ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# FACE RECOGNITION USING PCA, GABOR FILTER AND SVM TECHNIQUES

**Manoj Kumar [*], Neha Mehta**

[*] Electronics and Communication Department, Sat Kabir Institute Of Technology and Management, Haryana, India.

## ABSTRACT

Face recognition is the hot research topic from last few years but still it has become a difficult problem. The main challenges faced by the researchers are variation caused due to different expression and poses. The main feature that can be used to extract the features from variant images that are caused because of different variations is Gabor Wavelets. This technique makes it possible to use their facial image of person to authenticate him into a secure system. In this paper the Principle Component Analysis face recognition algorithm is used for recognizing the faces this technique effectively and efficiently represents pictures of faces into its eigen faces components and these eigen face components form eigen faces these eigen faces are the ghost images of original images.The significant feature known as eigen faces don't necessarily correspond to features such as eyes, ears and noses. It provides the ability to learn and later recognizes new faces in an unsupervised manner. The efficiency and robustness of a proposed algorithm is extensively tested using Standard Database (UCI), Non-Face and Own databases. An automatic user identification system consisting of detection, recognition and user management modules have been developed. The feature vector based on gabor filter are used as the input of the face/Non-face classifier, which is SVM on a reduced feature subspace extracted by using PCA.

**KEYWORDS**: PCA Algorithm, UCI Database,vector, gabor filter, recognition,modules.

## INTRODUCTION

With the advent of electronic banking, e-commerce, smart cards, and an increased emphasis on the privacy and security of information stored in various database, automatic personal identification has become a very important topic. Accurate automatic personal identification is now needed in a wide range of civilian applications involving the use of passports, cellular phones, automatic teller machines and driver license. Traditional knowledge-based (Password or Personal Identification Number (PIN)) and token-based (Passport, diver license, and ID card) identification are prone to fraud because PINs many be forgotten or guessed by an impostor and the tokens may be lost or stolen. Therefore, traditional knowledge-based and token-based only approaches are unable to satisfy the security requirements of our electronically interconnected information society. A perfect identity authentication system will need a biometric component. A biometric system can be operated in two modes: verification mode and identification mode. In the verification mode, a biometric system either accepts or rejects a user's claimed identity while a biometric system operating in the identification mode establishes the identity of the user without a claimed identity. Face identification is a more difficult problem than face verification because a huge number of comparisons need to be performed in order to complete identification. There are a number of potential civilian applications for a biometric system working in verification mode. For example, an ATM system which verified a user's face with a biometric upon each transaction need only to match the current face image (acquired at point of transaction) with a single template stored on the ATM card. A typical face verification system can be divided into two modules: enrolment and verification. The enrolment module scans the face of a person through a sensing device and then stores a representation (template) of the face in the database. The verification module is invoked during the operation phase. The same representation used in enrolment phase is extracted from the input face and matched against the template of the claimed identity to give a "yes/no" answer [14]. On the other hand, an identification system matches the input face with a large number of faces in the database and as a result, algorithm efficiency is a critical issue in an identification system [1].

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

## PERFORMANCE CRITERIA

### Identification System

Face identification systems performance is usually evaluated by recognition rate, which is calculated by matching a set of test face images with those in the database. Different algorithms can be evaluated by matching each test face image. The matching attempts performed for each test usually consist of correct matches and incorrect matches. A matching is considered as correct if the two face images being matched are from the same person, and incorrect otherwise. Recognition rate is defined as the ratio between the number of correct matches and the number of test images.

### Verification System

In a face verification system, system level performance evaluations are usually performed by cross matching the face images in the database. Different algorithms can be evaluated by matching each face image in the database with the rest of the images in the database. A threshold value is normally used such that a matching attempt is considered authentic when the matching score is equal or above the threshold value. Two metrics (FAR and FRR) are used to measure performance of the whole system [15]. The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of impostor attempts. The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. Analysis of the FAR shows how well the system can distinguish a correct match from an incorrect match and is usually related to the uniqueness of the features. On the other hand, FRR analysis focuses on the repeatability of the features between different faces of the same person and is related to the reliability of the features.

A system can be tuned for a particular application by varying the value of these two metrics. A low value for both metrics is often desirable. Unfortunately, trying to minimize FAR or FRR requires a trade off between each of the metric. The Receiver Operating Curve (ROC) plots FAR versus FRR (Jonsson, Kittler, Li, & Matas, 2002) for a system and can be used as a guide for the selection of an operating point for the system. The FAR is usually plotted on the horizontal axis as the independent variable and the FRR is plotted on the vertical axis as the dependent variable. The closer the ROC-curve to the x and y axes, the lower verification error and thus the more reliable the system [2]. In reporting the performance, the values of FAR and FRR for the ROC curve are computed by varying the threshold value and using:

$$FAR = n_{ac} / n_u \; ;$$
$$FRR = n_{re} / n_a \qquad (1)$$

In Equation (1), $n_a$ is the number of access attempt by an authorized user and $n_u$ is the number of access attempt by an unauthorized user. For a given threshold value, $n_{ac}$ is the number of acceptances and $n_{re}$ is the number of rejections. From the ROC-curve, the Equal Error Rate (EER) is defined as the point where the value of FAR equals the value of FRR. The value of EER can now be used to determine the performance of the system. The lower is the value of EER, the more reliable the system.

### Motivation and Solutions

As a hot research topic over the last 25 years, a large number of face recognition algorithms have been proposed in the literature. The next chapter contains a detailed survey of this research. With a number of different databases available, it is always very difficult to compare different face recognition algorithms. Even when the same database is used, researchers may use different protocols for testing. Whilst many of the algorithms perform well on a certain database, they do not achieve good results on other databases.To make a fair comparison, FERET evaluation (Phillips, Moon, Rizvi, & Rauss, 2000) and the Face Authentication Test (Messer et al., 2004) have been designed to evaluate different face identification and verification algorithms. However, these tests are not concerned with the speed of the algorithms. Since only accuracy is accounted for, the applicability of the algorithms to real-time applications is not considered. However, the trade-off between accuracy and speed is very important. In summary, a face recognition system should not only be able to cope with variations in illumination, expression and pose, but also recognize a face in real-time [1].

Though face recognition is quite a tough task for a computer, but for human beings face recognition seems to be much easier. The ability to recognize faces and understand the emotions they convey is one of the most important human abilities. It is very common that one can instantly recognize thousands of people. Even a baby is able to identify its mother's face within half an hour of birth. As with many perceptual abilities, the ease with which humans can recognize faces disguises the complexity of the task even when considering the many potential variations in such a dynamic real world object. An important outcome of research on artificial vision systems has shown that more than half of the cortex becomes more active during visual processing

(Hallinan, Gordon, Yuille, Gibilin, & Mumford, 1999). The visual cortex thus plays a very important role in face recognition. Simple cells in the visual cortex are known to be selective for four coordinates, each cell having an *x, y* location in visual space, a preferred orientation and a preferred spatial frequency (Daugman, 1985). Based on this observation, a number of researches have actually shown that the various 2D receptive-field profiles encountered in populations of simple cells are well described by a family of 2D Gabor wavelets, which were first proposed by Gabor (1946) for simultaneous time and frequency analysis. In addition to this biological motivation, it is also widely believed that local texture. Features in face images, extracted by a spatial-frequency wavelet analysis, are basically more robust against distortions caused by various illumination, expression and pose (Zhao, Chellapa, Rosenfield, & Phillips, 2000). In particular, among various wavelet bases with good characteristics of space-frequency localization, the Gabor function provides the optimal resolution in both spatial and frequency domain (Gabor, 1946; Daugman, 1985). As a result, this research will apply 2D Gabor wavelets to extract features for face recognition. Since the simple cells of human visual cortex are well modelled and the local features in space and frequency domain are simultaneously extracted with optimal resolution, the system thus developed might be able to mimic a human's recognition ability and be more robust against the variation of illumination, expression and limited out of plane face rotation.

## TYPES OF BIOMETRICS

***Finger Print Identification[2][4]***

A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings (where a ridge ends) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other). Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

***How does fingerprint biometrics work***

The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and ultrasound.There are two main algorithm families to recognize fingerprints:

- Minutia matching compares specific details within the fingerprint ridges. At registration (also called enrollment), the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.
- Pattern matching compares the overall characteristics of the fingerprints, not only individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrollment, small sections of the fingerprint and their relative distances are extracted from the fingerprint. Areas of interest are the area around a minutia point, areas with low curvature radius, and areas with unusual combinations of ridges.The figure prints are shown in figure.

***Finger Prints***

***Iris Identification[3][8]***

The iris is the elastic, pigmented, connective tissue that controls the pupil. It is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. It is the only internal human organ visible from outside and is protected by the cornea. The iris of the eye has a unique pattern which varies from eye to eye and person to person. First, an iris-recognition algorithm has to localize the inner and outer boundaries of the iris (pupil and limbus) in an image of an eye. Further, subroutines detect and exclude eyelids, eyelashes, and specular reflections that often occlude parts of the iris. The set of pixels

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

containing only the iris, normalized by a rubber-sheet model to compensate for pupil dilation or constriction, is then analyzed to extract a bit pattern encoding the information needed to compare two iris images. In the case of Daugman's algorithms, a Gabor wavelet transform is used. The result is a set of complex numbers that carry local amplitude and phase information about the iris pattern. In Daugman's algorithms, most amplitude information is discarded, and the 2048 bits representing an iris pattern consist of phase information (complex sign bits of the Gabor wavelet projections). Discarding the amplitude information ensures that the template remains largely unaffected by changes in illumination or camera gain (contrast), and contributes to the long-term usability of the biometric template. The iris scanning is shown in figure.

***Iris***

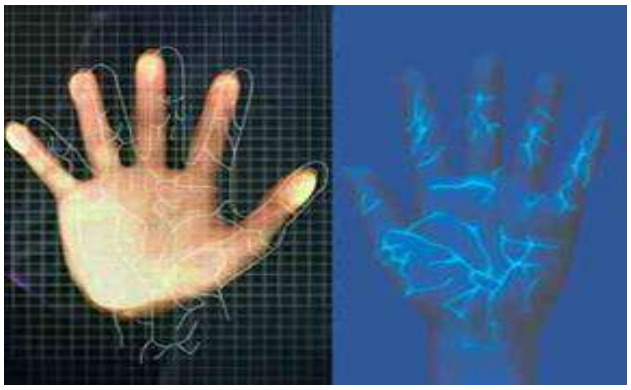
To prevent an image / photo of the iris from being used instead of a real "live" eye, iris scanning systems will vary the light and check that the pupil dilates or contracts.

***Face Identification***

Face recognition is a modus operandi that human performs routinely in their daily lives[10]. It is one of the primary biometric technologies that have become more and more important owing to rapid advancement in technologies such as digital cameras, internet and mobile devices, and increasing demands in security.Earlier Face Recognition Algorithms used simple geometric models but the face recognition process has now matured into a science of sophisticated mathematical representations and matching processes.Face Recognition algorithms can be divided into two main approaches - geometric, which looks at distinguishing features and photometric, which is a statistical approach that distill an image into values and comparing the values with templates to eliminate variances.

***Hand Geometry Identification***

Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand in respect of various dimensions and compare these measurements to the ones stored in a file. Viable hand geometry devices have been manufactured since the early 1980s, making hand geometry the first biometric to find widespread computerized use. It remains popular; common applications include access control and time-and-attendance operations. Systems that measure hand and finger geometry use a digital camera and light. To use one, you simply place your hand on a flat surface, aligning your fingers against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts. It uses this information to determine the length, width, thickness and curvature of your hand or fingers. It translates that information into a numerical template.



***Hand Print***

***Speaker Recognition***

The product allows developers to speech enable devices for talking clocks, household appliances, navigation aids, talking books, answering machines and voicemail systems, talking dictionaries, language translators, security system monitors, and cell phones to industrial warning system controls and educational electronic learning aids.

***Keystroke Recognition***

It involves a user typing his or her password or phrase on a keyboard. The system then records the timing of the typing and compares the password itself and the timing to its database. Verification takes less than 5 seconds.

***Face Recognition Technology***

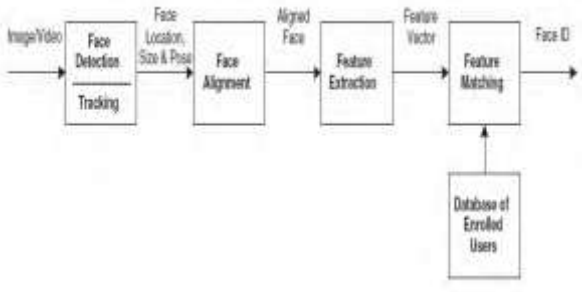
The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Using wide assortment of cameras, the visible light systems extract features from the captured image that do not change over time while avoiding superficial features such as facial

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis. Some of the challenges of facial recognition in the visual spectrum include reducing impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use real time- process to detect a person's head and locate the face automatically. Major benefits o facial recognition are that it is non-intrusive, hands-free, and continuous and accepted by most users. A general statement regarding the problem of machine recognition of faces can be formulated as follows: given still or video images of a scene, identify or verify one or more persons in the scene using a stored database of faces [1]. To address this given problem, a general procedure can be established by face detection, feature extraction, and recognition. Face detection is used to separate face-like objects from cluttered scenes. To be recognized, faces are usually represented in terms of vectors in a lower dimensional feature space extracted from the images [2]. Once the face features are available, the recognition step is based on the establishment of a similarity between feature vectors. Such a relation between two vectors of a known and an unknown identity is normally carried out by means of a similarity score.

**System Architecture**

Over the last two decades, research has focused on how to make face recognition systems fully automatic by dealing with problems such as localization of a face in a given image or video sequence and extraction of features such as eyes, mouth, etc. Meanwhile, significant advances have been made in the design of classifiers [20]. A face recognition system generally consists of four modules as depicted in Figure3 detection, alignment, feature extraction, and matching, where localization and normalization (face detection and alignment) are processing steps before face recognition (facial feature extraction and matching) is performed[11].




A typical face recognition system architecture

Face detection segments the face areas from the background by coarse estimating its location and scale in a given scene. In the case of video, the detected faces may also need to be tracked using a face tracking component [20]. The purpose of the face alignment is to refine the location and to normalize the faces provided by the face detection. Facial components, such as eyes, nose, mouth and facial outline, are prior located. Based on their positions, the input face image is normalized with respect to geometrical properties, such as size and pose, using geometrical transforms or morphing. The face is usually further normalized with respect to photometrical properties such as illumination and gray scale [24]. Subsequent to the alignment step, the feature extraction is performed on this stable representation to provide effective information that is useful for distinguishing among faces of different persons [25]. Afterwards, on the face matching stage, the extracted feature vector of the input face is matched (similarity measurement) against those of enrolled faces in the database to determine the identity of the face when a match has sufficient confidence or to indicate that the face is unknown otherwise [27]. Face localization and normalization are the basis for extracting effective features to represent the face pattern. They play a crucial role in how efficient the classification methods will distinguish between faces. Some other attributes that may classify face recognition systems consider its operational scenario. Within the possibilities significant differences exist. They are in terms of static images or video-based, image quality, amount of background clutter, variability of the images of a particular individual that must be recognized, matching criterion, and the nature, type, and amount of input from a user.

**Adopted Recognition Techniques(PCA, Gabor, SVM)**

Faces are usually represented by digital images whose dimension m×n related to the number of pixels is a high number even for small images. Methods which operate in this pure representation have a number of potential shortcomings, most of them related to the well-known curse of dimensionality. However, much of the surface of a face is smooth and has regular texture, which means that the value of a pixel is typically highly correlated with the values of its neighbors. Moreover, faces constraints such as symmetry can be also considered somehow a kind of redundancy in its representation [31].

The sensing of faces represented as high-dimensional arrays of pixels often belongs to a manifold of lower dimension. As a consequence, face recognition and computer vision research in general has shown increasingly interest in techniques that take advantage of this observation and apply algebraic and statistical

tools to extract and analyze such manifolds. The features in these manifolds (i.e., subspaces) provide more prominent and richer information for recognition than the raw image. The use of subspace modeling techniques has significantly advanced face recognition technology [28].To deal with the dimensionality problem, the approach used is Eigen Face approach (PCA) using Gabor Wavelets and Support vector Machine (SVM).

**Eigen Face Approach**

A set of eigen faces can be generated by performing a mathematical process called principal component analysis (PCA) on a different set of images of different human faces. It is one of the most versatile approaches for face recognition is derived from the statistical technique called Principal Component Analysis [32]. Popularized by Turk and Pentland [24], the use of PCA to represent faces is based on the idea that face recognition can be accomplished with a small set of features that best approximates the set of known facial images.

Eigen faces can be considered a set of "standardized face ingredients", derived from statistical analysis of many faces images. Any human face can be considered to be a combination of these standard faces. For example, one's face might be composed of the average face plus 10% from eigen face 1, 55% from eigen face 2, and even -3% from eigen face 3. Remarkably, it does not take many eigen faces combined together to achieve a fair approximation of most faces. Also, because a person's face is not recorded by a digital photograph, but instead as just a list of values, much less space is taken for each person's face.The eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern is how different features of a face are singled out to be evaluated and scored. There will be a pattern to evaluate symmetry, if there is any style of facial hair, where the hairline is, or evaluate the size of the nose or mouth. Other eigen faces have patterns that are less simple to identify, and the image of the eigen face may look very little like a face. The technique used in creating eigen faces and using them for recognition is also used outside of facial recognition. This technique is also used for handwriting analysis, lip reading, voice recognition, sign language/hand gestures interpretation and medical imaging analysis. Therefore, some do not use the term eigen face, but prefer to use 'eigen image'.

## PROPOSED ALGO

The entire sequence of training and testing is sequential and can be broadly classified as consisting of following steps:

Step 1: Input Images Taken From Camera and Standard DB and Non-Face Images.

Step 2: Prepare DB.

Step 3: Training.

Step 4: Scan DB.

Step 5: Testing.

Step 6: Decision.

Step 7: Recognised Input Data.

***Database Preparation***

The database was obtained by taking photographs of different persons by using camera etc. in similar condition like lighting, size, resolution etc. The database used in this thesis is formed by using three types of images such as photograph taken from camera, standard database downloaded from internet i.e. UCI database and some Non-faces images are downloaded from internet. These images were stored in training folder. The size of image must be equal to 1200×900 pixels and resolution must be set to 80 pixels/inch.

***Training***

The different steps involved in training are explained below:

- Select one (.jpg) file from database train database.
- By using that read all the faces of each person.
- Normalize all the faces and convert them to grey scale.Find the mean of all face images and subtract that mean from the data matrix of all face images read from train folder. Then form the co-variance matrix.
- Find the Eigen vectors of co-variance matrix.
- By using the values of these Eigen values and vectors form the eigen faces and display each Eigen face with its corresponding eigen value.

***Testing***

Testing is carried out by following steps:

- Select an image to be tested using open file dialog box.
- An image is read and normalizes and converted into grey scale.
- Then detect whether the selected image is a face image or not. It is performed by finding the number of pixels that must be greater than 1000 for a face image and skin edges and edges are determined by using canny edge detector. Then dialog box appears and shows the image is face or not.
- Then Gabor filter is applied and it perform the fast Fourier transforms analysis on the images and extract the features by rotating the images at different angles with different orientations and we obtain 40 Gabor oriented wavelets whose one block size equals to 64 ×64 with different values of k. Then negative of the image is formed to obtain the difference between the images.
- Last step matching is performed and the matching is done by using SVM that works as a classifier and

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

classifies the image with the stored database in training folder.

Now at last the comparison of different images selected is shown in the table that how many images are processed and what result we get.

## RESULTS

| Type of Database | Number of Image | Mean of Images | ED of the Images | Eigen Values of Images | Recognition Rate |
|---|---|---|---|---|---|
| Standard Database | 1 | 96.0689 | 2.5511e+ 007 | 0.242603 | 100 % |
| | 2 | 92.2993 | 2.0209e+ 007 | -0.384611 | 100 % |
| | 3 | 88.7130 | 2.0680e+ 007 | 0.405682 | 100 % |
| | 4 | 101.0530 | 2.4258e+ 007 | 0.0374906 | 100 % |
| | 5 | 88.5261 | 2.0729e+ 007 | 0.500978 | 100 % |
| | 6 | 89.5309 | 1.7457e+ 007 | - 0.0744252 | 100 % |
| | 7 | 91.7547 | 1.7025e+ 007 | 0.475836 | 100 % |
| | 8 | 100.4563 | 1.5876e+ 007 | 0.0225592 | 100 % |
| | 9 | 97.4746 | 1.5115e+ 007 | -0.233659 | 100 % |
| | 10 | 107.4908 | 2.5824e+ 007 | -0.0274596 | 100 % |
| | 11 | 114.5847 | 2.8224e+ 007 | -0.0148566 | 100 % |
| | 12 | 122.2205 | 3.1341e+ 007 | 0.0255765 | 100 % |
| | 13 | 93.0319 | 1.3099e+ 007 | -0.114518 | 100 % |
| | 14 | 117.7599 | 3.1357e+ 007 | 0.0469826 | 100 % |
| | 15 | 108.5405 | 3.202e+ 007 | -0.0245963 | 100 % |
| Non- Face Images | 1 | 93.3939 | Error | Error | Not Detected |
| | 2 | 73.1407 | Error | Error | Not Detected |
| | 3 | 198.5678 | Error | Error | Not Detected |
| | 4 | 99.7149 | Error | Error | Not Detected |
| | 5 | 104.4117 | Error | Error | Not Detected |
| | 6 | 52.8423 | Error | Error | Not Detected |
| | 7 | 84.7310 | Error | Error | Not Detected |
| | 8 | 98.1406 | Error | Error | Not Detected |
| | 9 | 48.6208 | Error | Error | Not Detected |
| Own Database | 1 | 112.8956 | 7.4100e+007 | 0.33753 | 100 % |
| | 2 | 169.0136 | 7.4039e+007 | 0.0620223 | 100 % |
| | 3 | 93.6556 | 9.0495e+007 | 0.2325450 | 100 % |
| | 4 | 121.1218 | 7.9094e+007 | -0.641815 | 100 % |
| | 5 | 161.5925 | 6.9829e+007 | 0.442539 | 100 % |
| | 6 | 91.6599 | 8.8146e+007 | -0.191703 | 100 % |

## REFERENCES

[1] De-Song Wang, Jian-Ping Li, Yue-Hao Yan "A Novel Authentication scheme of the DRM System based on Multimodal Biometric Verification and Watermarking Technique", IEEE 2008.

[2] Lin Lin Shen , " Recognition faces- An approach based on Gabor Wavelets", , pg-1-5, July 2005.

[3] Panpan Li, Renjin Zhang,"The evolution of biometrics" in the proc. Conference of the multi-media Computer Assisted Instruction Institute Guizhou Normal University Guiyang, China, ISBN 978-1-4244-6734-1/10.

[4] Jain, A.K., Bolle, R. Pankanti, S., "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publications. ISBN 978-0792383451.

[5] Isenor D K.Zaky S G, "Fingerprint identification using graph matching"2rd, 1986.

[6] Hao Chen, "The Advantages and Characteristic of Identity Technology", China Anti-Counterfeiting Report.1rd, 2008.

[7] Anil.K.Jain, Patrick Flynn, Arun A.Ross, "Handbook of Biometrics", Springer Science and Business Media, 2008.

[8] R.Sanchez-Reillo,C.Sanchez-Avila and J.A.Martin-Pereda, "Minimal Template Size for Iris Recognition", Proc. of the first Joint BMHS/EMBS Conference, Atlanta(U.S.A), October 1999.

[9] Raul Sanchez-Reillo, "Smart Card Information and Operations using Biometrics" IEEE AESS Systems Magazine, April 2001. ISBN 08856/8985/01.

[10] John Vacca, "Handbook of Biometric Computer and Information Security", Publisher Morgan Kaugmann.
[11] Stan Z. Li, Anil K. Jain, "Handbook of Face Recognition", Springer Science and Business Media, 2005.
[12] D.Maltoni, D.Maio, A.Jain, and S.Prabhakar, "Handbook of fingerprint Recognition." Springer Professional Computing, 2009.
[13] Wildes R.P., "IRIS Recognition: An Emerging Biometric Technology", Proceeding of IEEE, 85(9):1348-1363, 1997.
[14] A. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 2002.
[15] M. Burge and W. Burger. "Ear Biometrics in Computer Vision". Proc. 15th International Conf. of Pattern Recognition, vol. 2, pp. 822–826, 2000.
[16] W. Zhao, R. Chellapa, P. J. Phillips, and A. Rosenfeld, "Face Recognition: A Literature Survey, ACM Computing Surveys", 35(4):399–458, December 2003. chiacchia
[17] Sheng Zhang and Matthew Turk (2008), Scholarpedia, 3(9):4244
[18] Michael Kirby, "Geometric data analysis", JohnWiley & Sons, Inc., 2001.
[19] N. Petkov and P. Kruizinga, "Computational models of visual neurons specialized in the detection of periodic and a periodic oriented visual stimuli: Bar and grating cells", pp. 83–96, 1997.
[20] De-Song Wang, Jian-Ping Li, Yue-Hao Yan "A Novel Authentication scheme of the DRM System based on Multimodal Biometric Verification and Watermarking Technique", IEEE 2008.
[21] Gui Feng, and Qiwei Lin, "Iris feature based watermarking algorithm for personal identification", Proc. of SPIE, Vol. 6790, pp.679045, 2007.
[22] Seyed Mohammad Ahadi, Nima Khademi Kalantari, "A Robust Image Watermarking in the Ridge let Domain Using Universally Optimum Decoder" IEEE Transactions on circuits and systems for video technology, Vol 20, NO. 3 March 2010.
[23] P. Campisi, D. Kundur, and A. Neri "Robust digital watermarking in the ridge let domain," IEEE Signal Process. Lett., vol. 11, no. 10, pp. 826–830, Oct. 2004.
[24] Kang Ryoung Park, Dae Sik Jeong, Byung Jun Kang, and Eui Chul Lee, "A Study on Iris Feature Watermarking on Face Data", ICANNGA 2007, Part II, LNCS 4432, pp. 415-423, 2007.
[25] De-Song Wang Jian-Ping Li Yue-Hao Yan "A Novel Authentication Scheme of the DRM System based on Multimodal Biometric Verification and Watermarking Technique" ICACIA 2008.
[26] Rao, N.N. Thrimurthy, P. Babu, B.R." An efficient copyright protection scheme for digital images using biometrics and watermarking" ICCSIT August 2009.
[27] Edward, S.; Sumathi, S.; Ranihemamalini, R. "Person authentication using multimodal biometrics with watermarking", July ICSCCN. 2011.
[28] Desong Wang; Jianping Li; Memik, G "Authentication Scheme of DRM System for Remote Users Based on Multimodal Biometrics, Watermarking and Smart Cards" Intelligent Systems, 2009.
[29] Meihua Wang, Kefeng Fan " A Novel Digital Content Protection System Based on Iris Biometric" FSKD 2007
[30] Zuraini Othman," Preliminary Study on Iris Recognition System: Tissues of Body Organs in Iridology", 2010 IEEE EMBS Conference on Biomedical Engineering & Sciences 978-1-4244-7600-8/10©2010 IEEE.
[31] Zhenan Sun," Improving Iris Recognition Accuracy Via Cascaded Classifiers", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS 1094-6977© 2005 IEEE.