IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2016

A Survey on Various Spoofing Attacks and Image Fusion Techniques

Pravallika .P [1], Dr. K. Satya Prasad [2]

Department of ECE, University College of Engineering, JNTUK, Kakinada, India [1]

Professor, Department of ECE, University College of Engineering, JNTUK, Kakinada, India [2]

Abstract: Biometrics systems are used to verify or identify an individual from his physiological and biological characteristics. But now a days, some biometric systems fail to meet the security requirements in some practical cases. Among these threats and vulnerabilities that are facing by the current biometric systems are spoofing attacks. A spoofing attack is that when a person tries to act as someone else by false data and there by gaining illegal access to the biometric systems. Here the user makes use of some artificial gummy finger, iris image printed on paper or masks. The study of anti-spoofing, has been growing in interest in recent years. This paper presents an introduction to spoofing attacks and anti-spoofing measures. Here we also present about image fusion techniques in biometrics. It enhances the security of biometric systems by fusion of multiple biometric traits like iris, face, finger etc.

Keywords: Image fusion; anti-spoofing; biometric system; spoofing attacks

I. INTRODUCTION

The term "biometrics" is taken from the Greek words as bio means “life” and metric means “to measure”. It refers to the verification or the identification of a person. This method uses the physical parameters or the biological parameters as an in identification tool [10]. The biometric technology is now a days using everywhere in colleges offices, bank ATMs, etc., to enhance the security [1] of the legal and the personal information.

The disadvantages in PINs, passwords, tokens are they may be forgotten or shared or stolen. Thus biometric systems of identification are more secured.

Biometrics are often classified as physiological and behavioural characteristics. Physiological characteristics are related to the physical shape of the body. Examples such as DNA, palm print, hand geometry, iris recognition, retina and scent, fingerprint, palm veins, face recognition, Behavioural characteristics are related to the behaviour of the person, including but not limited to typing ,rhythm, gait, and voice.

Biometric technology used in many fields as Government applications such as e-passports, ID cards, and border control. However in the past few years the quality of biometric measurement has become a big issue.
Recently, the interest in the biometric systems security has led to the creation of very diverse initiatives on this major field of research. Biometrics[1] can be fraudulently accessed hence it is necessary to offer security to those systems.

Besides the advantages, biometric systems have some drawbacks, including the lack of secrecy, the fact that a biometric trait cannot be replaced. Our devices are now a day’s storages of personal, professional, commercial, and other kinds of information. Hence it is essential to be kept confidential and secured from fake traits. The attacks where the user submits a replica of the original biometric to the sensor. These attacks are referred to as spoofing attacks. The effect of these attacks lies upon fact that the sensor used is able to detect whether the submitted biometric trait is “fake” or “live”.

Fake biometrics [10] means, the user creates the fake identities like fingerprint, iris on printed paper or uses synthetic or gummy prints for identification. In fake biometrics the user first captures the identities of the real user and then create the fake sample for identification[1].

There are many methods to detect the fake users and hence these biometric systems are more secure, because every person will have different characteristics for identification. A multimodal [9] biometric system uses the multiple source of information for recognition of person.

Multimodal biometric system is more secure than single biometric system. The paper is organized as follows. In Section II, the Spoofing attacks is reviewed .The image fusion and its types is described in Section III. And then followed by Conclusion.

II. SPOOFING ATTACKS

As discussed earlier the biometric systems can be attacked by the frauds by using various imitating traits of the original users. Hence it is necessary to study about these attacks to counter act the situations of spoofing attacks[7]. The possible types of attacks and their images in each specific trait are discussed in this section II

DOI 10.17148/IJARCCE.2016.5860

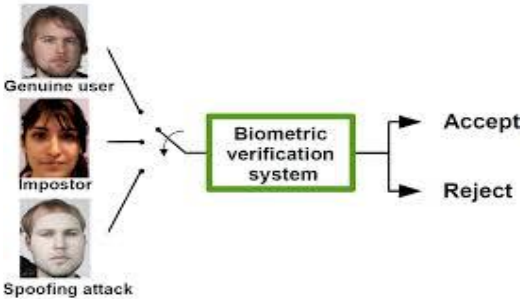


Fig.1. Diagram For Spoofing Attacks

There are different fraudulent access attempts using various synthetic traits and gummy prints and printed iris, face on papers. Basically the types of attacks [7] are classified a
Types of Attacks

- Direct Attacks: This attacks are done with artificial biometric samples, e.g. gummy fingers[7] and printed iris etc., In this type of attacks no exact knowledge regarding the system is wanted. Moreover, the attack is carried out in the analog domain, outside the digital restrictions of the system.
- Indirect Attacks: In this type of attacks the impostor needs to have some extra information about the internal operational of the system and, in some cases, physical access to some of the application mechanism is also needed.

Different levels of attacks against a biometric system are

- Artificial biometric traits may be presented at the sensor.
- Illegal data may be submitted to the system.
- The feature template may be changed by some program.
- Matcher may be changed with that gives high scores.

Basically the biometric systems consists of large database of biometric samples whose performance is quality assessed with a standard protocol of genuine and imposter traits. The performance is measured by the no. of misclassifications, i.e. genuine traits being classified as impostor trait and vice versa.

A. Fingerprint Spoofing

In case of fingerprint spoofing attacks the user uses his intelligence in photography to make a gummy fingerprint from a latent fingerprint. The latent fingerprint is first highlighted by using some forensic methods, and then a photograph was taken. This photograph is then used to take the print onto a copper plate to generate fake fingerprints. Although the fingerprint spoofing[3] is oldest technique used in various cases from past, it is necessary to provide security from these kinds of attacks. Hence the various researches have are under process to counter-act these attacks. A two stage process is generally used to create the spoof finger prints. The first stage is followed by reconstruction of fingerprint images from the real user's minutiae template. This first stage is called as "template to the image". The second stage, is termed as "from the image to the gummy fingerprint", the images were reconstructed to produce fake fingerprint trait. Almost 70% of the fake fingerprints are being accepted by the biometric systems.

Fingerprint spoofing [3] can be classified into two types as "consensual or direct casts" and "non-consensual or indirect casts". In the direct casts method, the fake traits are created with the collaboration of the fingerprints of the real user. In the indirect casts method, the user makes use of fingerprint left on the surfaces, to create the spoofed fingerprints and here the user is not required. In case of direct casts method the steps to be followed are:

a. The user makes use of soft material and keep stress on his finger to get the print of the finger as mold

b. The gelatin, liquid silicon, moldable plastic, wax, clay, such casting material is poured on the mould

c. The fake fingerprint is formed when the liquid gets hardened.

Fig.2. Diagram of Gummy Fingerprint Access

B. Iris Spoofing

The iris is the area of the eye where the colored circle, usually brown or blue, rings the dark pupil of the eye. Iris recognition systems use small, high-quality cameras to capture a black and white high-resolution photograph of the iris. In iris recognition the system use camera to take the input sample and the software compares the result with the stored templates. Iris biometrics will have the unique characteristics and features to verify the identity of an individual. This process takes two seconds and provides the data of the iris that are first mapped, recorded and stored for future verification.

Once the image is captured, the iris' [5] elastic connective tissue called the trabecular meshwork which is analyzed, processed into an optical "fingerprint," and translated into a digital form.

The iris can be differentiated by several characteristics like furrows, ridges, ligaments, crypts, rings, freckles, cornea, and a zigzag collarette. The inner edge of the iris is taken by an iris-scan algorithm which maps the iris' distinct patterns and characteristics. Iris' are composed before the birth and, except in the event of an injury to the eyeball, it remains unchanged throughout an individual's lifetime.

DOI 10.17148/IJARCCE.2016.5860

Iris patterns are extremely complex, carry an astonishing amount of information and have over 200 unique spots. The fact that an individual's right and left eyes are different and that patterns are easy to capture.

As the use of iris recognition in various biometrics systems for large identity applications is increasing. There are also cases of spoofing[9] are equally increasing, hence it is necessary to study about iris spoofing to counteract [5] the attacks . Iris spoofing is a mechanism in which user make use of fake iris to fraudulent access the identity of an individual.

Iris Forgeries

The iris spoofing can be done in major ways one of the spoofing technique in which the user uses the eye printouts on the glossy paper and it is shown in front of the cameras during the operation of identification.

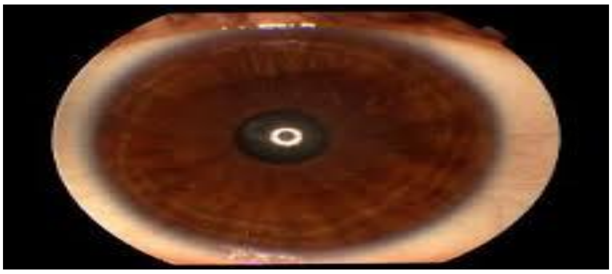


Fig.3. Diagram Of Printed Iris On Glossy Paper

One more type in iris forgery is making use of a prepared "eye movie", which can imitate the behaviour of real eye by using blinks, eyeball movements, pupil dynamics, etc..In such spoofing with the use of eye movie can be easily tested by asking some particular measure of eye behaviour. But the attacker can also able to react instantly hence, further anti-spoofing methods should be recognized. It is shown in Fig.4

Fig.4. Diagram Of Eye movie

Further we can see one more spoofing attack in which the intruder can make use of a artificial eye that is to present before the camera lens. The patterns that are available on the iris are printed on the rubber or some model of eye and in addition makes use of pupil diameters and iris tubercular meshwork during the preparation of eye model. It is shown in fig.5.

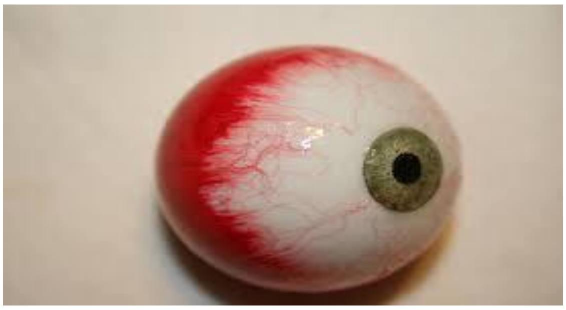


Fig.5. Diagram Of Artificial Eye Model

The one more possible spoofing attack is the usage of artificial contact lens in which the user can have the iris pattern printed on the lens as shown in Fig 6.

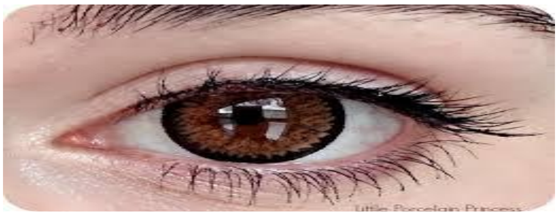


Fig.6. Diagram Of Iris Patterns On Lens

C. Face Spoofing

There are various biometric traits one of the traits is face recognition. It is used in various fields for identification of the person.In spite of increasing use of face recognition systems, there are face spoofing[4] attacks are also being under usage. Face spoofing techniques can be changed based on the current face recognition system. Any face recognition systems can be classified into two classes: two dimensional and three-dimensional systems. The spoofing attacks[7] in face recognition systems can be done by using photograph prints, mask of the user and by the video of the user. Spoofing with the help of photographs and videos are the easiest methods. The spoofing attacks with the use of photographs are called as "photo attacks", in which the user submitts a photograph of a genuine user before the lens of the recognition system by hard copy. Face spoofing[8] is very easy method because any one can capture the photographs of anyone without intimating them. And also with the help of social networking websites any photographs can be downloaded and they can be used for spoofing in photo attacks. It is shown in fig.7

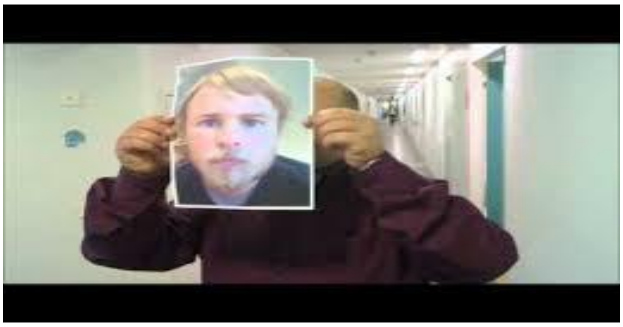


Fig.7 Spoof with Photograph Printout

DOI 10.17148/IJARCCE.2016.5860

In case of other attacks with videos, the success rate of spoofing with the persons video is more because in the video attacks the appearance of the person like head movement, and expressions are more live while displaying it in front of the camera lens. It may be difficult to capture a fake eye blinks in a fake face image but rather than that all the remaining features can be cheated easily with video attacks. It is shown in fig.8

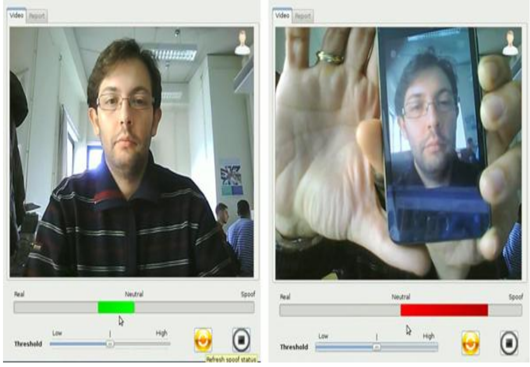


Fig.8. Video attack spoof

Due to the wide usage of the 2D recognition systems, it is very easy and simple to spoof the systems with video and photo attacks. In case of the 3D recognition systems it may be difficult to spoof but still it may be possible with the 3D face masks by using silicon gels, rubber etc. It is shown in fig 9

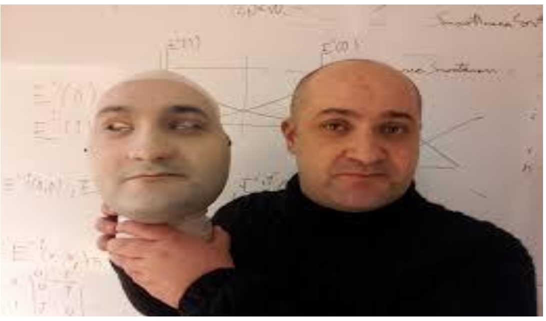


Fig.9 3D Face Mask spoof

One more spoofing attack can be described where the user makes use of a 2D photo [10] of the client and it is attached to the user shirt and stand before the system. This process may be simple yet it does not give any higher success rates because the user should try mimicking the 3D shapes of the face.It is shown in Fig. 10

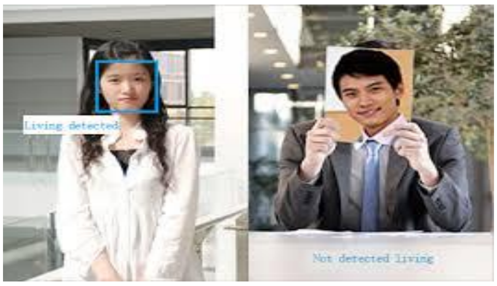


Fig.10 Live and Spoof Detections

The studies on liveness detection [10] techniques have been widely increased to handle the spoofing attacks. In case of detection of face liveness the system verify whether the input face image presented before the recognition system is real or not. Due to cost aspects the common type of spoof techniques are photo and video attacks.

Anti-spoofing[4] techniques for these type of attacks can be classified as three groups: liveness detection, texture analysis and motion analysis In the first type of detection , the system detects the liveness of the input face image by measuring some parameters like head movements, lip movements and eye movements.

In case with the second type of detection which is motion analysis , here the examination of the motion in the scene and movements of objects like screens , printed papers are examined by using trajectories of the face regions because they will be difference with the real and fake.With the third type of detection methods, face image texture is examined to detect the clues like blur etc.

III.IMAGE FUSION

Multisensory image fusion is the process of combining relevant information from two or more images into a single image. The resulting image will be more informative than any of the input images. Several situations in image processing require both high spatial and high spectral information in a single image. However, the instruments are not capable of providing such information either by design or because of observational constraints. One possible solution for this is data fusion.

The fusion[11] can be classified into two classes, as fusion before matching and fusion after matching shown. For fusion before matching, the information is integrated from multi biometric sources and fusion is done at the sensor level and fusion at the feature level. Whereas , fusion after matching is divided into fusion at the match score level and fusion at the decision level.

Fusion Before Matching

- Sensor Level Fusion: In this fusion level , the raw data from the sensor images are combined together. The source of information is contaminated by noise and background clutter .This level of fusion can be done in two cases as data of the same biometric trait is obtained using multiple sensors; or data from multiple snapshot of the same biometric traits using a single sensor.

- Feature level fusion : In this feature level fusion, different feature vectors extracted from multiple biometric sources are combined together into a single feature vector. Hence, only few researchers have focused on the feature level scheme compared to the other levels of fusions such as score level and decision level

Fusion After Matching

- Score level fusion : In this score level fusion, the matched outputs from multiple biometrics are combined together to improve the matching performance in order to verify or identify of an individual. This is the popular approach in the biometrics due to its simplicity in score collection.
- Decision level fusion: This fusion is similar to score-level fusion, except that the scores are replaced with match/non-match decisions.

The simple image fusion techniques like averaging method, select maximum, select minimum will not give the good fused image. The method like DWT & PCA gives the better fused image than averaging method, select maximum, select minimum. The various categories of image fusion are as follows

A. Multi modal Images

The multi modal images are the images of different modalities as infrared, visible and panchromatic images. It also includes the images with different cameras. The fusion of such modality images is called as multimodal image fusion[6]. The example of multi modal image is shown in Fig.11

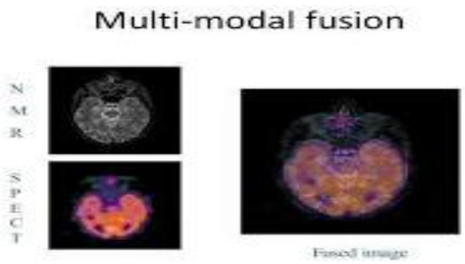
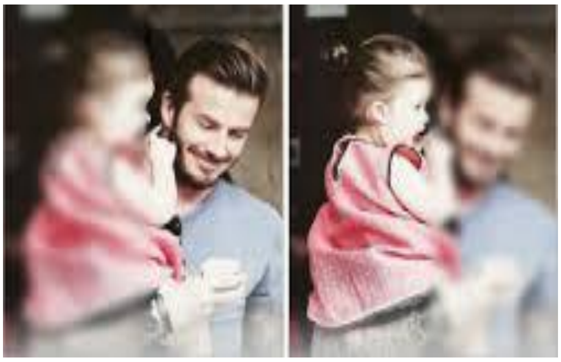


Fig.11. Multimodal Image Fusion

B. Multi focus Images

The multi focus images are the images taken from the digital camera and the resulting images are if focused on any part or object and being not focussed on entire picture correctly. The image fusion [13] with such kind of images are called as multi focus images. The fusion of all such images which are focused at different portions of image are called as multi focus image fusion. The example of such fusion image is shown in Fig.12



. Fig.12. Multi Focus Images

C. Multi view Images

The images which are taken in the different angles and view points are considered as multi view images. The fusion of such images are called as Multi view image fusion. The example of multi view image fusion [12] is shown in Fig.13

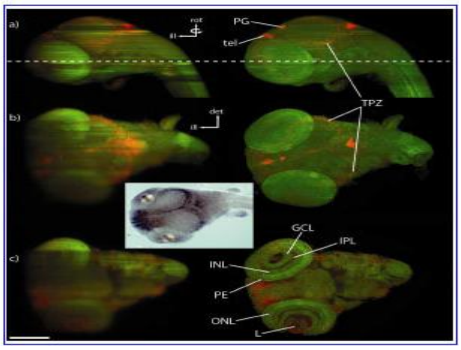


Fig.13 Multi View Image Fusion

D. Multi-Temporal Images

The images that are taken in different time scales are taken as multi temporal images. The fusion of such images are helpful in obtaining the modifications with respect to time

IMAGE FUSION ALGORITHMS

The Image fusion algorithms are useful in obtaining the image with each and every part or object in focus and gives the more detailed result for human or machine. Pixel-based, region-based and wavelet based fusion are the possible fusion algorithms [11].

A. Simple Average

This algorithm is so simple it gives the resulting image with all objects with high intensity focused. As we know that focused part will have higher intensities, so the simple average gives the image in highly focused high intensity range. The operation is that the pixel values of two images are added and divided by 2 then the average value is assigned to the corresponding pixel of the output image. This is again repeated for all the pixel values.

$$K\ (i, j) = \{X\ (i, j) + Y\ (i, j)\}/2$$

Where X (i , j) and Y (i, j) are two input images.

B. Select Maximum

As more focused part of the image is due to the higher pixel values. The resulting image of the maximum fusion technique is the highly focused output as this algorithm takes the value of the higher pixel P (i, j) value from the two images by comparision. The greatest pixel value is given to the corresponding pixel of the fusion image.

$$F(i,j) = \sum_{i=0}^{m} \sum_{j=0}^{m} max(A[i,j], B[i,j])$$

DOI 10.17148/IJARCCE.2016.5860

C. Select Minimum
This algorithm is similar to that of select maximum but it takes the the value of the lower pixel P (i, j) value from the two images by comparision.
The greatest pixel value is given to the corresponding pixel of the fusion image.

$$F(i,j) = \sum_{i=0}^{m}\sum_{j=0}^{m} min(A[i,j],B[i,j])$$

Where A, B are the Image Matrices

D. Principal Component Analysis
The PCA is one of the fusion algorithm in which it takes the multidimensional data sets into the lower dimensions for the ease of analysis.

This method gives the weights for every source image we take by making use of the eigen vector from the covariance matrix which being the higher eigen vector.

PCA algorithm steps are given as follows:

a. Firstly it produces the column vectors from the input images

b. Then it computes the covariance matrices of the two column vectors that are formed in step a.

c. Now, compute the eigen vectors and eigen values of the covariance matrices.

d. Normalize the column vector

e. The normalized eigen vectors will act as the weight values which, they will get multiplied with each and every pixel of the input image.

f. Finally the fused image is the fusion of the two scaled matrices

E. Discrete Wavelet Transform
The property in Discrete Wavelet Transforms [14] is that the spatial resolution in low-frequency bands is small but in high-frequency bands it is large. Because the mother wavelet is treated as high pass filter and the scaling function is treated as a low pass filter in the DWT implementation.

The DWT decomposes every image into four sub bands as low-low, low-high, high-low, high-high spatial frequency bands which are at different scales. The low-low image will have the small spatial resolution and it gives the approximate information to that of the original image. We can have the different possible levels of decomposition as shown in Fig 14.

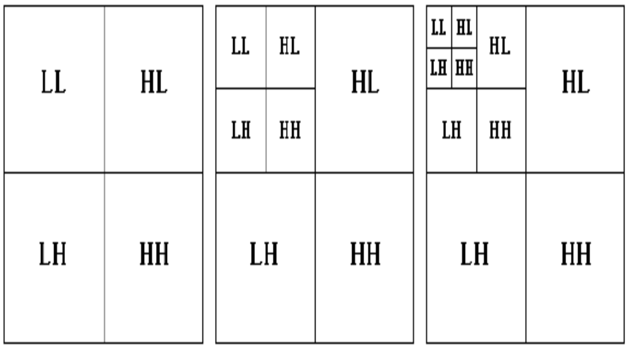


Fig.14 DWT Decompositions

After the level of decomposition in one level, we will have the four frequency bands. The next level of decomposition is now applied to the LL band of the one level decomposition stage. Thus we can have the N-level of decompositions possible.

The DWT technique is used for the following list of reasons as:

(a) It is one approach which is well suitable and useful in various image processing applications as image fusion etc.
(b) The discrete wavelet transform (DWT) can be used as segmentation technique in which the image can be decomposed into different coefficients while preserving the original image information. The coefficients from the different images are combined to create new coefficients so that we can have the information of the original images.
(c) The inverse discrete wavelets transform (IDWT), is applied to get the final fused image after all the coefficients are merged.

VI. CONCLUSION

The biometrics is now evolving technology which has been in the usage under various fields. As it is necessary to provide security to the biometric recognition systems from various possible spoofing attacks , we should study about the spoofing attacks and develop various counter-act measures. The image fusion is one of the possible counter measure which may reduce the rate of spoofing to the particular extent.

REFERENCES

[1] A. Jain, A. Ross, and S. Pankati, "Biometrics: A tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, June 2006.
[2] S. Marcel, M. Nixon, and S. Z. Li, Handbook of Biometric Anti-Spoofing. Springer, 2014.
[3] E. Marasco and A. Ross, "A survey on anti spoofing schemes for fingerprint recognition systems," ACM Comput. Surv.,vol. 47, no. 2, pp. 28:1–28:36, Nov. 2014.
[4] J. Galbally, S. Marcel, and J. Fierrez, "Biometric anti-spoofing methods: A survey in face recognition," IEEE Access, vol. 2, pp. 1–23, December 2014.

[5] X. He, Y. Lu, and P. Shi. A fake iris detection method based on fft and quality assessment. In Chinese Conf. on Pattern Recognition, pp. 316–319, 2008.

[6] J. Fierrez, "Adapted fusion schemes for multimodal biometric authentication," Ph.D. dissertation, Universidad Politecnica de Madrid, May 2006.

[7] I. Chingovska, A. Anjos, and S. Marcel, "Biometrics evaluation under spoofing attacks," IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2264–2276, December 2014.

[8] S. Z. Li and A. K. Jain, Eds., Handbook of Face Recognition. New York: Springer, 2nd edition, 2011.

[9] R. N. Rodrigues, N. Kamat, and V. Govindaraju. Evaluation of biometric spoofing in a multimodal system. In Int'l Conf. Biometrics: Theory Applications and Systems (BTAS), pp. 1–5, 2010.

[10] Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierre "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint,and Face Recognition" IEEE transactions on image processing, vol. 23, no. 2, february 2014

[11] Deepak Kumar Sahu, M.P Parsai ,"Different Image Fusion Techniques-A Critical Review ",International Journal Of Modern Engineering Research(IJMER),Vol 2 ,Issue.5,sep-oct 2012

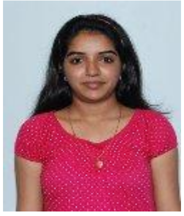
[12] S.JohnNisha, Anita,C.John Moses,"SURVEY ON PIXEL LEVEL IMAGE FUSION TECHNIQUES",2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)

[13] Dong-Chen He, Li Wang+ and Massalabi Amani, "A new technique for multi-resolution image fusion",IEEE 2004

[14] VadherJagruti,"Implementation of discrete wavelet transform based image fusion",IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 2, Ver. VIII (Mar - Apr. 2014), PP 107-109.

BIOGRAPHIES

Dr. K. Satya Prasad, awarded with 16 Ph.D scholars currently working as Professor of ECE Department in JNTUK with 36 years of teaching experience and 30 years of R&D experience. His Area of interests include signals & systems, Digital signal processing, Radar Telemetry and communications



Pravallika. P, received a B.Tech Degree under the stream of ECE from Kakinada Institute Of Engineering and Technology For Women. Currently pursuing M.Tech In JNTU Kakinada under the department Of Electronics and Communication Engineering.

DOI 10.17148/IJARCCE.2016.5860