cleaner than that obtained using

a single component Gaussian, in terms of high probability values for background regions. A larger database of skin pixels might bring out a greater difference in the performance using the two different models.

Also, obtaining the skin probability image using a multimodal Gaussian is computationally more expensive than that using a unimodal Gaussian. This is because, for each pixel, the probability density function has to be computed from M components using GMM instead of 1 component for a unimodal Gaussian. Research has shown that given a large database of skin pixels, a mixture model gives a better approximation of the underlying distribution and a better skin classification performance than a single component model. Hence, usually a compromise is made between classification performance and computational overhead.

Now days, the paradigm of Face Mining is in use to analyze the actual emotions of the criminals or accused persons. Many times, the persons pretend to have a specific expression on their faces which can be further evaluated using Face Sentiment Mining. To use this approach, the integration of high performance open source libraries including OpenCV are used with the association of data mining based predictions of actual emotions. The Cloud Based Integrations are done so that the global identification and recognition of the persons can be done using biometric devices.

Following expressions of Face can be analyzed using Face Mining;

a. Actual and Pretend based Expressions
b. Postures and Angles
c. Fake and Actual Smile
d. Fake and Actual Eye Movements

In the current scenario, the Chinese Police and Investigation Authorities are using Face Expression Analysis Glasses to detect the criminals as per the reports from Telegraph.

Now days, the paradigm of Face Mining is in use to analyze the actual emotions of the criminals or accused persons. Many times, the persons pretend to have a specific expression on their faces which can be further evaluated using Face Sentiment Mining. To use this approach, the integration of high performance open source libraries including OpenCV are used with the association of data mining based predictions of actual emotions. The Cloud Based Integrations are done so that the global identification and recognition of the persons can be done using biometric devices.

Following expressions of Face can be analyzed using Face Mining

a. Actual and Pretend based Expressions
b. Postures and Angles
c. Fake and Actual Smile
d. Fake and Actual Eye Movements

In the current scenario, the Chinese Police and Investigation Authorities are using Face Expression Analysis Glasses to detect the criminals as per the reports from Telegraph.

The camera is connected by an electronic lead to a hand-held device.

The device has an app where police officers can process images they have taken of suspicious individuals.

"The facial information captured by the glasses will be sent back to a database for comparison with the information of suspects on the wanted list," Zhang Xiaolei, a local police official told the Global Times newspaper.

The app allows access to the database that also provides information on whether the suspect is on the run from police, and even their recent Internet history. To work with such approaches, there is need to integrate data mining and knowledge discovery approaches with the different phases of data mining and extraction mechanisms. Henceforth, is the detailed description of data mining and knowledge discovery in assorted perspectives.

Biometric based Data Mining and Knowledge Discovery refers to the unique process of deep

analytics of data on multiple and assorted dimensions. Any type and domain of data can be fetched and analyzed using KDD and Machine Intelligence. Figure 17 illustrate this

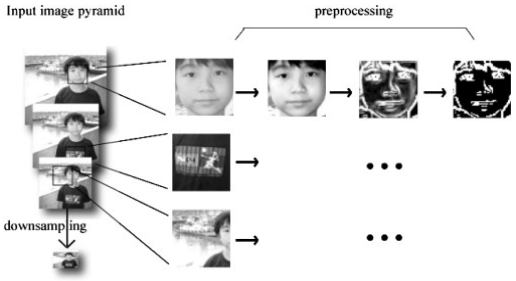


Figure 17: Data Mining and Associated Dimensions

This information will empower their clients the right to use, without any authorization. This response reveals the danger of information and related storage and encryption / decryption technology lead is in addition to luxury [107].

Biometric based data warehouse is responsible for the collection and storage of information engineering exact association. This information is collected works, then professional business information and check of data. Although the change in the overall data warehouse made, they are the subject of mainstream tilted sensing information stored is linked to an object or event occurring in reality. Check the data warehouse provided in order to provide a specific theme, rather than the company's functional and configured to have a part time varying from reliable sources. A data warehouse is a collection of exclusive data structure, which allows relatively quick and easy to carry large amounts of data over a wide range of queries. Traditional manufacturing information system is the first input data modification [108]. Since the production systems in need of such programs in the above-mentioned territories allows business complete, easy to run, which means that most data entry. On the other hand, fast and simple recovery of large amounts of data in its data storage system means allowed. This makes it suitable for so-called system-building enterprise decision support (DSS - Decision Support System).

By the means of the biometric integrated data warehouse, the purpose is to organize information in a manner well-run and analyze data. Although the data warehouse in FIG different behavior to calculate the information, they all share a significant amount of personality. Most data warehouse is a theme-oriented. This means that information is stored in a data warehouse in a way that allows it to be associated with the substance or the process of authenticity appearing and integrated data warehousing, transaction will be transferred back to the business system every day, which will allow data to be easily analyzed companies and organizations [109].

This is a significant data store control data is stable. As additional information, it should never be removed. This property is called non-volatile form of life. When a company uses the data warehouse to be stable; it will empower them to get better sympathy during their operations. Although, it should be known, some of the data warehouse is unstable. The reason for this is because many of the latest information terabyte data warehouse processing. Because they must be stored TB level data, many companies they have to be removed in the next scheduled time some people age. For example, some companies will methodically delete the 300-year-old data. What used to be built into the data storage; the correct data must be located. Typically, in order to more orders from the warehouse or historical information every day. Past information may be stored in a succession system, and are demanding removed. Typically, a data warehouse is situated on a mainframe server business. Selectively extracting and from different online transaction processing (OLTP) data applications and other data sources analyzed using hosted applications and user queries on the data warehouse database. From a data warehouse to emphasize useful analysis and access to different data sources to capture the data, but generally not from the point of view of who may need access to, and

sometimes begin specialized end user knowledge workers or local database [110].

With improvements in technology, as well as innovations in using data warehousing techniques, data warehouses have changed from Offline Operational Databases to include an Online Integrated data warehouse.

a. Offline preparation of a data warehouse is to store data, wherein the data is often not the banal and paste the data in real time from the network to the off-line system, where it can be used. It is often simpler and less technical type of data storage.
b. Offline data warehouse data storage on a regular basis to be effective, daily, weekly or monthly, and then stores the data contained in the arrangement, to any other place can do with it reported.
c. Real-time data is stored in a data warehouse where it is effective every moment with the arrival of the original data. For example, real-time data warehouse data may be from a point of sale system integration and efficient with each protocol is complete.
d. Integrated data warehouse data storage, available to other systems contact the system they manufacture. Some contain additional data warehouse is used by the data warehouse, so that they can correctly use the information to process and present information seems up.

Data warehouses and their architectures are different depending winning the particulars of an organization's state of affairs. Three ordinary architectures are:

a. Data Warehouse Basic
b. Data Warehouse Staging Area
c. Data Warehouse Staging Area integrated DataMarts

The metadata and uncooked data of a conventional OLTP system is there, as is an extra type of data, summary data. Summaries are very precious in data warehouses since they pre-compute long operation in go forward. For instance, a characteristic data warehouse inquiry is to get back amazing [111].

Biometric based Data mining, removing concealed prognostic information from large databases, it is very likely an influential new skill to help business centers most important information in its information warehouse. Technical data withdrawal forecast trends and behavior, enabling enterprises to develop practical, knowledge-driven decisions. Analysis tools go further than the typical display system provides decision to hold up nearly automatic procedure, potential analysis through data mining provides. Data mining tools can answer that traditionally covered time to decide business issues [112].

Biometric mining parameters include:

e. Associations - including the link for the event to another event related patterns.
f. Series or path review - including the associated pattern in which one event led to another event later.
g. Categories - including new models (the way data ALTER May the consequences of pre-arranged, but it does not matter).Cluster - to determine details and visual recording group not previously recognized.
h. Prediction / forecast analysis - including patterns in the data may lead to the prospect of a reasonable forecast.

The biometric integrated data mining technique is the consequence of an extended procedure of investigates and manufactured goods growth. This development begins when commerce information was primary stored on computer, constant with improvement in information right to use, and additional lately, generate technology that let user to find the way from side to side their information in real time. Data mining take this evolutionary procedure further than display data access and direction-finding to potential and practical in order release [113].

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V9I3201909
Volume 9 Issue 3 September 2019

There are many forms of data mining prediction. For example, a model based on education and other demographic factors predicted income. Related prediction probability (how likely this prediction is true?). Also known as the confident prediction probability (how much I have confidence that this could be a prediction?). Predictive data mining to produce some form of rules, which is the condition means that a given result [114]. This figure 18 explain.

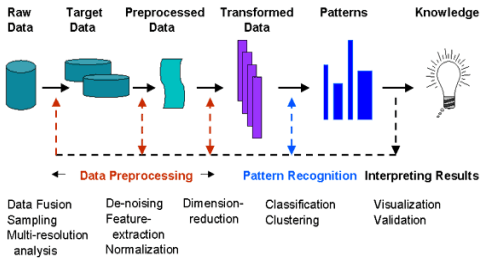


Figure 18. Face Recognition and Advance Mining Approach.

For example, rules may specify who holds a bachelor, lived in a neighborhood of people are likely to have more income than the regional average. There are rules associated supports (what proportion of the population to meet the rules?).

Data mining can be a lot of data derived from actionable information. For example, an urban planner may be used to predict the development of low-income housing program revenue model is based on statistical data. A car rental agent may recognize the use of a customer base to design a model for the promotion of high-value customers. Data mining is the main focus of the company with a strong focus on the consumer - the retail, financial, communications and marketing organization (figure 19). It enables companies to determine among "internal" factors, such as price, product positioning, or staff skills, and "external" factors such as economic indicators, competition, and customer demographics relationships. And, it enables them to determine the sales impact of customer satisfaction and corporate profits. Finally, it allows them to "in-depth" to view summary information detailed transactions [115].

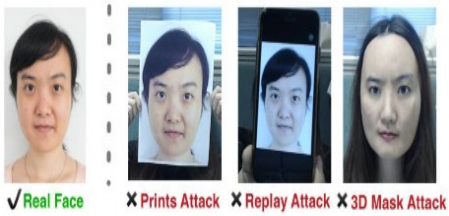


Figure 19. Face Features Mining

With biometric based object mining, retailers can use the customer purchase point of sale record the transmission based on individual purchase history targeted promotional activities. By mining demographic data from comment or warranty cards, the retailer can develop products and promotions to attract specific groups of customers. For example, Blockbuster Entertainment video rental history database of mine recommended leased to individual customers. American Express cardholders that the product can be analyzed according to their monthly expenditure [116].

Ideal starting point includes an internal data tracking along with all combinations of competitor activity external market data, customer contact data warehouse. Also, we may attempt to ridicule earlier to add external data properties of the new calculation. For example, rather than by the collection amount, we have the power to make a new quality: "total age of procurement Fig within 12 months more than 500 $" who often create great purchase customers may also be connected to whom react or not to take action available to customers. Thoughtful training data can be significantly better in may be exposed from the side to the other side of data mining order.

Withdrawal data can help you find patterns in the data and the associated influence means. However, the data mining itself does not work. They need to be familiar with your business, understanding your data, or to identify logical approach, it does not get rid of. Data mining data found secreted information, but it cannot tell you information related to your value [117].

Our strength is now conscious significantly as a result of the operation mode of the data over time. Data mining can determine a new pattern of increase may not be easy to discern immediately the other side of confirmed or are qualified to interpret from one side to the experience [118].

Data mining in large records to infiltrate similarity obtained its first commercial name between precious - precious ore veins and dismantling the mountain - for example, found that rose to connect the scanner gigabytes of data in food. Both processes require either screened from side to side a lot of material or clever curious to find it exactly the value. Sufficient size, quality, data mining technology known to the database can be, as long as these functions generate new business opportunities [119].

Automatic forecasting trends and behavior: Biometric mining or automatic discovery information is the process of prediction of large databases. Prior to the treatment it means that the user can be mechanically more models to try to appreciate the complex data. The high speed makes it wise to check a large number of user data. Better database, in the rotation and make way for a better prediction. The database can together better depth and width. Additional rows: Better samples give way lower opinion errors and inconsistency, and allow users to make inferences about small but important segments of a population [120].

In scenario of cloud integrated with biometric mining procedures for revocation is an example of cloud computing is ideal. With cloud computing and processing methodically stabbing extra every choice, it became a huge area to focus on biometric mining. Cloud based biometric mining and computing refers to the daily work of grasping the trend of the original Internet service for server cloud. Cloud computing Data mining is the way to remove the mining process data in the cloud from an invisible grid or semi-structured data source controls allow organizations to unify software and data storage management, and they are efficient, reliable and secure service guarantees customers. Cloud computing refers to the software, hardware, and services through the Internet, in the cloud data mining software in this manner also available [121].

From side to side through a cloud computing data mining can be reduced to maintain a modest company to benefit from data mining tools obstacle. Cloud computing is a new trend to rely on a network server to handle the task of cloud services. Cloud computing structured information in the data mining process to extract unstructured or semi-structured Web data sources in the cloud of data mining enabling enterprises to focus on software and data storage management, and for their efficient, reliable and safe service to protect customers. data mining technology, cloud computing will allow users to return to almost significant, including data warehouses, reducing infrastructure costs and storage space.

Biometric Mining using cloud computing has become an area as it now covers almost all business and scientific computing for forensic applications. The cloud provider provides a tool for data mining for better service. On the other side external attackers can use data mining tasks to access private data unauthorized by interacting it. The interaction data may involve two factors (i) the appropriate amount of data (ii) suitable mining algorithms. There are a number of mining algorithms that can be used to interact private data and therefore threatens the privacy of the data. In current era, the domain of Cloud Computing and Distributed Applications are key domains of research from last decade and number of algorithms and approaches devised so far in the sub domains of multiprocessor architectures and high performance computing. Various algorithms and approaches including nature inspired algorithms are developed and implemented to cope up the issues of performance and effectiveness. A Confusion Matrix assesses the degree of classification (or cluster) algorithm. Mutual Information is an information theory that deals with information between clusters and ground truth classifications. It is detected by a non-linear similarity between

two clusters. After fine tuning the mutual information of the correct opportunity to obtain a less bias in a different cluster. This figure illustrate this:

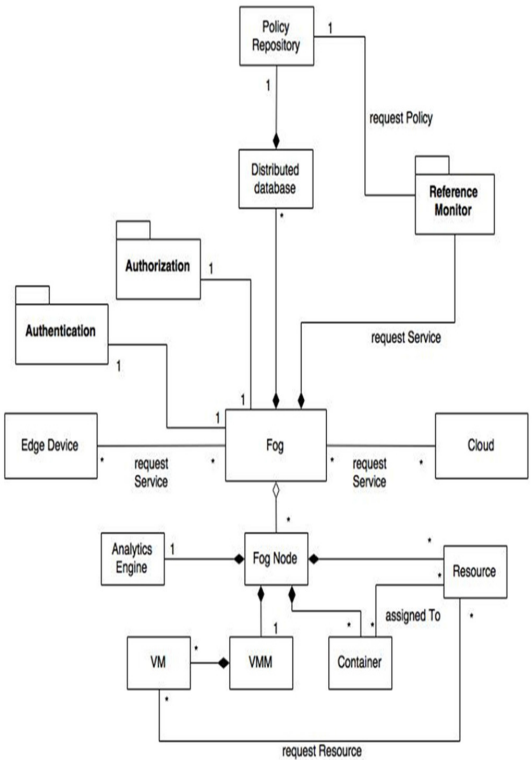


Figure 20: Dimensions for Face Recognition in Cloud [121]

In the above diagram in figure 20, there is a biometric based object and fog node which provides the unified or joint approach of all the operations in the cloud. In our proposed approach, there are multiple modules including security, integrity, cryptography and trust evaluation. All these factors are closely related and joined with the centralized cloud platform using fog. Main disadvantage of well-known "K-means" cluster procedure is its sensitivity to the preliminary decision about number of group centers, with a possible non-optimum convergence to achieve the best results at the global level, where it is generally need to know in advance the number of cluster for a particular data collection. Wei-Zhong and et. [121], mentioned that they had improved the initialization process by increasing the percentage sequence of the part of the cluster related to similar groups. Word "improvement" recommends that many of the proposals which are initialization method is far from ideal, especially in the light of the number of papers referred to this point. Further, "It may be found that a number of relatively weak and delicate sequence pattern is not easy to be found by the traditional "K-means" algorithms.

The author in the above work goes on to explain that, for many initialization strategies, particularly Random, Forgy, Macqueen, and Kaufmann - require selection of the centers to define a deterministic mapping is not appropriate choice of initial point it may result in distorted or incorrect partition. They select Fuzzy approach in implementing the "traditional" "K-means" algorithm. They also pointed out that methods are not appropriate for their purpose. Authors go on proposing a "new greedy initialization method to overcome potential problems of random initialization". The iterative method runs several time for each bigger iteration. This is called run. So every run contains several time In every run, new cluster centers can be randomly defined for the clustering of the form of a structure similarity, and that the choice of, and their distance from the selected points will be selected to initialize the collection. These points will be added to the initialize the array after minimum distance from the new point is larger than the specified distance.

V. CONCLUSION

Human Identification is specifically connected with the methodologies with the biometric location and preparing of the datasets so the investigation of specific individual should be possible for measurable applications. The researching specialists utilize these methodologies for criminal distinguishing proof and by and large examination of the human attributes. In this work, the various measurements and

viewpoints of the human qualities as far as biometric are indicated with the delineation of the datasets including natural attributes of EEG information. The natural attributes can be utilized for the ID of person including the mind waves. Likewise, this work calls attention to the varying focuses related with the biometric applications.

REFERENCES

[1] Pinto, J.R., Cardoso, J.S., Lourenço, A. and Carreiras, C., 2017. Towards a continuous biometric system based on ECG signals acquired on the steering wheel. Sensors, 17(10), p.2228.

[2] Douglas, M., Bailey, K., Leeney, M. and Curran, K., 2018. An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77(13), pp.17333-17373.

[3] Siegal, J., Rowell, S. and Hintz, T., Open Invention Network LLC, 2018. Method and system for providing online authentication utilizing biometric data. U.S. Patent 9,911,146.

[4] Kiserud, T., Piaggio, G., Carroli, G., Widmer, M., Carvalho, J., Jensen, L.N., Giordano, D., Cecatti, J.G., Aleem, H.A., Talegawkar, S.A. and Benachi, A., 2017. The World Health Organization fetal growth charts: a multinational longitudinal study of ultrasound biometric measurements and estimated fetal weight. PLoS medicine, 14(1), p.e1002220.

[5] Jones, N.A., Vasgaard, A. and Jones, M.A., Walmart Apollo LLC, 2018. Shopping Cart with RFID and Biometric Components and Associated Systems and Methods. U.S. Patent Application 15/879,589.

[6] Ghosh, S., Majumder, A., Goswami, J., Kumar, A., Mohanty, S.P. and Bhattacharyya, B.K., 2017. Swing-pay: One card meets all user payment and identity needs: A digital card module using NFC and biometric authentication for peer-to-peer payment. IEEE Consumer Electronics Magazine, 6(1), pp.82-93.

[7] Weising, G., Sony Interactive Entertainment Inc, 2017. Biometric interface for a handheld device. U.S. Patent 9,557,814.

[8] Radhakrishna Rao, C., 1952. Advanced statistical methods in biometric research. A Division of Macmillan Publishing Co, Inc New York; Collier-Macmillan Publishers; London.

[9] Wildes, R.P., 1997. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, 85(9), pp.1348-1363.

[10] Prabhakar, S., Pankanti, S. and Jain, A.K., 2003. Biometric recognition: Security and privacy concerns. IEEE security & privacy, (2), pp.33-42.

[11] Jain, A., Hong, L. and Pankanti, S., 2000. Biometric identification. Communications of the ACM, 43(2), pp.90-98.

[12] Wayman, J., Jain, A., Maltoni, D. and Maio, D., 2005. An introduction to biometric authentication systems. In Biometric Systems (pp. 1-20). Springer, London.

[13] Uludag, U., Pankanti, S., Prabhakar, S. and Jain, A.K., 2004. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6), pp.948-960.

[14] Kumar, A., Wong, D.C., Shen, H.C. and Jain, A.K., 2003, June. Personal verification using palmprint and hand geometry biometric. In International Conference on Audio-and Video-Based Biometric Person Authentication (pp. 668-678). Springer, Berlin, Heidelberg.

[15] Harris, J.A. and Benedict, F.G., 1918. A biometric study of human basal metabolism. Proceedings of the National Academy of Sciences, 4(12), pp.370-373.

[16] Zhao, W., Krishnaswamy, A., Chellappa, R., Swets, D.L. and Weng, J., 1998. Discriminant analysis of principal components for face recognition. In Face Recognition (pp. 73-85). Springer, Berlin, Heidelberg.

[17] Turk, M.A. and Pentland, A.P., 1991, June. Face recognition using eigenfaces. In Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91, IEEE Computer Society Conference on (pp. 586-591). IEEE.

[18] Wiskott, L., Fellous, J.M., Krüger, N. and Von Der Malsburg, C., 1997, September. Face recognition by elastic bunch graph matching.

In International Conference on Computer Analysis of Images and Patterns (pp. 456-463). Springer, Berlin, Heidelberg.

[19] Wright, J., Yang, A.Y., Ganesh, A., Sastry, S.S. and Ma, Y., 2009. Robust face recognition via sparse representation. IEEE transactions on pattern analysis and machine intelligence, 31(2), pp.210-227.

[20] Daugman, J., 2009. How iris recognition works. In The essential guide to image processing (pp. 715-739).

[21] Lim, S., Lee, K., Byeon, O. and Kim, T., 2001. Efficient iris recognition through improvement of feature vector and classifier. ETRI journal, 23(2), pp.61-70.

[22] Daugman, J., 2003. The importance of being random: statistical principles of iris recognition. Pattern recognition, 36(2), pp.279-291.

[23] Ma, L., Tan, T., Wang, Y. and Zhang, D., 2004. Efficient iris recognition by characterizing key local variations. IEEE Transactions on Image processing, 13(6), pp.739-750.

[24] Jain, A.K., Ross, A. and Prabhakar, S., 2004. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), pp.4-20.

[25] Jain, M.B., Srinivas, M.B. and Jain, A., 2008, October. A novel web based expert system architecture for on-line and off-line fault diagnosis and control (FDC) of power system equipment. In 2008 Joint International Conference on Power System Technology and IEEE Power India Conference (pp. 1-5). IEEE.

[26] Delac, K. and Grgic, M., 2004, June. A survey of biometric recognition methods. In 46th International Symposium Electronics in Marine (Vol. 46, pp. 16-18).

[27] Rashid, R.A., Mahalin, N.H., Sarijari, M.A. and Aziz, A.A.A., 2008, May. Security system using biometric technology: Design and implementation of Voice Recognition System (VRS). In Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on (pp. 898-902). IEEE.

[28] Venayagamoorthy, G.K., Moonasar, V. and Sandrasegaran, K., 1998, September. Voice recognition using neural networks. In Communications and Signal Processing, 1998. COMSIG'98. Proceedings of the 1998 South African Symposium on (pp. 29-32). IEEE.

[29] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S., 2009. Handbook of fingerprint recognition. Springer Science & Business Media.

[30] Jain, A.K., Ross, A. and Prabhakar, S., 2004. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), pp.4-20.

[31] Prabhakar, S., Pankanti, S. and Jain, A.K., 2003. Biometric recognition: Security and privacy concerns. IEEE security & privacy, (2), pp.33-42.

[32] Van der Putte, T. and Keuning, J., 2000. Biometrical fingerprint recognition: don't get your fingers burned. In Smart Card Research and Advanced Applications (pp. 289-303). Springer, Boston, MA.

[33] Kostílek, M. and Šťastný, J., 2012, September. EEG biometric identification: Repeatability and influence of movement-related EEG. In Applied Electronics (AE), 2012 International Conference on (pp. 147-150). IEEE.

[34] DelPozo-Banos, M., Travieso, C.M., Weidemann, C.T. and Alonso, J.B., 2015. EEG biometric identification: a thorough exploration of the time-frequency domain. Journal of neural engineering, 12(5), p.056019.

[35] Paranjape, R.B., Mahovsky, J., Benedicenti, L. and Koles, Z., 2001. The electroencephalogram as a biometric. In Electrical and Computer Engineering, 2001. Canadian Conference on (Vol. 2, pp. 1363-1366). IEEE.

[36] Ravi, K.V.R. and Palaniappan, R., 2007, December. A minimal channel set for individual identification with EEG biometric using genetic algorithm. In Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on (Vol. 2, pp. 328-332). IEEE.

[37] Saad M Darwish, Adel A El-Zoghabi, Oday A Hassen, "A Modified Walk Recognition System for Human Identification Based on Uncertainty Eigen Gait", International

conference of Machine Learning and Computing (IACSIT), Sarawak, Malaysia. 4 (4), 346, 2014.

[38] Oday A. Hassen, "Big Data Based Machine Learning and Predictive Analytics using Apache Mahout and Storm", Journals 2016, Thomson routers, impact factor 4.179.

[39] Oday A. Hassen, "Preventive Approach against HULK Attack in Network Environment". Journal 2017.International Journal of Computing and Business Research (IJCBR) Thomson routers, impact factor 4.179.

[40] Oday A. Hassen, "A Paramedic Evolution of Face Smile Detection". Journal 2017. Impact factors 4.179.

[41] Oday A. Hassen, Nur Azman Abo HAAR in Effectual Approach for Evaluation and Prediction of Face Smile Detection". Journal 2017.

[42] Oday A. Hassen, "Face smile and related dimension analysis using deep learning", International Journal of Enterprise Computing and Business Systems.

[43] Oday A. Hassen, Jamal Kh-Madhloom, Ali Abdullah Ali, Z, Z, Abidin, "Face Smile Detection and Predictive Recognition Using Binary Locality Preserving Projections", Scopus, USA, 2018.

[44] Ali Abdullah Ali, Oday A. Hassen, Mustafa Raheem Neamah, Jamal Kh-Madhloom, "Big Data Enabled Approach for Predictive Analysis of Accuracy Aware Face Smile Detection in Assorted Domains", Scopus, USA, 2018.

[45] Mustafa Raheem Neamah, Jamal Kh-Madhloom, Oday A. Hassen, Z, Z, Abidin, "Fuzzy Logic Integrated Security Aware Algorithm for Vulnerability Avoidance in Network Environment", Scopus, USA, 2018.

[46] Bhardwaj, Aditya, and C. Rama Krishna. "Efficient multistage bandwidth allocation technique for virtual machine migration in cloud computing." Journal of Intelligent & Fuzzy Systems Preprint: pp. 1-14, 2018.

[47] Griffith, A., 2006. An Exploration of the OpenEEG Project. CHG Wright's BioData Systems.

[48] Liu, Y., Lim, W.L., Hou, X., Sourina, O. and Wang, L., 2015, October. Prediction of human cognitive abilities based on EEG measurements. In Cyberworlds (CW), 2015 International Conference on (pp. 161-164). IEEE.

[49] Reina, L.F., Martínez, G., Valdeavellano, M., Destarac, M. and Esquit, C., 2010, September. ANIMA: Non-conventional brain-computer interfaces in robot control through electroencephalography and electrooculography, ARP module. In Mexican Conference on Pattern Recognition (pp. 71-79). Springer, Berlin, Heidelberg.

[50] Lawhern, V.J., Solon, A.J., Waytowich, N.R., Gordon, S.M., Hung, C.P. and Lance, B.J., 2016. Eegnet: A compact convolutional network for eeg-based brain-computer interfaces. arXiv preprint arXiv:1611.08024.

[51] Hassan, M., Shamas, M., Khalil, M., El Falou, W. and Wendling, F., 2015. EEGNET: an open source tool for analyzing and visualizing M/EEG connectome. PloS one, 10(9), p.e0138297.

[52] Felver, J.C., Tipsord, J.M., Morris, M.J., Racer, K.H. and Dishion, T.J., 2017. The effects of mindfulness-based intervention on children's attention regulation. Journal of Attention Disorders, 21(10), pp.872-881.

[53] Vanderhasselt, M.A., De Raedt, R., Brunoni, A.R., Campanhã, C., Baeken, C., Remue, J. and Boggio, P.S., 2013. tDCS over the left prefrontal cortex enhances cognitive control for positive affective stimuli. PloS one, 8(5), p.e62219.

[54] Schlögl, A. and Brunner, C., 2008. BioSig: a free and open source software library for BCI research. Computer, 41(10).

[55] Vidaurre, C., Sander, T.H. and Schlögl, A., 2011. BioSig: the free and open source software library for biomedical signal processing. Computational intelligence and neuroscience, 2011.

[56] Parvin, B., Yang, Q., Fontenay, G. and Barcellos-Hoff, M.H., 2002. BioSig: an imaging bioinformatic system for studying phenomic. Computer, (7), pp.65-71.

[57] Parvin, B., Yang, Q., Fontenay, G. and Barcellos-Hoff, M.H., 2003. BioSig: an

imaging bioinformatics system for phenotypic analysis. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 33(5), pp.814-824.

[58] Parvin, B., Cong, G., Fontenay, G., Taylor, J., Henshall, R. and Barcellos-Hoff, M.H., 2000. BioSig: A bioinformatic system for studying the mechanism of inter-cell signaling. In Bio-Informatics and Biomedical Engineering, 2000. Proceedings. IEEE International Symposium on (pp. 281-288). IEEE.

[59] Gremme, G., Steinbiss, S. and Kurtz, S., 2013. GenomeTools: a comprehensive software library for efficient processing of structured genome annotations. IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB), 10(3), pp.645-656.

[60] Casler, M.D., Tobias, C.M., Kaeppler, S.M., Buell, C.R., Wang, Z.Y., Cao, P., Schmutz, J. and Ronald, P., 2011. The switchgrass genome: tools and strategies. The Plant Genome, 4(3), pp.273-282.

[61] Lee, W. and Chen, S.L., 2002. Genome-tools: a flexible package for genome sequence analysis. Biotechniques, 33(6), pp.1334-1341.

[62] Plasmodium Genome Database Collaborative, 2001. PlasmoDB: An integrative database of the Plasmodium falciparum genome. Tools for accessing and analyzing finished and unfinished sequence data. Nucleic acids research, 29(1), pp.66-69.

[63] Cock, P.J., Antao, T., Chang, J.T., Chapman, B.A., Cox, C.J., Dalke, A., Friedberg, I., Hamelryck, T., Kauff, F., Wilczynski, B. and De Hoon, M.J., 2009. Biopython: freely available Python tools for computational molecular biology and bioinformatics. Bioinformatics, 25(11), pp.1422-1423.

[64] Han, M.V. and Zmasek, C.M., 2009. phyloXML: XML for evolutionary biology and comparative genomics. BMC bioinformatics, 10(1), p.356.

[65] Gentleman, R.C., Carey, V.J., Bates, D.M., Bolstad, B., Dettling, M., Dudoit, S., Ellis, B., Gautier, L., Ge, Y., Gentry, J. and Hornik, K., 2004. Bioconductor: open software development for computational biology and bioinformatics. Genome biology, 5(10), p.R80.

[66] Anders, S., Pyl, P.T. and Huber, W., 2015. HTSeq—a Python framework to work with high-throughput sequencing data. Bioinformatics, 31(2), pp.166-169.

[67] Perfect, J.R., 2000. Cryptococcosis. In Atlas of Infectious Diseases (pp. 79-93). Current Medicine Group, London.

[68] Rabouille, C. and Spiro, R.G., 1992. Nonselective utilization of the endomannosidase pathway for processing glycoproteins by human hepatoma (HepG2) cells. Journal of Biological Chemistry, 267(16), pp.11573-11578.

[69] Saeys, Y., Inza, I. and Larrañaga, P., 2007. A review of feature selection techniques in bioinformatics. 23(19), pp.2507-2517.

[70] Cock, P.J., Antao, T., Chang, J.T., Chapman, B.A., Cox, C.J., Dalke, A., Friedberg, I., Hamelryck, T., Kauff, F., Wilczynski, B. and De Hoon, M.J., 2009. Biopython: freely available Python tools for computational molecular biology and bioinformatics. Bioinformatics, 25(11), pp.1422-1423.

[71] Frank, E., Hall, M., Trigg, L., Holmes, G. and Witten, I.H., 2004. Data mining in bioinformatics using Weka. Bioinformatics, 20(15), pp.2479-2481.

[72] Paradis, E., Claude, J. and Strimmer, K., 2004. APE: analyses of phylogenetics and evolution in R language. Bioinformatics, 20(2), pp.289-290.

[73] Stevens, R., Baker, P., Bechhofer, S., Ng, G., Jacoby, A., Paton, N.W., Goble, C.A. and Brass, A., 2000. TAMBIS: transparent access to multiple bioinformatics information sources. Bioinformatics, 16(2), pp.184-186.

[74] Jain, A.K., Hong, L. and Kulkarni, Y., 1999, March. A multimodal biometric system using fingerprint, face and speech. In Proceedings of 2nd Int'l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC (pp. 182-187).

[75] Negin, M., Chmielewski, T.A., Salganicoff, M., Von Seelen, U.M., Venetainer, P.L. and Zhang, G.G., 2000. An iris biometric system

for public and personal use. Computer, 33(2), pp.70-75.

[76] Gamboa, H. and Fred, A., 2004, August. A behavioral biometric system based on human-computer interaction. In Biometric Technology for Human Identification (Vol. 5404, pp. 381-393). International Society for Optics and Photonics.

[77] Adam, H., Neven, H. and Steffens, J.B., Google Inc, 2010. Image based multi-biometric system and method. U.S. Patent 7,697,735.

[78] Monwar, M.M. and Gavrilova, M.L., 2009. Multimodal biometric system using rank-level fusion approach. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 39(4), pp.867-878.

[79] Jain, A., Hong, L. and Pankanti, S., 2000. Biometric identification. Communications of the ACM, 43(2), pp.90-98.

[80] Jain, A.K. and Nandakumar, K., 2012. Biometric Authentication: System Security and User Privacy. IEEE Computer, 45(11), pp.87-92.

[81] Sanchez-Reillo, R., Sanchez-Avila, C. and Gonzalez-Marcos, A., 2000. Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis & Machine Intelligence, (10), pp.1168-1171.

[82] Prabhakar, S., Pankanti, S. and Jain, A.K., 2003. Biometric recognition: Security and privacy concerns. IEEE security & privacy, (2), pp.33-42.

[83] Jain, A.K., Flynn, P. and Ross, A.A. eds., 2007. Handbook of biometrics. Springer Science & Business Media.

[84] Lee, J.C., 2012. A novel biometric system based on palm vein image. Pattern Recognition Letters, 33(12), pp.1520-1528.

[85] Meraoumia, A., Chitroub, S. and Bouridane, A., 2011, June. Fusion of finger-knuckle-print and palmprint for an efficient multi-biometric system of person recognition. In Communications (ICC), 2011 IEEE International Conference on (pp. 1-5). IEEE.

[86] Kharon, J.J. and Rozenberg, R., BIOLINK TECHNOLOGIES INTERNATIONAL Inc, 2002. Biometric system for biometric input, comparison, authentication and access control and method therefor. U.S. Patent 6,487,662.

[87] Wayman, J.L., 1999. Error rate equations for the general biometric system. IEEE Robotics & Automation Magazine, 6(1), pp.35-48.

[88] Ribarić, S., Ribarić, D. and Pavešić, N., 2003. Multimodal biometric user-identification system for network-based applications. IEE Proceedings-Vision, Image and Signal Processing, 150(6), pp.409-416.

[89] Pankanti, S., Bolle, R.M. and Jain, A., 2000. Biometrics: The future of identification [guest eeditors' introduction]. Computer, 33(2), pp.46-49.

[90] Denimarck, P., Bellis, D. and McAllister, C., Datalogic Scanning Inc, 2003. Biometric system and method for identifying a customer upon entering a retail establishment. U.S. Patent Application 09/909,576.

[91] Klontz, J.C., Klare, B.F., Klum, S., Jain, A.K. and Burge, M.J., 2013, September. Open source biometric recognition. In Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on (pp. 1-8). IEEE.

[92] Park, U., Jillela, R.R., Ross, A. and Jain, A.K., 2011. Periocular biometrics in the visible spectrum. IEEE Transactions on Information Forensics and Security, 6(1), pp.96-106.

[93] Darwaish, S.F., Moradian, E., Rahmani, T. and Knauer, M., 2014. Biometric identification on android smartphones. Procedia Computer Science, 35, pp.832-841.

[94] Ouanan, H., Ouanan, M. and Aksasse, B., 2015. Implementation and optimization of face detection frameworkbased on OpenCV library on mobile platforms using Davinci's technology. International Journal of Imaging and Robotics™, 15(4), pp.81-88.

[95] Siswanto, A.R.S., Nugroho, A.S. and Galinium, M., 2014, September. Implementation of face recognition algorithm for biometrics based time attendance system. In ICT for Smart Society (ICISS), 2014 International Conference on (pp. 149-154). IEEE.

[96] Velardo, C. and Dugelay, J.L., 2011, November. Real time extraction of body soft biometric from 3d videos. In Proceedings of the 19th ACM international conference on Multimedia (pp. 781-782). ACM.

[97] Dantcheva, A., Dugelay, J.L. and Elia, P., 2010, October. Person recognition using a bag of facial soft biometrics (BoFSB). In Multimedia Signal Processing (MMSP), 2010 IEEE International Workshop on (pp. 511-516). IEEE.

[98] Marcel, S., McCool, C., Matějka, P., Ahonen, T., Černocký, J., Chakraborty, S., Balasubramanian, V., Panchanathan, S., Chan, C.H., Kittler, J. and Poh, N., 2010. On the results of the first mobile biometry (MOBIO) face and speaker verification evaluation. In Recognizing Patterns in Signals, Speech, Images and Videos (pp. 210-225). Springer, Berlin, Heidelberg.

[99] Renuka, M., Kumar, R.S., Vimani, B., Babu, N.G. and Radhesyam, V., 2017. Biometric Identification Using Opencv Based On Arduino.

[100] Marinescu, L., 2015. Security System for Mobile Voting with Biometrics. Journal of Mobile, Embedded and Distributed Systems, 7(3), pp.100-106.

[101] Snelick, R., Uludag, U., Mink, A., Indovina, M. and Jain, A., 2005. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. IEEE transactions on pattern analysis and machine intelligence, 27(3), pp.450-455.

[102] Feng, Y.C. and Yuen, P.C., 2006, June. Protecting face biometric data on smartcard with reed-solomon code. In Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on (pp. 29-29). IEEE.

[103] Kelkboom, E.J., Gökberk, B., Kevenaar, T.A., Akkermans, A.H. and van der Veen, M., 2007, August. "3D face": biometric template protection for 3D face recognition. In International Conference on Biometrics (pp. 566-573). Springer, Berlin, Heidelberg.

[104] Määttä, J., Hadid, A. and Pietikäinen, M., 2011, October. Face spoofing detection from single images using micro-texture analysis. In Biometrics (IJCB), 2011 international joint conference on (pp. 1-7). IEEE.

[105] Boodoo, N.B. and Subramanian, R.K., 2009. Robust multi biometric recognition using face and ear images. arXiv preprint arXiv:0912.0955.

[106] Arandjelovic, O. and Hammoud, R., 2006, June. Multi-sensory face biometric fusion (for personal identification). In Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on (pp. 128-128). IEEE.

[107] Feng, Y.C., Yuen, P.C. and Jain, A.K., 2008, March. A hybrid approach for face template protection. In Biometric Technology for Human Identification V (Vol. 6944, p. 694408). International Society for Optics and Photonics.

[108] Haghighat, M., Zonouz, S. and Abdel-Mottaleb, M., 2015. CloudID: Trustworthy cloud-based and cross-enterprise biometric identification. Expert Systems with Applications, 42(21), pp.7905-7916.

[109] Kohlwey, E., Sussman, A., Trost, J. and Maurer, A., 2011, July. Leveraging the cloud for big data biometrics: Meeting the performance requirements of the next generation biometric systems. In Services (SERVICES), 2011 IEEE World Congress on (pp. 597-601). IEEE.

[110] Peer, P., Bule, J, Gros, J.Ž. and Štruc, V., 2013. Building cloud-based biometric services. Informatica, 37(2).

[111] Yuan, J. and Yu, S., 2013, April. Efficient privacy-preserving biometric identification in cloud computing. In INFOCOM, 2013 Proceedings IEEE (pp. 2652-2660). IEEE.

[112] Vallabhu, H. and Satyanarayana, R.V., 2012. Biometric authentication as a service on cloud: Novel solution. International Journal of Soft Computing and Engineering, 2(4), p.163.

[113] Stojmenovic, M., 2012, September. Mobile cloud computing for biometric applications. In 2012 15th International Conference on Network-Based Information Systems (pp. 654-659). IEEE.

[114] Omri, F., Hamila, R., Foufou, S. and Jarraya, M., 2012, April. Cloud-ready biometric system for mobile security access.

In International Conference on Networked Digital Technologies (pp. 192-200). Springer, Berlin, Heidelberg.

[115] Martınez, D.G., Castano, F.J.G., Rúa, E.A., Castro, J.L.A. and Silva, D.A.R., 2011, September. Secure crypto-biometric system for cloud computing. In Proc. 1st Int'l Workshop on Securing Services on the Cloud (pp. 38-45).

[116] Zhu, H.H., He, Q.H., Tang, H. and Cao, W.H., 2011. Voiceprint-biometric template design and authentication based on cloud computing security.

[117] Suryadevara, S., Kapoor, S., Dhatterwal, S., Naaz, R. and Sharma, A., 2011. Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security. In Int Conf Inform Network Technol (Vol. 4).

[118] Panchumarthy, R., Subramanian, R. and Sarkar, S., 2012, November. Biometric evaluation on the cloud: A case study with humanid gait challenge. In Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing (pp. 219-222). IEEE Computer Society.

[119] Dakhane, D.M. and Arokar, A.A., 2012. Data secuity in cloud computing for biometric application. International Journal of Scientific & Engineering Research, 3(6), p.1.

[120] Kochetkov, A., 2013. Cloud-based biometric services: just a matter of time. Biometric Technology Today, 2013(5), pp.8-11.

[121] Omar, M.N., Salleh, M. and Bakhtiari, M., 2014, August. Biometric encryption to enhance confidentiality in Cloud computing. In Biometrics and Security Technologies (ISBAST), 2014 International Symposium on (pp. 45-50). IEEE.

About the Author:

Oday A. Hassen Received the B.Sc. degree in mathematics from the Department of Mathematics, University of Mustansiriyah, Iraq in 2004, and M.Sc from department of information technology, Science College, Alexandria University, Egypt. Currently he is PHD student in university Technical Melaka (UTeM), Malaysia until now. His research and professional interests include image processing, authentication, security technologies, and pattern recognition.