Volume 3, No. 11, November 2012

Journal of Global Research in Computer Science

ISSN-2229-371X

REVIEW ARTICAL

Available Online at www.jgrcs.info

BIOMETRIC TECHNIQUES AND FACIAL EXPRESSION RECOGNITION-A REVIEW

Renu Nagpal[*1], Pooja Nagpal[2] and Sumit Malhotra[3]

*[1]CSE Department,Bhai Gurdas Institute of Engineering & Technology,Sangrur, Punjab,India

er.renunagpal@gmail.com[1]

[2] CSE Department,Rayat Institute of Engineering & Information Technology,Ropar, Punjab,India

Poojanagpal48@gmail.com[2]

[3] CSE Department,Bhai Gurdas Institute of Engineering & Technology,Sangrur, Punjab,India

Sumitmalhotra.mail@gmail.com[3]

Abstract: The type of authentication, the one relies on measurable physical characteristics that can be automatically checked, and is becoming more popular and demanded. It is called biometrics. This study aims to give the basic review on the biometric techniques and discussion to facial expression recognization in still images and in videos also and to discuss both the techniques for intelligent computers or robots that are mind implemented. An automatic system for the recognition of facial expressions is based on a representation of the expression, learned from a training set of preselected meaningful features. As a first we investigate the emotionally intelligent computers which can perceive human emotions. Biometric uses a variety of processes and techniques to analyze the authentication of the living person. Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics such as fingerprints, eye retinas, irises, voice patterns, facial patterns and hand measurements, for authentication purposes. In this research paper there is a stress on biometric and techniques of biometric also we have discussed facial expression recognition for both static and dynamic techniques to recognize human facial expression to recognize universally recognized five principal emotions namely angry, disgust, happy, sad and surprise along with neutral in still images and also in video sequence.

INTRODUCTION TO BIOMETRICS

Biometric is the science and technology of recording and authenticating identity using physiological or behavioral characteristics of the subject. A biometric representation of an individual. It is a measurable characteristic, whether physiological or behavioral, of a living organism that can be used to differentiate that organism as an individual. Biometric data is captured when the user makes an attempt to be authenticated by the system. This data is used by the biometric system for real-time comparison against biometric samples.

The biometric template is created through the enrollment process, in which initial biometric samples are captured. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy.Many existing government identity management systems employ biometrics to assure that each person has only one identity in the system and that only one person can access each identity. Traditional methods of establishing a person's identity include knowledge based (e.g., passwords) and token based (e.g., ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security. Biometrics offers the identity of an individual may be viewed as the information associated with that person in a particular identity management system .For example, a bank issuing credit cards typically associates a customer with her name, password, social security number, address and date of birth. Thus, the identity of the customer in this application will be defined by these personal attributes (i.e., name, address, etc.). By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. Biometrics has also been used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.

Biometric Characteristics:

Biometric characteristics can be divided in two main classes:

a. Physiological are related to the shape of the body.Examples include, but are not limited to fingerprint, face recognition, DNA, hand and palm geometry, iris recognition, which has largely replaced retina and scent.

Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics for this class of biometrics

Under this there are some common characteristics of Biometrics like:

a. Universality: Every individual accessing the application should possess the trait.
b. Uniqueness: The given trait should be sufficiently different across individuals comprising the population.
c. Permanence: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.

d. Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.
e. Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
f. Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
g. Circumvention: This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.

Key Elements of all Biometric Systems:

All biometric systems consist of three basic elements:

a. Enrollment,
b. Templates, and
c. Matching.

Enrollment is the process of collecting biometric samples from a person and the subsequent generation of a template. Typically, the device takes three samples of the same biometric and then averages them to produce an enrollment template.

Templates are the data representing the enrollee's biometric. They are created by the biometric device, which uses a proprietary algorithm to extract "features" appropriate to that technology from the enrollee's samples. These features are also referred to as minutiae points for some technologies, such as fingerprint systems. Because templates are only a record of distinguishing features of a person's biometric characteristic or trait (and not an image or complete record of the actual fingerprint or voice), the template is usually small and allows for the near-instantaneous processing time characteristic of biometric authentication. The small size of some templates allows for storage on magnetic stripes or bar codes placed on plastic cards or smart cards.

For any biometric technology, a small percentage of the population will be unable to produce a usable template. This failure to enroll (or acquire) is the failure of the technology to extract adequate distinguishing features appropriate to that technology. For example, a small fraction of the population cannot be fingerprinted either because their prints are not distinctive enough (e.g., no bifurcations that can be picked up by the system) or because of the individual's occupation or age, which can alter distinguishing features.

Matching is the process of comparing a submitted biometric sample against one (verification) or many (identification) templates in the system's database. In general, verification applications provide more security than identification applications because a biometric and at least one other piece of input (e.g., PIN, password, token, user name) are required to match a template. Verification provides a user with control over his own data and over the biometric authentication process, provided that the template is stored only on a card. That is, such a system would not allow for clandestine, or involuntary, capture of biometric data because the individual would know if he were providing the card. Because the search seeks only a match against one template in the database, verification applications require less processing time, less memory, and less cost than identification applications. Accuracy and error rates must be examined by the end-user when choosing biometric devices. Identification applications require a highly robust and distinctive biometric, otherwise the error rates falsely matching and nonmatching users' samples against templates breaches security and inhibit convenience. Applications where the end-user wants to identify criminals (immigration, law enforcement, etc.) or other types of "wolves in sheep's clothing" must use an identification application. Other types of applications may require a verification application. In many ways, deciding whether to use verification or identification requires a balance between the end-user's needs for security and convenience.

Template management is an integral component of balancing privacy, security, and convenience issues. All biometric systems face a common issue: The template database must be stored somewhere. Biometric templates must be protected to prevent identity fraud and maintain user privacy. Possible solutions include storage on the biometric device itself, a central computer that is remotely accessed, a plastic card or token with a bar code or magnetic stripe, Radio Frequency Identification Device (RFID) cards and tags, optical memory cards, PCMCIA (Personal Computer Memory Card International Association) cards, and smart cards. An important security issue with regard to template database management is whether the database will serve a unique purpose or if it will be used for multiple purposes. For example, a facilities manager might use a fingerprint reader to control building access. He might also want to use the same fingerprint template database to identify employees logging onto their computer network. The transmission of data across wires to a central database presents risks that the biometric template might be captured or stolen. An additional privacy and security concern is what additional personal information will be stored about each user with his biometric template and whether his biometric is used to link to other personal information about him.

COMMON BIOMTRICS MODALITIES

The field of biometrics is a polarizing and controversial topic, with multiple voices debating the merits and demerits of the technology. Many of the discussions have focused on hypothetical, deeply technical and philosophical issues. There are a lot of different types of biometric systems. Here's description and pros and cons of the most popular ones.

a. Fingerprint
b. Face
c. Iris
d. Voice

e. Hand Geometry

Fingerprint Readers:

Fingerprint readers are the most common type of biometrics and the most closely associated in the minds of consumers with the industry as a whole. Fingerprint systems work by scanning the tips of one or more fingers and comparing the scans against known images. There are several types of scanning and matching technologies in use today, but the user experience is pretty straightforward, put finger on a small sensor, wait a second or two for the result. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

Advantages:

a. Most people instinctively understand the concept of fingerprint scanning, so there's fairly little user training required.
b. Fingerprint sensors are quite small, don't consume a lot of power and are becoming inexpensive to manufacture, making it possible to put fingerprint biometric systems on laptops, cell phones, Personal digital assistance and even Universal Serial Bus thumb drives.
c. Fingerprints are the oldest and best-developed sector in the biometrics industry, so there are many vendors and product choices available to the consumer.
d. Fingerprint biometric systems have recently become mandated for certain classes of U.S. federal government ID cards, which should spur even more feature development and interoperability among vendors.

Disadvantages:

a. Though accuracy has been steadily improving, there is still a real perception that fingerprint scanners are too fidgety for everyday use.
b. Fingertips are more likely to be dirty than other parts of the body. Dirty fingers can foil the matching process. Dirty fingers also lead to dirty fingerprint readers, which then lead to more poor scans.
c. Because many fingerprint systems are not 100% reliable, they are frequently configured with some sort of backup authentication mechanism – such as a Personal Identification Number (PIN) or password - that can be entered in the event that a person can't get a good scan. The existence of these backup mechanisms makes fingerprints more useful as a convenience feature, than as an improvement to overall security.
d. As a result of a cultural association with criminal proceedings, many people have a strong aversion to having their fingers scanned. This is a significant barrier to widespread adoption in several countries.
e. The proliferation of vendors and products has a downside: the fingerprint biometrics industry is rife with incompatible technologies. Interoperability will improve with time.

Face Recognition:

Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Because a face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (*i.e.* the subject does not necessarily know he has been observed). For this reason, facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas.

Advantages:

a. Facial recognition system can be used wherever a camera can be put. Many cameras can be installed throughout a location to maximize security coverage without disrupting traffic patterns.
b. Face recognition systems can be installed to require a person to explicitly step up to a camera and get their picture taken, or to automatically survey people as they pass by a camera. The later mode allows for covert scanning of many people at the same time.
c. Face scanning is non obtrusive, can be done at a comfortable distance and does not require the user to touch anything.
d. Video or pictures can be replayed through a facial recognition system for surveillance or forensics work after a security event.
e. New 3D facial recognition systems are reportedly showing a surprisingly high level of accuracy and reliability.

Disadvantages:

a. Accuracy of traditional 2D face recognition systems has been historically poor. Such systems may be fooled by hats, beards, sunglasses and face masks (of the type made popular in international airports during the latest Seven Acute Respiratory Syndrome scare-SARS.) Even changes of lighting and camera angle can have a significant effect on the accuracy of 2D systems.
b. 3D systems, though potentially much more accurate, are still in their infancy. 3D systems will probably also be less nimble at processing large crowds – one of the main advantages of traditional 2D systems.
c. Some people view mass-scale facial recognition cameras as the ultimate "big brother" encroachment of security at the expense of privacy. While there are many good arguments on both sides of that debate, potential public distaste for such systems should be considered before implementation.

Iris Recognition:

The eyeball has lots of unique and accessible identifying characteristics that remain fairly constant over an individual's lifetime, making it a potentially ideal source of biometric data. There are two primary places in the eye that are used for biometrics systems today. They are the retina and the iris. A third type, combining aspect of the two as well as other ocular features is called whole eye. Iris scanning measures the iris pattern in the colored part of the eye, although the iris color has nothing to do with the biometric. Iris patterns are formed randomly. As a result, the iris patterns in a person's left and right eyes are different, and so are the iris patterns of identical twins. Iris scanning can be used quickly for both identification and verification applications because the iris is highly distinctive and robust.

Advantages:

a. Iris-based systems are non-intrusive and can be used at a distance of a couple of feet. Using an iris-based system is a bit like looking into a bathroom mirror.
b. Unlike with fingerprint readers, virtually all people with healthy eyeballs can be successfully enrolled and scanned with eye-recognition systems.

Disadvantages:

a. A Beam of light into the eyeball at a fairly close distance can produce some sort of vaguely unpleasant sensations.
b. Quality eye recognition equipment tends to be more expensive today than fingerprint readers.

Voice Recognition:

Voice recognition also known as speaker recognition, is the problem of identifying a speaker from a short utterance. While speech recognition systems are concerned with transcribing speech and need to ignore speech idiosyncrasies, voice recognition systems need to amplify and classify them. There are many sub problems, such as whether the recognition is text-dependent or not, whether the environment is noisy, whether operation must be real time, and whether one needs only to verify speakers or to recognize them from a large set. Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology. However, voice recognition can be affected by environmental factors such as background noise. This technology has been the focus of considerable efforts on the part of the telecommunications industry and the U.S. government's intelligence community, which continue to work on improving reliability.

Advantages:

a. Public acceptance
b. No contact required
c. Commonly available sensors (telephones, microphones)

Disadvantages:

a. Difficult to control sensor and channel variances that
b. significantly impact capabilities
c. Not sufficiently distinctive for identification over large databases

Hand Geometry:

According to Feldman, "hand geometry technology creates mathematical pattern abstractions using data derived from the length, width, thickness, curvature and surface area of the hand and four fingers. The quality of the enrolment image will affect how often the system falsely rejects the individual in the future The hand geometry-based systems require the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured the human hand presents a sufficiently peculiar conformation of anatomical features to enable authentication, but is not considered sufficiently unique to provide full identification, a simple hand geometry system will measure length and thickness of digits, width of the palm at various points and the radius of the palm. This results in a relatively simple identification that can be expressed in a very simple, compact string of data.

Advantages:

a. Easy to capture
b. Believed to be a highly stable pattern over the adult
c. lifespan

Disadvantages:

Use requires some training

a. Not sufficiently distinctive for identification over large databases; usually used for verification of a claimed enrollment identity
b. System requires a large amount of physical space

APPLICATIONS

a. Applications vary and range from logical access to a personal computer, to physical access of a secure laboratory.The practical applications of biometric technologies are diverse and expanding, as new needs are identified. Some areas where Biometrics can be used are:
b. They can be used in a variety of collection environments as identification systems.
c. Biometrics are also used for accountability applications, such as recording the biometric identities of individuals boarding an aircraft, signing for a piece of equipment, or recording the chain of evidence.
d. Biometrics performs more reliably in controlled environments, such as offices and laboratories, than in uncontrolled environments, such as outdoors.
e. ***Business:*** Compliance, Risk Mitigation, Less administration, Accurate payrolls
f. ***Banks:*** ATMs, VPNs, Automated branches, Cash Dispensing, Point of Sale, Access Control.
g. ***E-Business:*** B2B Trading exchanges, Payment gateways, Call centers, Data Centers.
h. ***ATM machine use:*** Most of the leading banks have been experimenting with biometrics for ATM machine use and as a general means of combating card fraud.

i. ***Workstation and network access:*** Many are viewing this as the application, which will provide critical mass for the biometric industry and create the transition between sci-fi device to regular systems component, thus raising public awareness and lowering resistance to the use of biometrics in general.
j. ***Travel and tourism:*** There are multi application cards for travelers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc.
k. ***Telephone transactions:*** Many telesales and call center managers have pondered the use of biometrics.

BENEFITS

a. A biometric can't be stolen, misplaced, forgotten or copied.
b. Biometrics can provide an automated means for identification of an individual or verification of a claimed identity.
c. Biometrics are typically passive and designed to be safe to use.
d. Biometric systems usually implement ordinary computing and video technology, such as that encountered in a person's day-to-day activities.
e. Controlling access to physical locations (laboratories, buildings, etc.) or logical information (personal computer accounts, secure electronic documents, etc).
f. Biometrics can also be used to determine whether or not a person is already in a database, such as for social service or national ID applications.
g. Convenience of having authenticating mechanisms with a user. We can't forget parts of our body at home, and we can't lend it. We don't need to memorize fingerprints and then change it every 3 months as with passwords.
h. Biometrics can last virtually forever, until something is amputated or damaged.
i. No more forgotten passwords, lost cards or stolen pins. You are your own password.
j. Positive Identification-It identifies you and not what you have or what you carry.
k. It provides highest level of security.
l. It offers mobility.
m. Increased security when controlling access to confidential data and IT systems.
n. Reduced risk of fraudulent use of identity by employees.
o. Biometrics can potentially provide cost savings through relocating security resources or diminishing the expenses associated with password maintenance, or it could cause extra costs by highlighting problems that were previously missed. The cost benefits vary from application to application as well.

DEMERITS

a. There is a factor of users accepting or not accepting a particular biometric technique. Some people are still hesitant to be authenticated using fingerprints, since it was associated for a long time with criminals and prisons
b. Most biometric technologies are patented, which means it is very expensive to companies to license the use and implementation of any type of biometrics.
c. Another big issue in biometric implementation is software support for the biometric hardware devices.
d. An automatic personal identification system based solely on fingerprints or faces is often not able to meet the system performance requirements.
e. In case of face recognition, face will sometimes change with time or injury, and that poses a problem
f. Fingerprint verification is reliable but inefficient in database retrieval.
g. Some voice recognition systems has some problems since the voice changes with a human's mood and illness and background noise poses some problems.

FACIAL EXPRESSION RECOGNITION

Automatic recognition of facial expressions may act as a component of natural human machine interfaces Such interfaces would enable the automated provision of services that require a good appreciation of the emotional state of the service user, as would be the case in transactions that involve negotiation, for example. Some robots can also benefit from the ability to recognize expressions .

Automated analysis of facial expressions for behavioral science or medicine is another possible application domain From the viewpoint of automatic recognition, a facial expression can be considered to consist of deformations of facial components and their spatial relations, or changes in the pigmentation of the face. Research into automatic recognition of facial expressions addresses the problems surrounding the representation and categorization of static or dynamic characteristics of these deformations or face pigmentation.

There is a vast body of literature on emotions. Recent discoveries suggest that emotions are intricately linked to other functions such as attention, perception, memory, decision making, and learning. This suggests that it may be beneficial for computers to recognize the human user's emotions and other related cognitive states and expressions. Ekman and Friesen [7] developed the Facial Action Coding System (FACS) to code facial expressions where movements on the face are described by a set of action units (AUs). Each AU has some related muscular basis. This system of coding facial expressions is done manually by following a set of prescribed rules. The inputs are still images of facial expressions, often at the peak of the expression. Ekman's work inspired many researchers to analyze facial expressions by means of image and video processing. By tracking facial features and

measuring the amount of facial movement, they attempt to categorize different facial expressions. Recent work on facial expression analysis and recognition has used the "basic expressions" (i.e., happiness, surprise, fear, disgust, sad, and anger) or a subset of them. The two recent surveys in the area [16, 8] provide an in depth review of the existing approaches towards automatic facial expression recognition. These methods are similar in that they first extract some features from the images, then these features are used as inputs into a classification system, and the outcome is one of the preselected emotion categories. They differ mainly in the features extracted from the video images and in the classifiers used to distinguish between the different emotions. Mehrabian reported that facial expressions have a considerable effect on a listening interlocutor; the facial expression of a speaker accounts for about 55 percent of the effect, 38 percent of the latter is conveyed by voice intonation and 7 percent by the spoken words.

As a consequence of the information that they carry, facial expressions can play an important role wherever humans interact with machines. Some robots can also benefit from the ability to recognize expressions. Automated analysis of facial expressions for behavioral science or medicine is another possible application domain [6] [9].

STATIC AND DYNAMIC FACIAL EXPRESSION RECOGNITION

In Case of Expression Recognition from still image, face detection is the first stage which is desired to be automated. In most of the research, face is already cropped and the analysis starts with feature extraction and tracking. In the rest, automated face detectors are used. These can be classified mainly into two classes: vision-based detection and detection using infrared (IR) cameras. Spors and Rabenstein [5] use skin color detection and principal component analysis (PCA) based eye localization to locate the face for their tracking algorithm. To reduce the computational complexity further, the eye detection and tracking task is divided into two steps in their work. First the eye is localized. When the position of the eyes is known, tracking is performed using a luminance-adapted block matching technique.

Numerous features have been applied to the facial expression recognition problem. Image-based models rely on the pixel values of the whole image (holistic) or related parts of the image (local). On the other hand, model-based approaches create a model that best represents the face by using training images. Feature points are also used as features to feed in the classifier or to play an avatar. Difference images are used to find the eye coordinates from the image pairs gathered by IR cameras. In the initial research done in this area, markers were used to analyze the facial data. In addition, optical flow and motion models are also used in feature extraction and tracking.

The image-based and model-based approaches are more dominant in the literature. As an image-based technique, Gabor wavelets are widely used in facial feature detection. Dubuisson et al. [14] apply triangulation to the magnitude of the filtered image which is passed through the Gabor kernel. Then, they detect the three boxes containing the facial features (eye regions and the mouth region) with a classification of the regions laying in the convex envelope of the triangulation. Gokturk et al. [23] create a 3D deformable model from stereo tracking and apply PCA in their study. The resulting model approximates any generic shape as a linear combination of shape basis vectors. The additional optical flow tracking computes the translational displacement of every point.

Statistical approaches have three main stages: "capture", "normalization" and "statistical analysis". In brief, in the capture part, one defines a certain number of points (landmarks) on the contour of the object in question for shape and uses image warping for texture. The following shape normalization is done using Procrustes Analysis and texture normalization is done by removing global illumination effects between frames. Finally, Principal Components Analysis (PCA) is performed to analyze the variances between object shapes or textures and this information is also used for synthesis. Active Shape Models (ASMs) and Active Appearance Models (AAMs) are two widely used statistical approaches where both of them are proposed by Cootes et al. in [21] and [19] respectively. The AAM approach is used in facial feature tracking due to its ability in detecting the desired features as the warped texture in each iteration of an AAM search approaches to the fitted image. Ahlberg [7], and Abboud and Davoine [20] use AAM in their work. In addition, ASMs - which are the former version of the AAMs that only use shape information and the intensity values along the profiles perpendicular to the shape surface are also used to extract features such as the work done by Votsis et al. [22].

To recognise expression the outstanding technique is the kNN, as they report. In the work of Franco and Treves [18], a rectangular region of the face that involves one eye and half of the mouth and nose is cropped from the images. The pixel values of this cropped rectangle are given as input to the neural networks (NN) classifier for classification into one of neutral, happy, sad or surprised expressions. In addition to analysis from image sequences, there is also work done on still images. Buciu [30] applies discriminant non-negative matrix factorization (DNMF), Abboud and Davoine apply decision tree based classifier [20], and Buciu and Pitas [16] apply nearest neighbor using cosine similarity measure and maximum correlation classifier to the images selected from Cohn-Kanade image database [31]. Dubuisson et al. [14] also use the same database and perform two types of classification. A binary classifier is used to distinguish between two confusing classes and a 6-class classifier is used for general classification.

In case of Dynamic expression Recognition Feature extraction methods can be categorized according to whether they focus on motion and deformation of faces and facial features. Motion extraction approaches directly focus on facial changes occurring due to facial expressions, whereas deformation-based methods do have to rely on neutral face images in order

to extract facial features. In motion feature extraction image processing is performed in two steps. In the first step, a velocity vector is obtained from every two successive frames by using a gradient based optical flow algorithm [21]. To improve performance, the region for processing is confined to two small regions, one is eye-brow region, and another is mouth region. These regions were selected based on the results from three-dimensional measurements of expressions, and as such they proved to be the regions in which the changes were most pronounced. In the second step, a feature vector construction processing is applied to a vertical and a horizontal component of the velocity vector field at the regions around an eye and the mouth.

The use of optical flow to track motion is advantageous because facial features and skin naturally have a great deal of texture. Using feature vector construction, a low-dimensional weight vector in eigenspace can be obtained to represent the high-dimensional dense flows of each frame. Based on the displacement and weight vectors, the motion information is converted to symbol sequences from which we can recognize facial expressions.These regions were selected based on the results from three-dimensional measurements of expressions, and as such they proved to be the regions in which the changes were most pronounced.

Facial expression Recognition can be regarded as a pattern recognition problem. It is necessary to model dynamic facial feature vector sequence in order to analyze facial expression sequence. Modeling facial expression needs to take into account the stochastic nature of human facial expression involving both the human mental state, which is hidden or immeasurable, and the human action, which is observable or measurable. For example, different people with the same emotion may exhibit very different facial actions, expression intensities and durations. Individual variations notwithstanding, a human observer can still recognize what emotion is being expressed, indicating that some common element underlies each motion. Therefore, the purpose of facial expression modeling is to uncover the hidden patterns associated with specific expressions from the measured (observable) data. Facial expression modeling requires a criterion for measuring a specific expression. It is desirable to analyze a sequence of images to capture the dynamics. Expressions are recognized in the context of an entire image sequence of arbitrary length. A recognition system is develop based on the stochastic modeling of the encoded time series describing facial expressions, which should perform well in the spatio-temporal domain, analogous to the human performance.

SUMMARY

Every individual is unique, while the overall human structure is the same; this approach puts biometrics in a great demand in the constantly updating field of security. Biometrics is a science of automatically identifying individuals based on their unique physiological or behavioral characteristics. A number of civilian and commercial applications of biometrics-based identification are emerging. At the same time, a number of legitimate concerns are being raised against the use of biometrics for various applications; three of them appear to be the most significant: cost, privacy, and performance. Though the approach is still in its infancy, many people believe that biometrics will play a critical role in future computers, and especially in electronic commerce. It seems like every part of a human body was tested to determine if it is produce a unique pattern: face and ear shapes, voice and odor, retina and iris, fingerprints, DNA, gait and veins of a hand. Obviously for convenience reasons, only normally visible parts of a body were implemented; probably users wouldn't want to take the shoes off to measure a toes pattern or the pressure applied while walking. May be someday we will be authenticating people by a heart beat or a spit out, it all depends on the progress we are making in the field, the demand of different identifiers and hackers success in reproducing someone's characteristics.

This paper is an introduction to biometric and its techniques and review on facial expression recognition. This may help us to predict future trends/behaviors, allowing business to make proactive and knowledge-driven decisions.

REFERENCES

[1]. Boles W. and Boashash B. (1998), "A human identification technique using images of the iris and wavelet transform", IEEE Trans. Signal Proc., Vol. 4, pp. 1185-1188.

[2]. Woodward J., Orlans N. and Higgins (2007), "Identity Assurance in the information Age: BIOMETRICS", Tata McGraw Hill, New Delhi.

[3]. Wildes R. P., Asmuth J. C. (1994), "A System for Automated Iris recognition", Proc. of IEEE workshop on Application of Computer Vision, Florida, pp 121-128.

[4]. Tan T., Zhu Y. and Y. Wang (2002), "Biometric personal identification based on iris pattern", ICPR2000: the 15th International Conference on Pattern Recognition, Barcelona, Spain, pp. 805-808.

[5]. Jain A., Ross A., Prabhakar S. (2004), "An introduction to Biometric recognition", IEEE Trans. on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No.1, pp. 4-20.

[6]. Bourel, F., Chibelushi C.C., Low A.A., (2002) "Robust Facial Expression Recognition Using a State- Based Model of Spatially-Localised Facial Dynamics", Proc. Fifth IEEE Int. Conf. Automatic Face and Gesture Recognition, pp. 106-111.

[7]. Bartlett, M. A., Hager, J. C., Ekman P., and Sejnowski T., (1999) "Measuring facial expressions by computer image analysis", Psychophysiology, Vol. 36, No. 2, pp. 253–263.

[8]. Cohen, I., Sebe, N., Cozman, F., Cirelo, M., and Huang, T.,(2004) "Semi-supervised learning of classifier" Theory, algorithms, and applications to human-computer interaction. Vol.26, No. 12, pp.1553–1567.

[9]. Cohen, I., Sebe, N., A., Garg, L. Chen, Huang, T.S..,(2003) "Facial expression recognition from video sequences: Temporal and static modeling",. CVIU, Vol. 91, pp.160–187.

[10]. Cootes, T. and Kittipanya-ngam, P.,(2002) "Comparing variations on the active appearance model algorithm.", In BMVC, pp 837– 846.

[11]. Cootes, T., Edwards, G., and Taylor C.,(2001) " Active appearance models". PAMI, Vol. 23, No. 6, pp. 681–685.

[12]. Chellappa, R., Wilson C.L., Sirohey S.,(1995) "Human and Machine Recognition of Faces: a Survey", Proc. IEEE, Vol. 83, No. 5, pp. 705-741.

[13]. Donato, G., Bartlett, M.S., Hager, J.C. , Ekman, P., Sejnowski, T.J.,(1999) "Classifying Facial Actions", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 21, No. 10, pp. 974-989.

[14]. Ekman, P., and Friesen, W.,(1978) " Facial Action Coding System: Investigator's Guide", Consulting Psychologists Press.

[15]. Fasel, B. and Luettin, J..(2003)" Automatic facial expression analysis:" A survey. Pattern Recognition, Vol. 36, pp.259–275.

[16]. Geetha, A., Ramalingam, V., Palanivel, S. and Palaniappan, B.," Facial expression recognition – A real time approach" Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram, India, Vol. 36,pp. 303-308.

[17]. Jain, A.K., Duin R.P.W., Mao J.,(2000) "Statistical Pattern Recognition: A Review", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 22, No. 1, pp. 4-37.

[18]. Kapoor, A., Yuan Qi and Picard, R. W., (2003) " Fully Automatic Upper Facial Action Recognition", MIT Media Laboratory, Cambridge.

[19]. Lien, J., Kanade T., Cohn J., and C. C. Li.,(2000) "Detection, tracking and classification of action units in facial expression" Journal of Robotics and Autonomous Systems, Vol. 31, pp. 131–146.

[20]. Lien, J.J., Kanade, T., Cohn, J.F., Li, C-C.,(1998) "Automated Facial Expression Recognition Based on FACS Action Units", Proc. Third IEEE Int. Conf. Automatic Face and Gesture Recognition, pp. 390-395.

[21]. Pantic, M. and Rothkrantz, L.,(2000) " Automatic analysis of facial expressions: The state of the art",. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. 12, pp.1424–1445

[22]. Samal, A., and Iyengar, P.A. , (1992) "Automatic Recognition and Analysis of Human Faces and Facial Expressions: A Survey", Pattern Recognition, Vol. 25, No. 1, pp. 65-77.

[23]. Tian, Kanade, T., and Cohn J. F.,(2001) "Recognizing action units for facial expression analysis" Pattern Analysis and Machine Intelligence, Vol. 23, No. 2.

[24]. Tao, H. and Huang, T. (1998) " Connected vibrations: A modal analysis approach to non-rigid motion tracking", In Proc. IEEE Conference on Computer Vision and Pattern Recognition, pp. 735–740.

[25]. Viola, P., and Jones, M.,(2004) "Robust real-time object detection" ,International Journal of Computer Vision, Vol. 57, No. 2, pp.137–154.

[26]. Yang, J., Zhang, D., (2004) "Two-dimensional pca: a new approach to appearance-based face representation and recognition", IEEE Trans. Pattern Anal. Mach. Intell.Vol. 26, No. 1, pp. 131–137.

Short Bio Data for the Author

Renu Nagpal received diploma in Computer Engineering in 2002 from Technical Board,Chandigarh. B. Tech degree in Computer Science and Engineering in 2005 under Punjab Technical University,Jalandhar. Presently she has completed her M.Tech in 2010 from Yadavindra College of Engineering,Guru Khashi Campus,Talwandi Sabo,Bathinda(Punjab).Now she is pursuing Phd from Punjab Technical University,Jalandhar. Her interests include, Image Processing, Swarm Intelligence, neural networks,bacteria foraging. She has contributed near about 10 technical papers in various national and international conferences. She is a life member of ISTE.

Pooja Nagpal received diploma in Computer Engineering in 2004 from Technical Board, Chandigarh. B. Tech degree in Computer Science and Engineering in 2007 under Punjab Technical University,Jalandhar.She has completed her M.Tech in 2011from Yadavindra College of Engineering, Guru Khashi Campus,Talwandi Sabo,Bathinda(Punjab) Her interests include, Image Processing,Optimozation and Swarm Intelligence .She has contributed near about 8 technical papers in various national and international conferences. She is a life member of ISTE.

Sumit Malhotra received B. Tech degree in Computer Science and Engineering in 2006 under Guru Nanak Dev University,Regional Campus,Jalandhar.Since 2011 he is pursuing his M.Tech from Punjabi University Patiala(Punjab). His interests include,data mining .He has contributed near about 4 technical papers in various national and international conferences. She is a life member of ISTE.