International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

Constraints of 2D Face Recognition Crafts Way for 3D Face Recognition Technique

Gagandeep Jagdev[1], Sukhpreet Singh[2], Tejinder Singh[3], Devinder Singh Joshi[4]

[1]Dept. of Comp. Science, University, Punjabi University Guru Kashi College, Damdama Sahib (PB), India

[2,3,4]Guru Kashi University, Talwandi Sabo (PB), India

Email address: [1]gagans137@yahoo.co.in

***Abstract*—**There are many biometric techniques in existence today. Face recognition technology is one of them which make use of computer software to determine the identity of the person. Today conservative methods of identification like possession of certain type of identity cards, use of passwords etc. are not at all reliable for identity purposes where security is a critical factor. There is no surety in the fact that person using ATM card to withdraw money from any ATM machine is actual owner of the card. When credit and ATM cards are lost or stolen, it is not a big game for the unauthorized user to make an accurate guess of the correct personal codes. It is a common practice between we people that despite of strict warning we continue to choose easily guessed PIN's and passwords. Often we prefer our birthdays, cell numbers, house numbers and vehicle numbers. Identity cards can be lost, fake or misplaced and passwords can be forgotten or compromised. But a face is unquestionably connected to its owner. Face does not suffer the limitations of been borrowed, stolen or easily copied. Face recognition technology is the fastest and least intrusive biometric technology. Human face is one such part of the human body that can help us to identify and differentiate between two individuals. Unlike fingerprint recognition technology or palm recognition technology which requires people to place their fingers or hand on a reader or precisely position their eye in front of a scanner, face recognition systems unobtrusively take pictures of people's faces as they enter a defined area. There is no intrusion or delay, and in most cases the subjects are entirely uninformed of the process. They do not know that they are under surveillance [14]. In this research paper we will deeply discuss about two popular 2D face recognition algorithm techniques and also explore the facts where 2D face recognition technique falls short in proper identification and how 3D face recognition techniques removed the complexities of 2D face recognition technique.

***Keywords*—**2D face recognition; 3D face recognition; biometric; Eigenface; FRT (face recognition technique); illumination.

I. INTRODUCTION

As the necessity for higher levels of security rises, technology is bound to swell to fulfill these needs. Any new creation, enterprise, or development should be uncomplicated and acceptable for end users in order to spread worldwide. This strong demand for user-friendly systems which can secure our assets and protect our privacy without losing our identity in a sea of numbers, grabbed the attention and studies of scientists toward what's called biometrics. Since, after 9/11 biometrics is getting a titanic attention all over the world by scientist, researchers and engineers. Now days everywhere in the world security is given the top priority to counter the possible treats from terrorists and hence biometrics and security are the synonyms. Biometric systems are spreading rapidly at all security prone areas such as airports, banks, offices also with documentation like passport, identity card, driving license, etc. Reliable user identification is increasingly becoming important in the Web enabled world today and there has been a significant surge in the use of biometrics for user identification. Many corporate heads use laptops and personal digital assistants (PDAs) loaded with sensitive business and personal information. According to the Gartner group, over 250,000 mobile gadgets are lost or stolen every year, and only 25-30 per cent of these ever make it back to their rightful owners. Such mishaps have created a dire need to ensure denial of access to classified data by unauthorized persons. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometrics technology is based on identification of individuals by a physical or behavioral characteristic. Examples of recognition of physical characteristics are fingerprints, iris, and face or even hand geometry. Behavioral characteristic can be the voice, signature or other keystroke dynamics. Biometrics is the budding area of bioengineering. It is the automated method on basis of which one can identify a person based on his/her physiology. Biometrics modes of identification have been found to be the most compelling and intriguing authentication technique. Tokens can be lost, stolen or duplicated and passwords can be forgotten or shared. Forgotten passwords and lost smart cards are a nuisance for users and waste the expensive time of system administrators. However, biometrics can authenticate you as you. Biometrics is a means of using parts of the human body as a kind of permanent password. Using biometrics for identifying and authenticating human beings offers unique advantages over traditional methods. Biometrically secured resources effectively eliminate risks, while at the same time offering a high level of security and convenience to both the users and the administrators.

Advantages of Biometrics

- *Increased security* - Swipe cards and PIN numbers can easily be obtained by potential intruders, whereas acquiring a subject's biometric requires specialist knowledge and equipment, and in most cases would not be possible without alerting the subject's attention.
- *Reduced fraud* - It becomes extremely difficult for somebody to willingly give up his or her biometric data, so sharing identities is virtually impossible. In addition, because it becomes necessary to expose one's own biometric data (i.e. your own face), potential fraudsters are reluctant to attempt false verification.
- *Cost reduction*. By replacing plastic swipe cards, all cost associated with producing, distributing and replacing a lost card is completely eliminated.

Gagandeep Jagdev and Mandeep Kaur, "Constraints of 2D face recognition crafts way for 3D face recognition technique", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 41-46, 2015.

ISSN: 2454-1532

Face is a person's most exclusive physical characteristic through which he or she can be identified uniquely. As like humans have the ability to identify faces since their existence on the planet earth, the computers now have begun to catch up with the humans.

Advantages of FRT over Other Biometrics

- *Non-intrusive.* Whereas most biometrics require some degree of user interaction in order to acquire biometric data, such as looking into an eye scanner or placing a finger on a fingerprint reader, accurate face recognition can be performed by simply glancing at a camera from a distance. This non-contact biometric acquisition is highly desirable when subjects being scanned are customers, that may have some reluctance due to the big-brother stigma or associated criminality-surrounding acquisition of personal data and therefore the whole process needs to be kept as convenient as possible. This capability can be taken a step further, using strategic camera placement to perform recognition even without the subject's knowledge. An obvious example would be CCTV cameras monitoring an area for known criminals or tracking a suspected terrorist from one location to another.
- *Public acceptance.* It has become apparent that face recognition systems generally receive a higher level of public acceptance than most other biometrics. This is perhaps partly due to the non-intrusive nature of face recognition as described above, but may also be the result of greater understanding and empathy of how the technology is capable of recognizing a face; it is well known that the public fear what they do not understand. Another factor is the association that other biometrics have with crime (i.e. fingerprints). Whatever the reason, people have become accustomed to their facial image being required by numerous organisations and few people now object to looking at a camera for the purpose of biometric recognition. It is another thing entirely to require a more committed action on behalf of the subject, such as leaning into an eye scanner or making contact with some other scanning device. With many obvious benefits of integrating biometrics into governmental organizations (such as the NHS, welfare system or national ID cards), public acceptance is an important factor if these systems are to be implemented nationwide.
- *Existing databases*. One key hold-up for any large organisation considering implementation of a biometric system is the amount of time required in collection of a biometric database. Consider a police force using an iris recognition system. It would take a number of years before the database was of sufficient size to be useful in identifying suspects. Whereas large databases of high quality face images are already in place, so the benefits of installing a face recognition system are gained immediately after installation.
- *Analogy to human perception.* Perhaps the greatest advantage, (which is also often the most ignored) is that the biometric data required for face recognition (an image of a face) is recognizable by humans. This allows for an additional level of backup, should the system fail. A human reviewing the same biometric source (the reference image and live query image) can always manually check any identification or verification result.

There are two methods through which faces of the individuals can be recognized. One is of identification and second one is of verification. There is big difference between working of these two methods as explained below.

Verification – Verification refers to the process which requires a PIN or a kind of a password. After a user provides an appropriate password his/her face is compared with the face which lies against that particular account in the database or template. It means that verification is a one to one mapping. If the face passes in the matching process, the person is recognized as a authorized user, else not. This is where the system compares the given individual with who that individual says they are and gives a yes or no decision

Identification – Unlike verification, identification is a one to many sort of mapping. In this no password or PIN is used. The face is compared with all the faces which already exist in the template. This is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches

All identification or authentication technologies operate using the following four stages:

- *Data acquisition/capture*: A physical or behavioral sample is captured by the system during enrollment and also in identification or verification process. Physical sample may be face, fingerprints, iris etc. Behavioral sample may be person's signature, gait etc. In case of face recognition the input can be recorded video of the speaker or a still image. A sample of 1 sec duration consists of a 25 frame video sequence. More than one camera can be used to produce a 3D representation of the face and to protect against the usage of photographs to gain unauthorized access.
- *Extraction*: In this step unique data is extracted from the sample and a template is created. A pre-processing module locates the eye position and takes care of the surrounding lighting condition and color variance. First the presence of faces or face in a scene must be detected.
- *Comparison*: Once the face is detected, it must be localized and normalization process may be required to bring the dimensions of the live facial sample in alignment with the one on the template. The template is then compared with a new sample.
- *Match/non match*: Finally the system decides if the features extracted from the new sample are a match or a non match.

Digital video camera is used to analyze the characteristics of a person's face images. It observes and measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are then stored in a database and are later on used as a comparison when a user stands before the camera. This biometric has been widely advertized as a fantastic system for recognizing potential threats like terrorist attacks, criminals etc. But till date it has not seen wide acceptance in high-level usage. It is projected that biometric facial recognition technology will soon overtake fingerprint biometrics as the most popular form of user authentication [15].

Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. Each human face has approximately 80 nodal points. Some of these measured by the Facial Recognition Technology are:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

These nodal points are measured creating a numerical code, called a face print, representing the face in the database.

Gagandeep Jagdev and Mandeep Kaur, "Constraints of 2D face recognition crafts way for 3D face recognition technique", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 41-46, 2015.

ISSN: 2454-1532

II. Algorithms Developed for 2D Face Recognition

Face recognition is a challenging problem because of the ethnic diversity of faces and variations caused by expressions, gender, pose, illumination and makeup. Appearance based (2D) face recognition algorithms were the first to be investigated due to the wide spread availability of cameras. One of the classic face recognition algorithms uses the eigenface representation of Turk and Pentland which is based on the Principal Component Analysis (PCA). Linear Discriminate Analysis (LDA), Independent Component Analysis (ICA), Bayesian methods and Support Vector Machines (SVM) have also been successfully used for appearance based face recognition [11], [12].

Eigenface-based recognition and Fisherfaces based recognition were the two most popular techniques of the algorithms that existed for 2D face recognition and are discussed below.

A. Eigenface-Based Recognition

The oldest type of face recognition using eigenfaces was published by Turk and Pentland in the year 1991. This algorithm is based on PCA (Principle Component Analysis). PCA seeks directions that are efficient for representing the data. It is relatively simple fast and robust. The method works by analyzing face images and computing eigenfaces which are faces composed of eigenvectors. The comparison of eigenfaces is used to identify the presence of a face and its identity [4], [5]. The working of Eigenface-based recognition algorithm is explained below.

- First, the set of training images is given as an input into the system to initialize it. It determines the face space which is set of images which are similar to faces.
- Secondly, when a face is encountered, an Eigenface is calculated for it.
- Thereafter few statistical analyses are performed between the input image and some known faces to determine that the image presented is a face at all.
- Next, after the image is determined to be a face, it is the job of the system to recognize that whether it knows the identity of the face or not.
- Last, if an unknown face is seen again and again, the system can learn to recognize it.

There are also some limitations of eigenfaces.

- This technique is not well suited for robustness to changes in lighting, angle, and distance.
- 2D recognition systems do not capture the actual size of the face, which is a fundamental problem.
- These limits affect the technique's application with security cameras because frontal shots and consistent lighting cannot be relied upon.

B. Fisherfaces Based Recognition

Fisherfaces algorithm was developed in 1997 by P.Belhumeur et al. The algorithm is based on Fisher's Linear Discriminant Analysis (LDA). As compared to eigenfaces, this algorithm is faster than eigenfaces in some cases. Moreover this algorithm has lower error rates and works well in different illumination conditions. This technique is also capable of recognizing different facial expressions unlike Eigenface-based algorithm. Two important points related to functioning of LDA are mentioned below.

- LDA maximizes the between-class scatter
- LDA minimizes the within-class scatter

III. 3D Face Recognition Technique

Two-dimensional face recognition systems use a standard 2D image (either colour or grey scale), often captured by means of a camera and frame-grabber, web-cam or scanned photograph, to perform recognition. Such systems have been in use for a number of years; incorporated into biometric access systems in airports, used in identification procedures in police departments and CCTV surveillance systems. However, these two-dimensional approaches are held back by a few critical problems. Firstly, such systems are extremely sensitive to head orientation, meaning that in order to achieve a positive verification the subject must be facing directly towards the camera (front-to-parallel orientation). The result is that throughput of site access systems is considerably reduced (subjects often have to attempt several verifications to achieve the correct orientation) and surveillance systems rely on luck that the subject will face the camera. The second major problem is lighting conditions. If the subject is enrolled in an environment with different lighting conditions (including direction, intensity and colour) to that when verification is performed, the subject is often falsely rejected.

Compared to the wealth of research carried out into 2D face recognition, there has been relatively little research into 3D facial recognition. There appears to be three main reasons for this:

- *Availability of data.* 2D images of faces are readily available on-line and easily created with use of a standard camera. 3D facial surface data, however, is scarcely available, if at all, and creation of such data can be a complex and expensive process.
- *Range of applications*. 3D recognition limits the possible applications to time and attendance, surveillance (in a highly controlled environment) and security applications, due to the need for especially dedicated equipment. This can be seen as particularly limiting, when compared to 2D methods, which could be applied to searching, indexing and sorting the existing image archives of legacy systems.
- *Human analogy*. Humans are capable of recognizing a face in a photograph (a 2D image) to a high degree of accuracy. This has lead to the notion that a 2D image is all that is necessary for a machine to recognize a face.

There are several issues that are responsible for plaguing 2D face recognition systems. 3D face recognition is expected to be robust to the types of issues that plague 2D systems. 3D systems generate 3D models of faces and compare them. 3D face recognition systems are more accurate because they capture the actual shape of faces. In addition to face recognition, skin texture analysis can be used to improve accuracy by 20 to 25 percent. The acquisition of 3D data is one of the main problems for 3D systems [2], [3], [13].

A. Stereo Acquisition Technology

Among different existing biometric alternatives, facial images offer a good trade-off between acceptability and reliability. There is no second thought in the fact that iris and fingerprint biometrics provide accurate authentication, and are more established as biometric technologies but the acceptability of face as a biometric makes it more convenient. 3D face recognition is primarily aimed at boosting the accuracy of the face modality, thereby creating a reliable and non-intrusive biometric. Today there is wide range of 3D acquisition technologies, with different cost and operation characteristics. The most cost-effective solution is to use several standardized and adjustable 2D cameras to acquire images simultaneously, and to reconstruct a 3D surface. This concept is called stereo acquisition and number of cameras may be two or more. A positive aspect of stereo acquisition technology is that the acquisition is fast

Gagandeep Jagdev and Mandeep Kaur, "Constraints of 2D face recognition crafts way for 3D face recognition technique", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 41-46, 2015.

ISSN: 2454-1532

and calibration settings helps in adjusting the distance to the cameras. The reconstruction process for stereo acquisition can be made easier by projecting a structured light pattern on the facial surface during acquisition. If a projection apparatus is provided, the structured light methods can work even with a single camera. This usually entails a larger cost when compared to stereo systems, but provides higher scan accuracy. The potential drawbacks of structured light systems are

- Sensitivity to external lighting conditions
- Requirement of a specific acquisition distance for which the system is calibrated.
- Third problem related with structured light is that the projected light interferes with the color image, and needs to be turned off to generate it. Some sensors have the capability of avoiding this problem by using near infrared structured light. Yet a third category of scanners relies on active sensing. A laser beam reflected from the surface indicates the distance, producing a range image. These types of laser sensors, used in combination with a high resolution color camera, give high accuracies, but sensing takes time.

The typical acquisition distance for 3D scanners varies between 50 cm and 150 cm, and laser scanners are usually able to work with longer distances (up to 250 cm) when compared to stereo and structured light systems. Structured light and laser scanners require the subject to be motionless for a short duration (0.8 to 2.5 seconds in the currently available systems), and the effect of motion artifacts can be much more damaging for 3D in comparison to 2D. Laser scanners are able to provide 20-100µm accuracy in the acquired points. The presence of strong motion artifacts would make a strong smoothing necessary, which will dispel the benefits of having such a great accuracy. Simultaneous acquisition of a 2D image is an asset, as it enables fusion of 2D and 3D methods to potentially greater accuracy. The amount of collected data affects scan times, but also the time of transfer to the host computer, which can be significant. For instance a Minolta 910 scanner requires 0.3 seconds to scan the target in the fast mode (about 76K points), and about 1 second to transfer it to the computer. Longer scan times also result in motion-related problems, including poor 2D-3D correspondence [10].

Although 3D offers additional information that can be exploited to infer the identity of the subject, this is still not a trivial task: External factors such as illumination and camera pose have been cited as complicating factors. However, there are internal factors as well: Faces are highly deformable objects, changing shape and appearance with speech and expressions. Humans use the mouth and the vocal tract to produce speech; and the whole set of facial muscles to produce facial expressions. Human vision can deal with face recognition under these conditions. Automatic systems are still trying to devise strategies to tackle expressions. A third dimension complicating face recognition is the time dimension. Human faces change primarily due to two factors. The first factor is ageing: All humans naturally age. This happens very fast at childhood, somewhat slower once adulthood is reached. The other factor is intentional: Humans try to change the appearance of their faces through hair style, make-up and accessories. Although the intention is usually to enhance the beauty of the individual, the detrimental effects for automatic face recognition are obvious [6], [7].

B. Steps Involved in 3D Face Recognition Technology

A newly-emerging trend in facial recognition software uses a 3D model, which claims to provide more accuracy. Capturing a real-time3D image of a person's facial surface, 3D facial recognition uses distinctive features of the face -- where rigid tissue and bone is most apparent, such as the curves of the eye socket, nose and chin -- to identify the subject. These areas are all unique and don't change over time.

Using depth and an axis of measurement that is not affected by lighting, 3D facial recognition can even be used in darkness and has the ability to recognize a subject at different view angles with the potential to recognize up to 90 degrees (a face in profile). Using the 3D software, the system goes through a series of steps to verify the identity of an individual as shown in Fig. 1 [8], [16].

- *Detection* - Acquiring an image can be accomplished by digitally scanning an existing photograph (2D) or by using a video image to acquire a live picture of a subject (3D).
- *Alignment* - Once it detects a face, the system determines the head's position, size and pose. As stated earlier, the subject has the potential to be recognized up to 90 degrees, while with 2D, the head must be turned at least 35 degrees toward the camera.
- *Measurement* - The system then measures the curves of the face on a sub-millimeter (or microwave) scale and creates a template.
- *Representation* - The system translates the template into a unique code. This coding gives each template a set of numbers to represent the features on a subject's face.
- *Matching* - If the image is 3D and the database contains 3D images, then matching will take place without any changes being made to the image. However, there is a challenge currently facing databases that are still in 2D images. 3D provides a live, moving variable subject being compared to a flat, stable image. New technology is addressing this challenge. When a 3D image is taken, different points (usually three) are identified. For example, the outside of the eye, the inside of the eye and the tip of the nose will be pulled out and measured. Once those measurements are in place, an algorithm (a step-by-step procedure) will be applied to the image to convert it to a 2D image. After conversion, the software will then compare the image with the 2D images in the database to find a potential match.
- *Verification or Identification* - In verification, an image is matched to only one image in the database (1:1). For example, an image taken of a subject may be matched to an image in the Department of Motor Vehicles database to verify the subject is who he says he is. If identification is the goal, then the image is compared to all images in the database resulting in a score for each potential match (1: N). In this instance, you may take an image and compare it to a database of mug shots to identify who the subject is.

Gagandeep Jagdev and Mandeep Kaur, "Constraints of 2D face recognition crafts way for 3D face recognition technique", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 41-46, 2015.

International Journal of Scientific and Technical Advancements

ISSN: 2454-1532

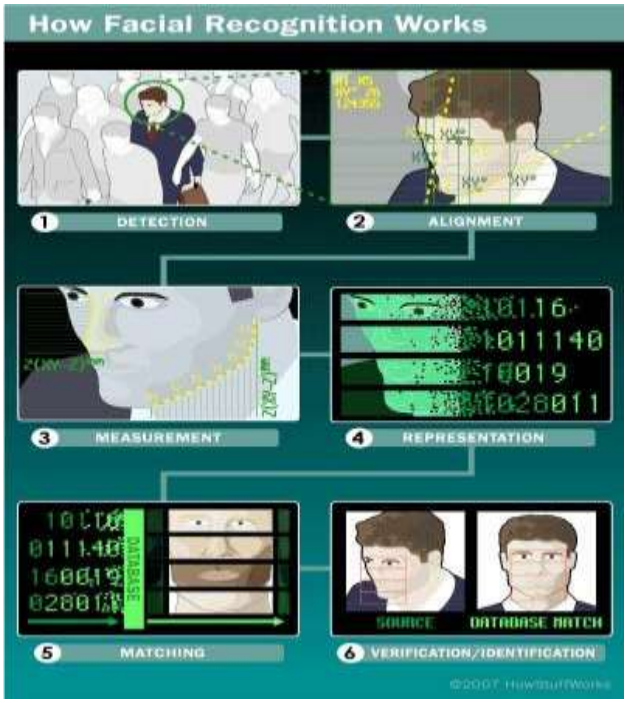

Fig. 1. Steps involved in 3D face recognition technology.

C. 2.5D and 3D images

Generally, for 3D face recognition is intended a class of methods that work on a three-dimensional dataset, representing both face and head shape as range data or polygonal meshes. The main advantage of the 3D based approaches is that the 3D model retains all the information about the face geometry. Moreover, 3D face recognition also growths to be a further evolution of 2D recognition problem, because a more accurate representation of the facial features leads to a potentially higher discriminating power. In a 3D face model, facial features are represented by local and global curvatures that can be considered as the real signature identifying persons. The 3D facial representation seems to be a promising tool coping many of the human face variations, extra-personal as well as intrapersonal. Two main representations are commonly used to model faces in 3D applications that are 2.5D and 3D images (see Fig. 2). A 2.5D image (range image) consists of a two dimensional representation of a 3D points set (x,y, z), where each pixel in the X–Y plane stores the depth value z. One can think of a 2.5D image as a grey-scale image, where the black pixel corresponds to the background, while the white pixel represents the surface point that is nearest to the camera. In particular, a 2.5D image taken from a single viewpoint only allows facial surface modeling, instead of the whole head. This problem is solved by taking several scans from different viewpoints, building a 3D head model during a training stage. On the contrary, 3D images are a global representation of the whole head, and the facial surface is further related to the internal anatomical structure, while 2.5D images depend on the external appearance as well as environmental conditions. The simplest 3D face representation is a 3D polygonal mesh, that consists of a list of points (vertices) connected by edges (polygons). There are many ways to built a 3D mesh, the most used are combining several 2.5D images, properly tuning a 3D morphable model or exploiting a 3D acquisition system (3D scanner). A further difference between 2.5D and 3D images is that last ones are not affected by self-occlusions of the face, when the pose is not full-frontal [9].

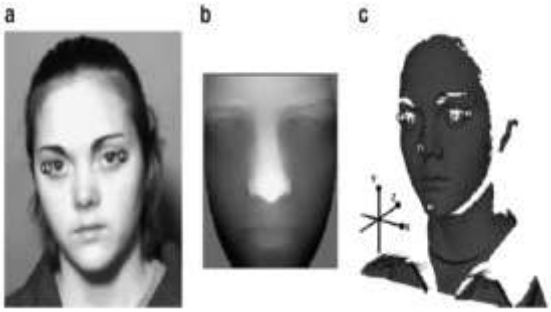

Fig. 2 (a) 2D image (b) 2.5D image (c) 3D image.

IV. Conclusion and Future Work

Face recognition systems used today work very well under constrained conditions, although all systems work much better with frontal mug-shot images and constant lighting. All current face recognition algorithms fall under the vastly varying conditions under which humans need to and are able to identify other people. Next generation person recognition systems will need to recognize people in real-time and in much less constrained situations.

We believe that identification systems that are robust in natural environments, in the presence of noise and illumination changes, cannot rely on a single modality, so that fusion with other modalities is essential. Technology used in smart environments has to be unobtrusive and allow users to act freely. Wearable systems in particular require their sensing technology to be small, low powered and easily integral with the user's clothing. Considering all the requirements, identification systems that use face recognition and speaker identification seem to us to have the most potential for wide-spread application [1].

Cameras and microphones today are very small, light-weight and have been successfully integrated with wearable systems. Audio and video based recognition systems have the critical advantage that they use the modalities humans use for recognition. Finally, researchers are beginning to demonstrate that unobtrusive audio-and-video based person identification systems can achieve high recognition rates without requiring the user to be in highly controlled environments.

References

[1] T. Choudhury, Future of Face Recognition Technology, 2000.

[2] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, “2D and 3D face recognition: A survey,” *Elsevier Pattern Recognition Letters*, vol. 28, pp. 1885–1906, 2007.

[3] A. M. Bronstein, M. M. Bronstein, and R. Kimmel, “Three-dimensional face recognition,” *International Journal of Computer Vision*, second review – 3, pp. 1-44, 2004.

[4] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*, 2nd Edition, 2011.

[5] K. Delac and M. Grgic, *Face Recognition*, I-Tech Education and Publishing, 2007.

[6] L. Akarun, B. Gokberk, and A.A. Salah, “3D face recognition for biometric applications,” *IEEE 13th Signal Processing Conference European*, pp. 1 – 5, 2005.

[7] P. B. Sharma and M. M. Goyani, “3D face recognition techniques - a review,” *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, issue 1, pp.787-793, 2012.

[8] Dr. P. P. Pittalia and K. H. Solanki, “An invention approach to 3D face recognition using combination of 2D texture data and 3D shape data,” *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 2, issue 11, pp. 1-5, 2013.

[9] T. D. Heseltine, “Face recognition: two-dimensional and three-dimensional techniques,” PhD Thesis, Department of Computer Science, The University of York, 2005.

[10] N. Dahm and Y, Gao, “A novel pose invariant face recognition approach using a 2D-3D searching strategy,” *IEEE 20th International Conference on Pattern Recognition*, pp. 3967-3970, 2010.

[11] http://people.csse.uwa.edu.au/ajmal/papers/eccv06_ajmal.ppd

ISSN: 2454-1532

[12] J. H. Shah, M. Sharif, M. Raza, and A. Azeem, "A survey: linear and nonlinear pca based face recognition techniques," *The International Arab Journal of Information Technology*, vol. 10, no. 6, pp. 536-545 , 2013.

[13] Dr. S. B. Thorat, S. K. Nayak, and J. P. Dandale, "Facial recognition technology: an analysis with scope in India," *International Journal of Computer Science and Information Security(IJCSIS)*, vol. 8, no. 1, pp. 325-330, 2010

[14] K. Bonsor and R. Johnson, How Facial Recognition Systems Work, How Stuff Works.

[15] J. Dowden, Facial Recognition: The most "Natural" Forensic Technology, Evidence Technology Magazine.

[16] K. Bonsor, How Facial Recognition Systems Work, Howstuffworks, 2006.

Gagandeep Jagdev and Mandeep Kaur, "Constraints of 2D face recognition crafts way for 3D face recognition technique", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 41-46, 2015.