# Establishing User Authentication using Face Geometry

Indradip Banerjee
Department of CSE, National Institute of Technology, Durgapur, West Bengal, India.

Dipankar Chatterjee
Department of CA, Management Institute of Durgapur, Rajbandh, West Bengal, India.

Souvik Bhattacharyya
Department of CSE, University Institute of Technology, Burdwan, West Bengal, India.

Gautam Sanyal
Department of CSE, National Institute of Technology, Durgapur, West Bengal, India.

## ABSTRACT
The use of digital media or information is very precarious for increasing of hacker in the nation. So the information security is one of the commanding articles to shield it. The biometric information security is one information security mechanism, which is powerful than conventional cryptography system. The biometric system plays a vital role in person recognition. The main reason of biometry is so popular in security, because there is no risk if something might be lost or stolen in case of traditional IDs and passwords. After several comparisons among possible features of a human face geometry processing approaches, an authorized person recognition system have been designed and developed. Freely accessible sample faces of different persons are used in this novel biometric authentication system. Furthermore, the functionality to extract features of face has been implemented to compare the new samples with user templates. The implementation has been evaluated by the FAR (False Acceptance Rate) and FRR (False Rejection Rate) of the system in order to reduce FAR. Examining the Distance between some objects of faces and angles between objects points are used in this system and this is the novelty.

## Keywords
Biometric Approach, Face Geometry, Euclidean distance, City block metric, Minkowski distance, Chebychev distance, Cosine distance.

## 1. INTRODUCTION
Automatic recognition system of an individual derived from the physiological and behavioural [1-6] characteristic is describing the Biometric security system. The term "biometrics" is derived from a Greek words bio means "life" and metric means "to measure". Biometric systems ascertain a person's identity based on pattern analyses carried out on specific human traits [2,3]. Physiological based biometric systems consist of fingerprints, retina, iris, hand geometry, hand vein, ear shape and facial recognition systems. These features are typically unchangeable exclusive of causing disturbance to human being. On the other hand, behavioural biometric characteristics are later stabilizing over a period of time. Some of the examples of behavioural-based biometric systems are voice recognition, keystroke dynamics, signature verification and gait analysis. Figure 1 describes the classification of biometric techniques and Figure 2 describes the process involved in using a biometric system for security. In existing system there are various methods have been developed by most of the researchers using different biometric features. Some of them are discussed below:

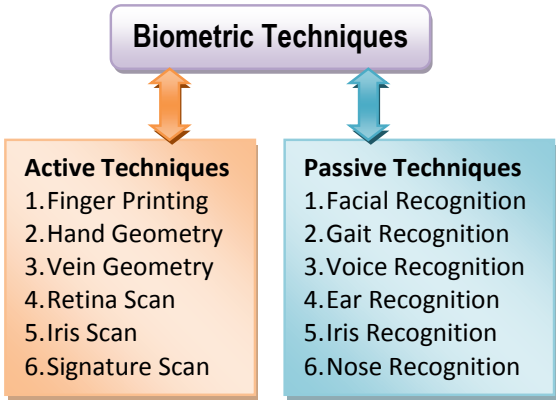


**Fig 1: Classification of biometric techniques**

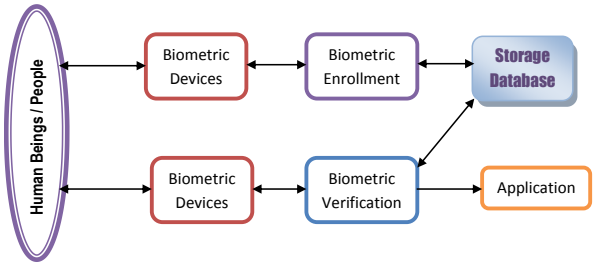


**Fig 2: How a biometric system work**

**Fingerprints:** Fingerprint [7] one of the biometric security which is based on fingertip pattern recognition. There are three basic patterns of fingerprint ridges: 1) Arch: Ridges enter from one side of the finger, forming in the center and exit the other side of the finger. 2) Loop: Ridges enter from one side of a finger then form a curve and then exit on that same side. 3) Whorl: The ridges form circularly around a central point on the finger. There are several approaches to fingerprint verification. Some of them follow the conventional method of matching finer points; others use straight pattern matching mechanism. Some of fingerprint verification approaches can detect a live finger where as some cannot. Various fingerprint devices are available than any other biometric system. Scientists have found that family members are inherited patterns, so they often share the same general fingerprint patterns.

**Retina:** Analyzing the complex structure of the capillaries that is the layer of blood vessels at retina which is not entirely genetically determined i.e. back of eye is involved in this

procedure. For that reason each person's retina is unique. Find out the unique patterns of the retina using low intensity light source through an optical coupler is the process to identify. The technology can work well but it is not convenient if human uses glasses or having close contact with the reading device [8]. The Advantages in this technique is Low rates of false positives and false negative. This technique is highly reliable because no two people have the same retinal pattern. But the measurement accuracy affected by various eye diseases like cataracts, diabetes and glaucoma or retinal degenerative disorders.

**Face:** Face biometry [9] depending on analyzing facial characteristics. It involves a digital camera to grow a facial image of the user for authentication. In this system it automatically identifying or verifying a person from an image. One of the ways to do this is to compare some selected facial features from the image and a facial database. Among the different biometric techniques, facial recognition may not be the most reliable and efficient.

**Hand Geometry:** In this mechanism the shape of the human hand is computed and analyzes [10]. Hand geometry is based on the palm and fingers structure, width of the fingers in different places, length of the fingers, thickness of the palm area, etc. while these measurements are not very distinctive among people, so hand geometry be capable for identity verification, i.e. personal authentication. This biometric system recommends a good stability of performance characteristics and is reasonably straightforward to apply. This is suitable where lots of users are there in the system and they access infrequently. In this system the accuracy level is very high and performance is flexible.

**Nose:** The nose biometric technique [11] works through features extracting from a nose and by the help of various classification techniques. Geometric ratios and nose ridge shape both demonstrate the procedures of nose's biometric. The nose's biometric is largely unknown and for that reason it is very flexible in performance but the recognition procedure is currently far lower than other biometrics.

**Ear:** One of interesting authentication technique is ear biometric security. Analyzing ear shape and area measurement of a human can identify people [12]. Ear biometrics appears as a well-organized biometric method for human identification and could be used like other biometrics because the human ear goes through little changes as course of age. Now a day the 2D and 3D domain are presented in this biometric feature.

**Signature:** Signature recognition is one of the behavioural biometric systems. Signature signing features like writing speed, velocity and pressure are used for identifications. Signature verification devices are logically accurate in operation and lend themselves to applications where a signature is an accepted identifier [13]. It can be operated in two different ways: Static: Users write their signature on paper then digitize through a scanner or camera and the biometric system recognizes the signature analyzing its shape. Dynamic: Users write their signature in a digitizing tablet.

**Iris:** In this iris-based biometric [14], the system can analyzing features using mathematical pattern-recognition techniques. It stores the measurement of the colored ring of tissue surrounds the pupil of eye. Iris biometrics uses a fairly conventional camera element and obliges no close contact among the user and reader. In this system, first localize the inner and outer boundaries of the iris (pupil and limbus) from an eye image. Then detect and exclude eyelids, eyelashes and specular reflections that often unused parts of the iris. The set of pixels contain the iris, normalized by a rubber-sheet model to compensate for pupil dilation or constriction, then analyzed to extract bit pattern information which is needed for compare of two iris images. This system work with glasses and few devices can work well in identification mode also.

**Voice:** Voice biometrics [15] has the most probable for enlargement, because it requires no new hardware—most PCs already contain a microphone. Speaker recognition is the identification of the human beings that who is speaking. By the help of characteristics of their voices the verification process occurs. But the noisy voice can affect verification.

**Vein geometry:** In this technique the vein of hand, vein of finger, vein of palm etc are used for authentication purpose. It is not observable under visible light so the security is very high. The infrared sensors used for captured and detect the structure of the vein patterns. There are two kinds of imaging technology have been used to develop this system, which are Far-infrared (FIR) and Near-infrared (NIR). Visibility of the vein structure depends on different issues like age, thickness of the skin, ambient temperature, physical activity, depth of the veins under the skin. Additionally, skin texture for instance moles, warts, scars and hair can also distress the imaging excellence of the veins. L. Wang et al. [16] proposed a verification system of human beings using the thermal-imaged vein pattern in the back of hand. A. Kumar et al. [17] presents a technique which can authenticate a person based on minutiae matching of vein junction points.

In this contribution author presents an approach of face geometry authentication system which is based on the measurement of distances and angles of face objects like eye, nose, mouth etc. Rest of the paper has been organized as the following sections: Section 2 describes some allied works on biometry authentication system. Section 3 deals with proposed method. Mathematical analysis is shown in Section 4 and section 5 for the algorithms. In section 6 experimental results are discussed and analyzed. Section 7 draws the conclusion.

## 2. ALLIED WORK

Biometrics system intends to recognize an individual through physiological or behavioral attributes, for instance face, fingerprint, iris, retina and DNA also [18]. In biometric technique there are various ways and all biometric techniques differ according to security level, user acceptance, cost and performance. Some of the techniques are describe below:

Recognition using face and fingerprints features has been widely learning area for the researchers and is presently used in a wide variety of applications because of high accuracy rate. Uses of face and fingerprint features also used in video surveillance system [19]. Identification of people without physical contact using face features is very opportune for the recognition [20]. This is very sensitive method for facial expression and changes in lighting. Filtering a large-scale biometric database containing information like gender and age, recommended this method by Wayman [21]. This biometric method can develops the speed and efficiency of search. But, the elements like age, gender, civilization and occupation can distress performance of biometric system [22]. Park and Jain describe a technique for identifying facial mark situated on the face [23], but it is not efficient due to evaporate the temporary created mark for a long time authentication system.

Comparisons of the variety of biometric method are based on the different aspect. Each of the biometric methods like fingerprint, face, hand geometry, voice and iris have the diverse characteristics like universality, Uniqueness, permanence, performance and Measurability [24]. These characteristics are totally dissimilar for each biometric category. These can be considered as High, Medium and Low in [25]. Any physiological or behavioral attribute of human beings can provide as a biometric characteristic on which it satisfies the said requirements [26]. Table 1 compares the biometric features based on different aspects.

**Table 1. The comparisons of biometric characteristics**

| Biometric Features | Universality | Uniqueness | Permanence | Performance | Measurability |
|---|---|---|---|---|---|
| **Finger Print** | Medium | High | High | High | Medium |
| **Face** | High | High | Medium | Low | High |
| **Hand Geometry** | Medium | Medium | Medium | Medium | High |
| **Voice** | Medium | Low | Low | Low | Medium |
| **Iris** | High | High | High | High | Medium |

Universality: Everyone must contain these features.

Uniqueness: Every person has the distinctive characteristics. No two individuals have the same value.

Permanence: The characteristic should be unchanged over a stipulated period of time.

Performance: Accuracy and speed measurement done over it.

Measurability: Measurement is easy in this case.

Verchol et.al [33] developed an algorithm based on hand geometry, through which the distance parameters are calculated and stored in the database. Pentland et.al have introduced a face detection and recognition system that uses the KLT (Karhunen Loeve Transform) coefficients of the templates equivalent to the considerable facial skin texture like eyes, nose and mouth [34]. After gone through their work the author enthused to develop this features based novel biometric system.

## 3. FACE GEOMETRY

All of the biometric techniques are different because of dissimilar approaches like security level, user acceptance, cost, performance, etc. One of the physiological characteristics for recognition is Face geometry, which is the new and novel approach discussed here. The relative location of human face objects like mouth, eye, nose etc in the face is unique for each human being. Face length, height, width, curvatures and relative location of face objects distinguish every human being are different person.

Face geometry have several advantages compared to other biometric techniques:

- Medium cost as it only needs a platform for standing and medium resolution camera.
- Low-computational cost algorithm gives fast results.
- Not required to store the full image, only storage is required for storing some parameter values. So, the template size is low, which reduces the storage spaces.
- It is very easy and attractive to users, because the system is faster comparatively other biometric features.

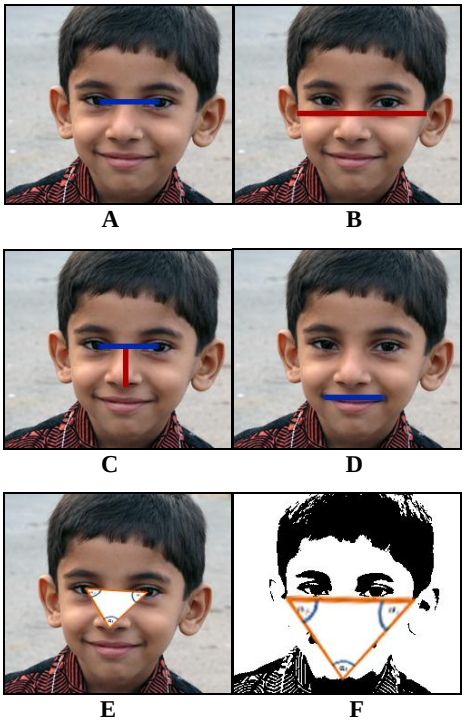


**Fig 3: Face Geometry Technique**

In figure 3, it has been observe that the face geometry of a human face. Figure 3.A shows the distance between both the eyes. Figure 3.B measure the distance between both the ears of the face. Figure 3.C is to measure the distance from forehead to nose. Figure 3.D measure the length and width of leap in human face. Figure 3.E calculates the angles between both the eyes and the nose. Here there are three angles found to measure, where the sum of three angles is $180^0$. Figure 3.F calculates the angles between both the ears and the mouth of a human face. The sum of angles is $180^0$ like the previous case.

The low cost, high speed processors and advanced algorithm in computer application made it possible to produce the concept of face geometry at a cost that made them affordable in the commercial access control market also. Environmental factors for instance dry weather or entity variance, for example dry skin does not come out to have any unenthusiastic effects on the verification accuracy of face geometry-based systems. The performance of these systems might be inclined if people use designable spectacles or sun glass. Face geometry is acceptable by the people, because they do not require showing anything in front of a device. It just takes the picture of human beings from a particular distance and then processes it for verification.

## 4. PROPOSED METHODOLOGY

Author introduced a novel authentication procedure based on face geometry. The image capturing system which we have used here is a digital camera and a flat white surface. Firstly user places his face in front of camera and white surface situated at back of face. After the image is captured, find out the area information of the face. Transforming to binary

image after calculating threshold value is the first step. Since there is clear distinction in intensity between the face and the background, a binary image is obtained. The output binary image has values of 0 i.e. black for all pixels in the input image and 1 i.e. white for all other pixels. Background lightning effects and the noise make counterfeit pixels in the image. After image filtering procedure, the system can remove these pixels and to justify edges of the face in the next step. An algorithm for feature extraction from the face geometry was created in programming environment of MATLAB and it is based on counting pixel distances in specific areas of the face objects. Extract the center point of face, eyes and nose objects from the captured image and measure the distance using Euclidean distance, City block metric, Minkowski distance, Chebychev distance, Cosine distance. After that, draw the straight line between three points and creates a triangle. Then measure the angles ($\alpha_1$, $\alpha_2$, $\alpha_3$) of triangle and store the results in the database. The $\alpha_1$, $\alpha_2$, $\alpha_3$ are compared at the time of verification to find out the authenticate user of the system. Figure 4 describes the block diagram of the work.

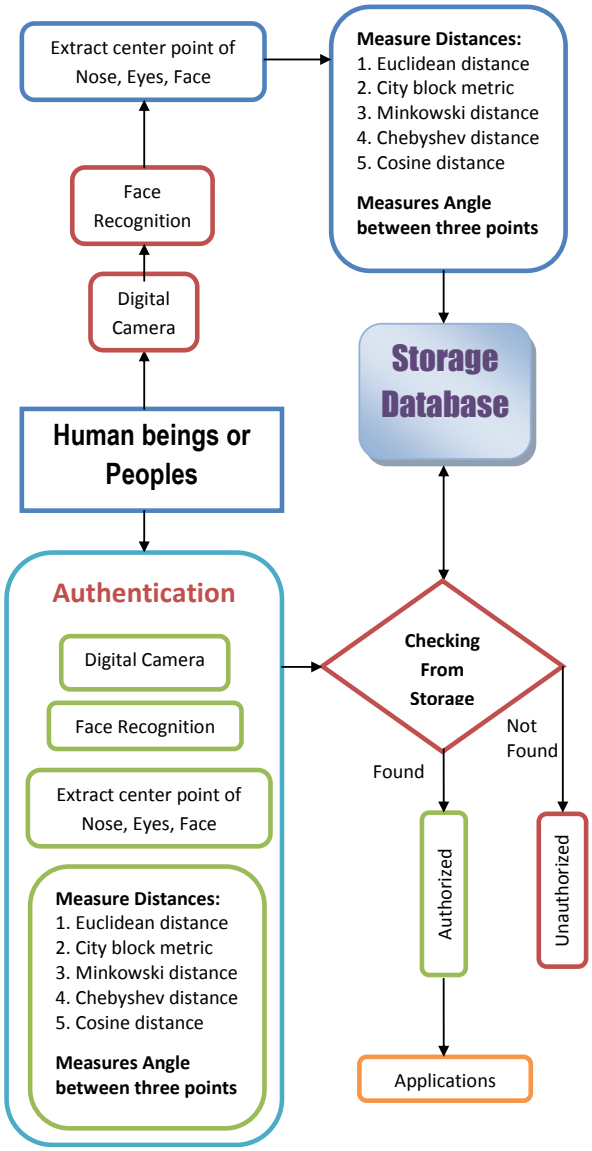


**Fig 4: Proposed block diagram**

## 5. Mathematical Analysis

The author have proposed a novel approach in this contribution which is based on distance measurement and angle measurement of different objects of face geometry of human beings. The distance metric and angle measurements are given below:

### 5.1 Euclidean distance

The Euclidean distance [27] or Euclidean metric is the ordinary distance in between two points. This formula is given by the Pythagorean formula. Euclidean space becomes a metric space by using this formula as distance. The associated norm is called the Euclidean norm. Earlier years the Pythagorean metric refers this literature.

$$d(p,q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \ldots + (q_n - p_n)^2}$$

$$= \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2} \quad \ldots\ldots\ldots (1)$$

The Euclidean distance between points $p$ to $q$ and $d(p,q)$ is the length of the line segment shown in eq.(1). Where $n$ is the dimension of the feature vector, $q_i$ is the component of one geometric face object and $p_i$ is the component of another object. In this work the author have measure the distance in between one position to another of a human facial geometric position.

### 5.2 City block metric

The City block distance between two points, $p$ and $q$, with k dimensions is calculated and generates distance $D_{CB}$ [28].

$$D_{CB} = \sum_{j=1}^{k} |a_j - b_j| \ldots\ldots\ldots\ldots (2)$$

The City block distance is forever greater than or equal to zero. If the measurement is zero that means the points are identical and if it is high then the points are shown little similarity. Find out the middle position of both the eyes and measure the distance in between the middle point and nose through this metric.

### 5.3 Minkowski distance

It is a metric of Euclidean space and it can be considered as a generalization of the Euclidean distance and the Manhattan distance [29]. The eq.(3) shows the distance.

$$P = (x_1, x_2, \ldots, x_n), Q = (y_1, y_2, \ldots, y_n) \in \Re^n$$

$$M_p = \left( \sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p} \ldots\ldots\ldots\ldots (3)$$

$P$ and $Q$ are two points of geometric face vectors and $M_p$ is the distance between that two vectors. In this distance metric operation find out the distance in between both the eyes and the nose of a human face geometric position.

### 5.4 Chebyshev distance

This distance between two points $p$ and $q$, with coordinates $p_i$ and $q_i$, respectively and $D(p,q)$ is Chebyshev distance in between that two points which is furnished in eq.4. [30]

$$D(p,q) = \max_i (|p_i - q_i|) \ldots\ldots\ldots (4)$$

Mathematically, the Chebyshev distance is a metric induced by the supremum norm or uniform norm. This technique measure the distance between each of the eyes with nose individually.

## 5.5 Cosine distance

Distance between two points *p* and *q*, with coordinates $p_i$ and $q_i$, respectively and *Cos(p,q)* is Cosine distance in between that two points which is furnished in eq.5.

$$Cos(W_1, W_2) = \frac{\sum_{i=1}^{n} p_i q_i}{\sqrt{\sum_{i=1}^{n} p_i^{\,2} \sum_{i=1}^{n} q_i^{\,2}}} \quad \ldots\ldots(6)$$

Salton and Buckley explained the concept of the Cosine-distance measure in [31]. Through this technique the author measure the distance between eyes, nose, mouth of a human facial geometric position.

**Table 2. Different values of metric used case wise**

| Metric Used | Case 1 | Case 2 | Case 3 | Case 4 | Case 5 | Case 6 | Case 7 |
|---|---|---|---|---|---|---|---|
| Euclidean Distance | 41.87 | 856.24 | 16.40 | 224.08 | 24.04 | 33.97 | 79.51 |
| Cityblock Distance | 59.00 | 978.00 | 23.00 | 245.00 | 34.00 | 48.00 | 88.00 |
| Minkowski Distance | 41.87 | 856.24 | 16.40 | 224.08 | 24.04 | 33.97 | 79.51 |
| Chebyshev Distance | 32.00 | 846.00 | 13.00 | 223.00 | 17.00 | 25.00 | 79.00 |
| Cosine Distance | 0.00 | 0.16 | 0.00 | 0.02 | 0.00 | 0.01 | 0.01 |
| Angle1 | 16 | 16 | 7 | 19 | 12 | 8 | 34 |
| Angle2 | 16 | 4 | 13 | 140 | 12 | 12 | 41 |
| Angle3 | 148 | 160 | 160 | 21 | 156 | 160 | 105 |

## 5.6 Angles of Triangle

A basic geometrical shape is called triangle. A polygon with three corners $\alpha_1$, $\alpha_2$, $\alpha_3$ and three sides (A, B, C) or edges are the line segments. A triangle with vertices A, B and C is represented by Δ ABC. The three interior angles A, B and C will always add up to 180° i.e. A+B+C=180°. In Triangle there are three types: Isosceles, Equilateral and Scalene. *Isosceles*: Isosceles triangle has two same lengths of sides and two angles which are the same as each other. *Equilateral*: In this type of triangle, it has three equal lengths and all the angles are same, that means all angles are equals to 60°. *Scalene*: The scalene triangle has all three length of sides are different and angles are also not same. In this method these three types of triangle has been used which is depending on the human face geometry. Draw the straight line in between three points i.e. two eye and one nose. Then find out the angles of the triangle and store it in the database for authentication. If the object or the human beings and the camera distance can vary, even in this case the angles may not be change and through this measurement the speedy authentication process can prepared.

The values of distances parameters and angles are shown in the above table (Table 2). In this table there are seven cases are exposed, where as more than 200 cases have tested through this algorithm.

# 6. ALGORITHMS

## 6.1 Authentication Database Algorithm

- Capture the images ($IM_{IMAGE}$) using digital camera.
- Calculate the threshold ($T_{THRES}$) of the $IM_{IMAGE}$
- Transfer $IM_{IMAGE}$ to Binary image ($BIN_{IMAGE}$) using $T_{THRES}$ and detect face boundary.
- Detect or find out the center points of face (*F*), eyes (E) and nose (*N*) objects from $IM_{IMAGE}$
- Measure distance in between these three points and store in database
    - Euclidean distance
    - City block metric
    - Minkowski distance
    - Chebyshev distance
    - Cosine distance
- Measure angle between three points *F*, *E*, *N* and store in the database.
- End

## 6.2 User Authentication Algorithm

- Capture the images ($IM_{IMAGE}$) using digital camera.
- Calculate the threshold ($T_{THRES}$) of the $IM_{IMAGE}$
- Transfer $IM_{IMAGE}$ to Binary image ($BIN_{IMAGE}$) using $T_{THRES}$ and detect face boundary.
- Detect or find out the center points of face (*F*), eyes (E) and nose (*N*) objects from $IM_{IMAGE}$
- Measure distance (*D*) in between these three points and store in database
    - Euclidean distance
    - City block metric
    - Minkowski distance
    - Chebyshev distance
    - Cosine distance
- Measure angle between three points *F*, *E*, *N*
- Check the parameters *F*, *E*, *N* and the distance *D* one by one from the stored database.
    - If found then valid user
    - Else not valid user
- End

# 7. RESULT & ANALYSIS

For the phase of analysis, several images of face are taken from the users. Extract the features from the images, where a set of measurements are performed. Final representation depends on the method used for recognition. Features vectors for each of the users are then stored in the database. In the phase of recognition, a single picture is required, for obtaining the features. The face biometric approaches [9] are the process to recognize the features vector like some pimples, some spot etc in the face, but in this approach authors developed some distance measurement along with some angle representation technique, which is faster than others.

To estimate a biometric system's accuracy the most commonly used metrics are the False Rejection Rate (FRR) and False Acceptance Rate (FAR). Percentage of authorized individuals rejected by the system is called FRR and the percentage that unauthorized persons are accepted by the system is FAR [32]. Where it has been shown that the FAR and FRR have the same value is called Equal Error Rate (ERR).

FRR = Number of false rejections / Number of accesses

FAR = Number of false acceptances / Number of accesses

**Table 3. Average FRR and FAR in percentage values**

| Process Used | FRR | ERR |
|---|---|---|
| Distance Parameters<br>1. Euclidean distance<br>2. City block metric<br>3. Minkowski distance<br>4. Chebyshev distance<br>5. Cosine distance | 0.0% | 0.0% |
| Angles Parameters | 0.0% | 0.0% |

System has been tested on the database nearly with 500 face images. The process is done by a system which is based on digital camera and computer system. The distances parameters and angles are the value, which are compared to the distance and angles obtained from the recognition process. The best values of FRR, FAR and ERR achieved for different computational methods are shown in Tab.3. Here the TSR (Total Success Rate) is 100% because the FRR and ERR together are 0.0% in both the cases. The system was tested with different parameters depending on used methods and the results in Tab.3 are the best achieved values.

# 8. CONCLUSIONS

In this development it has been shown the possibilities of using face geometry as the biometric characteristic for automatic authentication system. Varchol and Levický have used two distance parameter in their paper for hand geometry authentication purpose [33]. Pentland et.al have introduced a face detection and recognition system with the help of KLT (Karhunen Loeve Transform) coefficients and the considerable facial skin texture like eyes, nose and mouth [34]. Some relevant work has been carried out by most of the researchers in the field of face recognizing system through some facial characteristics. But in this face geometry authentication system authors proposed the distance and angle features of facial objects like face, nose and eyes, which is enough unique for verify a human beings. The results and analysis also gives the best performance in this system. In addition, the method could be enhanced by incorporating additional information, such as nose and ear geometry features in a data integration manner and also is able to develop some hybrid technique along with some other biometric approaches.

# 9. REFERENCES

[1] Jain.A.K, Hong.L, Pankanti.S: Biometric identification. Communications of the ACM 43 (2000) P. 91-98.

[2] A. K. Jain, A. Ross and S. Pankanti, Biometrics: A tool for information security, IEEE Transactions on Information Forensics and Security, vol.1, no.2, pp.125-143, 2006.

[3] K. A. Rhodes, Information Security: Challenges in Using Biometrics, United States General Accounting Office, 2003.

[4] A. K. Jain, A. Ross and S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology, vol.14, no.1, pp.4-20, 2004.

[5] S. Prabhakar, S. Pankanti and A. K. Jain, Biometric recognition: Security and privacy concerns, IEEE Security and Privacy, vol.1, no.2, pp.33-42, 2003.

[6] A. K. Jain and A. Kumar, Biometrics of next generation: An overview, The 2nd Generation Biometrics, 2010.

[7] Subhra Mazumdar; Venkata Dhulipala. "Biometric Security Using Finger Print Recognition". University of California, San Diego. p. 3. Retrieved 30 August 2010.

[8] Retina and Iris Scans. Encyclopedia of Espionage, Intelligence, and Security. Copyright © 2004 by The Gale Group, Inc.

[9] R. Brunelli, Template Matching Techniques in Computer Vision: Theory and Practice, Wiley, ISBN 978-0-470-51706-2, 2009.

[10] Miroslav Bača; Petra Grd and Tomislav Fotak (2012). "4: Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics". New Trends and Developments in Biometrics. InTech. Retrieved 1st December 2013.

[11] Shangling Song; Kazuhiko Ohnuma; Zhi Liu; Liangmo Mei; Akira Kawada; Tomoyuki Monma "Novel biometrics based on nose pore recognition" 2009.

[12] Surya Prakash, Umarani Jayaraman & Phalguni Gupta, A Skin-Color and Template Based Technique for Automatic Ear Detection, Proceedings of 7th International Conference on Advances in Pattern Recognition (ICAPR 2009), pp. 213-216, Kolkata, India, February 2009.

[13] Yeung, D; , H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G.. "SVC2004: First international signature verification competition". Lecture Notes in Computer Science. LNCS-3072: 16–22. 2004.

[14] Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons." Proceedings of the IEEE, vol. 94 (11), 2006, pp. 1927-1935.

[15] Homayoon Beigi, Speaker Recognition, Biometrics / Book 1, Jucheng Yang (ed.), Intech Open Access Publisher, 2011, pp. 3-28, ISBN 978-953-307-618-8.

[16] Wang, L.-Y., G. Leedham, and D. S.-Y. Cho, Infrared Imaging of Hand Vein Patterns for Biometric Purposes,

The Institution of Engineering and Technology, Computer Vision, Vol. 1, pp. 113-122, 2007.

[17] Kumar, A., K. and K., V. Prathyusha, Personal authentication using hand vein triangulation, IEEE Trans. Image Process., Vol. 38, pp. 2127-2136, 2009.

[18] J. Pedraza, M. A. Patricio, A. de Asís, and J. M. Molina, "Privacy and legal requirements for developing biometric identification software in context-based applications," International Journal of Bio-Science and Bio-Technology, vol. 2, no. 1, pp. 13–24, 2010.

[19] Min-Gu Kim, Hae-MinMoon, Yongwha Chung and Sung BumPan. "A Survey and Proposed Framework on the Soft Biometrics Technique for Human Identification in Intelligent Video Surveillance System" Hindawi Publishing Corporation Journal of Biomedicine and Biotechnology Volume 2012, Article ID 614146.

[20] G. A. Atkinson and M. L. Smith, "Using photometric stereo for face recognition," International Journal of Bio-Science and Bio-Technology, vol. 3, no. 3, pp. 35–44, 2011.

[21] J. L. Wayman, "Large-scale civilian biometric system—issues and feasibility," Card Tech/Secure Tech ID, 1997.

[22] E. Newham, The Biometrics Report, SJB Services, 1995.

[23] U. Park and A. K. Jain, "Face matching and retrieval using soft biometrics," Information Forensics and Security, vol. 5, no. 2, pp. 406–415, 2010.

[24] Sulochana Sonkamble, Dr. Ravindra Thool, Balwant Sonkamble, "Survey Of Biometric Recognition Systems And Their Applications" Journal of Theoretical and Applied Information Technology. Vol. 11 No 1, pp.45-51.

[25] Muhammad Khurram Khan, Jiashu Zhang and Shi-Jinn Horng, "An Effective Iris Recognition System for Identification of Humans", IEEE 2004.

[26] Natalia A. Schmid, Joseph A.O'Sullivan, "Performance Prediction Methodology for Biometric Systems using a Large Deviations Approch", IEEE Transaction of Signal Processing, October 2004.

[27] Elena Deza & Michel Marie Deza (2009) Encyclopedia of Distances, page 94, Springer.

[28] Fichet, B. (1987). The role played by L1 in data analysis. In Statistical Data Analysis based on the L1-norm and related methods (Y.Dodge, ed.). Amsterdam: North-Holland..

[29] Kruskal J.B. (1964): Multidimensional scaling by optimizing goodness of fit to a non metric hypothesis. Psychometrika 29(1):1-27.

[30] James M. Abello, Panos M. Pardalos, and Mauricio G. C. Resende (editors) (2002). Handbook of Massive Data Sets. Springer. ISBN 1-4020-0489-3.

[31] Salton and Buckley, Gerard Salton and Christopher Buckley. Term-weighting approaches in automatic text retrieval. Information Processing & Management, 24(5):513-523, 1988.

[32] KUNG, S. Y., MAK, M. W., LIN, S. H. Biometric Authentication. Published as Prentice Hall Professional Technical Reference. New Jersey: First Printing, September 2004.

[33] Peter Varchol, Dušan Levický, Using of Hand Geometry in Biometric Security Systems, Radioengineering, Vol. 16, No. 4, P.82-87, December 2007.

[34] Mathew Turk and Alex Pentland, "Eigen Faces For Recognition"; Journal Of Cognitive Neuroscience Vol.3, No.1, pp.71-86, 1991.

**Indradip Banerjee** is a Research Scholar at National Institute of Technology, Durgapur, West Bengal, India. He received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. He is registered and pursuing his PhD(Engg.) at Computer Science and Engineering Department, National Institute of Technology, Durgapur, West Bengal, India. His areas of interest are Information Security, Steganography, Cryptography, Text Steganography, Image Steganography, Quantum Steganography, Steganalysis and Biometric Security. He has published 21 research papers in International and National Journals and Conferences.

**Dipankar Chatterjee** received his M. Tech.(IT) from KSOU in Mangalore, Karnataka. MCA degree from India-Tamil Nadu-AAMEC under Bharathidasan University, Trichy in 2003 and B.Sc. (Hons.) in Physic from The University of Burdwan in 1998. Currently he is working as an Assistant Professor in Department of Computer Application of Management Institute of Durgapur, Rajbandh, and Durgapur-12. His areas of interest are Information Security, Steganography, Steganalysis and Biometric Security.

**Souvik Bhattacharyya** received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. He has received Ph.D (Engg.) from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor and In-Charge in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Natural Language Processing, Network Security and Image Processing. He has published nearly 65 papers in International and National Journals and Conferences.

**Gautam Sanyal** has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 150 papers in International and National Journals / Conferences. Three Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.