International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 151-158 March 2018 - Sept 2018 www.csjournals.com

# Fake Face Recognition using Thermal Imaging

**Navpreet Kaur**
Assistant Professor, Department of Computer Science, Govt.College for women, Bhodia Khera

**Abstract:** Spoofing with photograph or video is one of the most common manners to attack a face recognition system. In this paper, we present a non intrusive and real time method to address this problem, based on fusion of thermal imaging and skin elasticity of human face. In this technique, face images is captured using camera sensor and thermal sensor at the same time. Before capturing the images, user is asked to do some movement like chewing and forehead movement simultaneously, so that a full movement to face skin can be given and then sequence of face images is captured with a gap of few milliseconds. Then one of the image from image sequence is compared with the thermal image after thinning and noise removal. Then after applying correlation coefficient between images and then discriminate analysis using some method, face skin is discriminate from the other materials like gelatin, rubber, cadaver, clay etc. In comparison to other face liveness detection, this method will be much user friendly. On the other hand, one of the images captured for liveness detection can be used for face recognition.
**Keywords:** Biometrics, Face recognition, Fake Face Detection, Liveness Detection, Skin Elasticity, thermal infrared imaging.

## 1. Introduction:

Face recognition is a process of identifying and verifying a person by recognizing his face. Face recognition has become an important issue in many applications such as security systems, credit card verification, criminal identification etc [1]. Due to recent pattern recognition advances applied to face recognition, biometric systems based on facial characteristics have been largely applied to problems, including access control, surveillance and criminal identification[2].

One of the negative implications of increased technological advancement is the ease with which, one can spoof into a biometric identification system. Face or iris recognition systems can be spoofed by static facial or iris images. Several spoofing techniques have been developed to deceive the biometric systems, and the security of such systems against attacks is still an open problem. Spoofing attacks occur when a person tries to masquerade as someone else falsifying the biometrics data that are captured by the acquisition sensor in an attempt to circumvent a biometric system. Therefore, there is an increasing need to detect such attempts of attacks to biometric systems.

Since the acquisition sensor is the most vulnerable part (any user has easy access to this part of the system), spoofing attack techniques have become more attractive for impostor users. Moreover, unlike the authentication systems based on passwords and smart cards, some of our biometric data such as faces are widely available in social networks, personal web sites, and can be easily sampled directly with a digital camera.

In the context of face biometrics, an impostor tries to access the system as a valid user with three approaches [3] : (1) showing photography of a valid user; (2) showing a video of a valid user, or (3) showing a 3D facial model of a valid user. If any of these approaches succeeds, the uniqueness characteristic of the biometric system will be violated and the system will become fragile [1].To improve security for the biometric systems, liveness detection (or vitality

detection) is proposed to defeat this kind of spoof attacks. Liveness detection is an anti-spoofing method ensuring that only the biometric from a live, authorized person is submitted for enrollment, verification and identification.

## 2. Liveness Detection In Face Recognition

In a biometric system there are three ways for introducing liveness detection:

1. Using extra hardware: This approach is an expensive approach. In this approach extra hardware is used to acquire the life signs.
2. Using software: In this approach some software is used to classify the fake and real images. It is done at processing stage.
3. Using combination of hardware and software: in this approach a combination of hardware and software is used to classify the fake and real images.

In these approaches first approach is an expensive but fast approach. Second approach is relatively less costly but takes much time in comparison to first. Last approach is a combination of these two so it is expensive as well as time consuming. But it provide a good high end solution for livens detection which is difficult to breech.

Some examples of the fake face image is shown in the figure 1. In this example, faces made of material like silica gel, rubber, photo and video replay are shown [4]. In general, fake faces have two main properties:

1. Large variations. Although the positive class, namely the genuine face, has limited variation (all genuine faces are human skins), the negative class, i.e., the fake faces, can range from photos, videos to masks and so on. When it comes to material level, the variety is even larger: take face mask for example- there are rubber mask, plastic mask, silica gel mask, etc. It's almost impossible to give a complete list. Some examples of fake faces are shown in Fig.2.

2. Indistinguishable under visible light. Fake is, by its definition, indistinguishable for human eyes. Therefore, without extra aid, only visual face images are insufficient and impossible for the detection of fake faces.

Fig 1: Some Fake face examples. Materials from left column to right are: silica gel, rubber, photo and video replay

Two of the most important challenges nowadays refer to: (1) the need of designing and deploying non-intrusive methods without extra devices and human involvement; and (2) designing detection methods robust to changes in pose and illumination.

## 3. Related work

In this section, we review the literature on non-intrusive methods without extra devices and human interaction, since such methods are preferable in practice because they are easily integrated to existing face recognition systems.

Regarding the data-driven characterization, some methods are based on the analysis of skin properties such as texture and reflectance. Li et al. [5] proposed an anti-spoofing solution to photo attacks under the assumption that the size of photos is smaller than a live face and the expressions and poses of the face contained in photos are invariant. These characteristics are detected by analyzing the 2D Fourier spectrum, because photos certainly contain fewer high frequency components, and a threshold is used to detect a spoofing attack. Although the reported results have been satisfactory, in practice these assumptions do not hold. Movements are easy to simulate rotating or bending the photos. Furthermore, the method will probably fail for photos with high quality.

In [6], Tan et al. proposed a solution based on the Lambertian reflectance properties to distinguish between valid and fake users under the assumption that the surface roughness of both classes is different. The authors use two methods for extracting latent reflectance features: variational retinex based and difference-of-Gaussian (DoG). The authors reported promising results on a publicly available database (NUAA Database) composed of true accesses and attacks of 15 subjects using both photo-quality and laser-quality prints.

Bruno et. al. presented a solution that works with both printed and LCD displayed photographs, even under bad illumination conditions without extra-devices or user involvement [7]. They conducted no of tests on large databases that show good improvements of classification accuracy as well as true positive and false positive rates. G. kim et al has given a single image-based face liveness detection method for discriminating 2-D paper masks from the live faces [8]. In this still images taken from live faces and 2-D paper masks were found to bear the differences in terms of shape and detail. In order to effectively employ such differences, they exploit frequency and texture information by using power spectrum and Local Binary Pattern (LBP), respectively.

In a recent work, Peixoto et al. [10] extended the technique proposed in [6] to an image-based spoofing detection based on the fact that the brightness of the LCD screen affects the recaptured image, which makes the image edges more susceptible to a blurring effect. To capture this information, the authors propose an intermediate step before extracting latent reflectance features that consists in applying adaptive histogram equalization to the images. The reported results on the publicly available NUAA Database and Yale Face Database show that the proposed extension reduced the classification error in more than 50% for high-quality printing spoofs in the NUAA database and 65% for images recaptured from an LCD monitor for the Yale Face Database. In another work Aruni et al. has provide a method of detecting a tempered face image detection based on second order gradient technique[11].

Optical flow analysis has also been considered in the literature. Bao et al. [12] obtained a reference field from the actual flow field data on fake and valid images to estimate their differences. Kollreider et al. [13] presented a method based on the optical flow algorithm for

capturing and tracking subtle movements of different facial parts, assuming that facial parts on real faces move differently than on photos.

In order to incorporate temporal information from videos captured from an image, Schwartz et al. [14] presented a holistic method for describing faces combining several feature descriptors. Considering only the facial region, the authors extract several features using descriptors that capture different characteristics of the images, such as shape, color and texture. They reported improved results, but the combination of these descriptors generated high dimension feature spaces that may not be suitable for standard classification methods.

Considering behavior modeling, some works have focused on eye blinking [15], [16] and small movements of parts of the head and face [17] to detect specifically photo-based spoofing. Considering that a person blinks approximately once every two to four seconds, Pan et al. [15] proposed the use of an undirected conditional random field framework to represent eye blinking from hidden Markov models that relax the independence assumption of generative modeling, with the advantage that the method allows to relax the assumption of conditional independence of the observed data.

## 4. Fusion of Skin Elasticity and Thermal Imaging

**4.1 Visible Face Recognition:** Face recognition algorithms can be classified into two broad approaches according to feature extraction schemes for face representation: feature-based and appearance-based methods. Feature-based face recognition techniques compute a set of geometrical features on the face such as the eyes, the nose, and the mouth. A number of early face recognition algorithms are based on feature-based methods. Properties and geometric relations such as the areas, distances, and angles between the feature points are often used as descriptors for face recognition. The performance of feature-based face recognition methods depends on the accuracy of the feature locating algorithms used.

Appearance-based methods find the global properties of the face pattern. Many face recognition algorithms in this category project an image into a subspace with linear transforms and find the similarity of reference images to an input image. Several leading commercial face recognition products use the face representation methods based on the Karhunen-Loeve expansion, such as the eigenface and the local feature analysis (LFA)[18]. The LFA represents face images in terms of locally correlated features derived statistically from a representative ensemble of faces. Local representations offer robustness against variability due to the changes in localized regions of the objects. A selection (or sparsification) step produces a minimally correlated and topographically indexed subset of features that define the subspace of interest. The features used in the LFA methods are less sensitive to illumination changes, easier for estimating the rotations, and have less computational burden than the eigen face method. Skin elasticity is a visible face detection method. In this method a no of face images are captured at a specified gap interval as shown in figure 2 and they are compare with each other to detect wheither the image captured are real image or fake images.

**4.2 Thermal Face Recognition:** Advantages of thermal IR imaging in face recognition include the invariance to illumination changes. Face recognition using the visible spectrum may not work properly in low lighting conditions. The use of the thermal IR spectrum for face recognition reported improvements in the recognition accuracies under a wide variety of illumination

conditions [19,20]. Thermal IR imagery is less sensitive to the variations in face appearance caused by illumination changes due to the fact that thermal IR sensor measures the heat energy radiation, not the reflectance, from the object. While the visible spectrum provides features that depend only on surface reflectance, thermal IR images produce features that uncover thermal characteristics of the face. Thermal face recognition utilizes such anatomical information of the human face as features unique to each individual that can be measured at a distance using passive IR sensors. Similar recognition techniques proposed for visible face recognition have been applied in thermal face recognition as well. Appearance-based face recognition algorithms applied to thermal IR imaging consistently performed better than when applied to visible imagery. Initial research approaches to thermal face recognition extracts and matches thermal contours for identification using techniques that include elemental shape matching and eigen face methods. Automated face recognition using elemental shapes in real time has reported 96% accuracy for cooperative access control applications [21]. Anon-cooperative, nonreal- time faces-in-the-crowd version of thermal face recognition reported 98% accuracy with no false positives for more than 100 people represented in a database of 500 images.

### 4.3 Proposed Work

Fusion techniques exploit synergistic integration of the information obtained from different data sources or from multiple pattern classifiers to improve the overall classification accuracy [22]. Data fusion combines the data from multiple sources to produce a more informative form than the original. The registration is intrinsic when the various wavelength bands come from the same sensor, but is more complicated when several different sensors are involved. Numerous attempts have been made in face recognition based on the fusion of different types of data. Face recognition algorithms based on the fusion of visible and thermal IR images demonstrated higher performance than individual image types. In this propose work we combine skin elasticity and thermal imaging techniques to detect liveness detection. Skin elasticity is a normal visible face recognition while thermal imaging is a thermal technique to detect the liveness in a capture image using heat property of the image.

In this technique thermal camera is fitted at predetermine distance from the visible camera. Images are captured at the same time from both the camera by specified instruction. For skin elasticity process a set of image sequence is captured with a gap of few milliseconds. Then one image of these set of images and image captured from thermal camera are matched with a few pre processing methods and result is calculated base on this matching and determine wheither the images are from real person or fake images or fake faces.

### A. Proposed Algorithmic Approach:

Step 1. Request the user to perform live activities like chewing, smile, forehead movement etc.

Step 2. Now at the same time capture a sequence of face images with a gap of few milliseconds and a thermal image using low IR thermal imaging camera.

Step 3. Now select one of the image from the set of image sequence to compare with thermal image in such a way it is captured at the same time.

Step 3. Now perform grey scale method on both selected images.

Step 4. Now convert both resulted images into binary image using binary scaling method.

Step 5. According to distance of thermal camera from the visible image camera perform angular deviation on thermal image after thinning on both images.

Step 6. Now superimpose matching on both images and calculate the matching percentage.

Step 6. If calculated value is greater than the threshold value then the image captured are real time images. And if parallelly, skin elasticity test on the set of image sequence is passed then image captured are from real person without any fake face.

Step 7. If at any one stage the process fails then complete process fails and resulted into fake image analysis.

## B. Flowchart of Proposed Approach

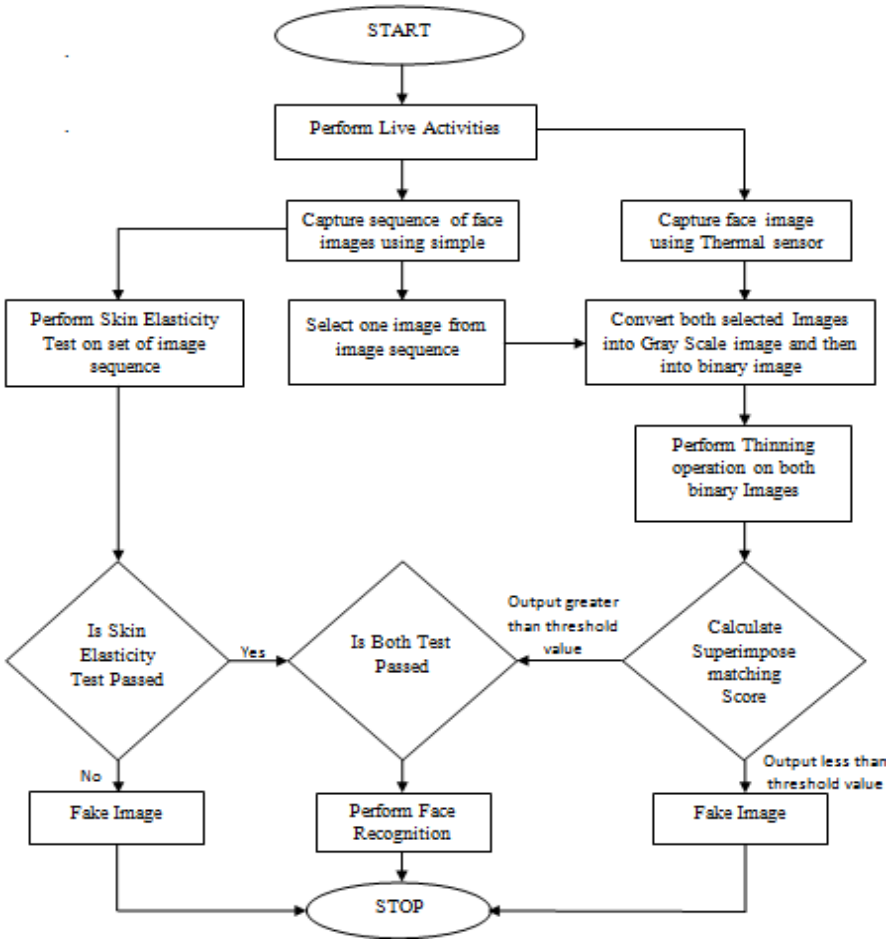


Figure 2 Flowchart of Proposed Approach

**Advantages**: Advantages of fusion of these two liveness detection techniques are following:

1. Thermal imaging is capable of identifying fake face and images captured from photo or video
2. Skin elasticity is capable of distinguishing fake faces that uses gelatin, rubber, clay etc. material.
3. Using both these techniques we will be capable of identifying real face from fake faces.
4. Other Advantages of this approach is that it is user friendly approach.
5. Since it involve thermal imaging camera (Hardware) technique and skin elasticity technique (software based method), so we need not to rebuild the face database.
6. One image of the set of image sequence can be used for face recognition.

## 5. Conclusion and Future Work :

Spoofing concerns with the security of the biometric system. Liveness detection can detect invalid user by identifying the liveness of the user. By using liveness test, we can make it more secure against unauthorized access. Liveness detection technique should be of such type that security can be added to biometric system with minimum cost of hardware and adaptable to old database without requirement of reconstructing it. In this paper we have discussed face liveness detection, in which spoofing can be controlled in a smart way. In this paper, a novel approach of fusion of two liveness detection techniques are shown. One is based on skin elasticity and other is thermal imaging technique. In these techniques thermal imaging technique is capable of distinguishing image of real face from images that are captured from video or photos. While skin elasticity method is capable of distinguishing the real image from images that are using fake faces made of gelatin, clay, rubber etc. materials. In future these this technique can be experimented at practical level on set of large database.

## References:

1. Mayank Agarwal, Nikunj Jain, Mr. Manish Kumar and Himanshu Agrawal Face Recognition Using Eigen Faces and Artificial Neural Network, IJCTE Vol. 2,No 4, pp. 1793-8201, Aug-2010
2. A. Jain and B. Klare, "Matching Forensic Sketches and Mug Shots to Apprehend Criminals," Computer, vol. 44, no. 5, pp. 94–96, 2011.
3. A. K. Jain and A. Ross, Handbook of Biometrics. Springer, 2008, ch. Introduction to Biometrics, pp. 1–22.
4. Zhiwei Zhang, Dong Yi, Zhen Lei, Stan Z. Li, Face Liveness Detection by Learning Multispectral Reflectance Distributions Automatic Face & Gesture Recognition and Workshops (FG 2011), 2011 IEEE, pp 436-441, March 2011.
5. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live Face Detection Based on the Analysis of Fourier Spectra," in Biometric Technology for Human Identification, 2004, pp. 296–303.
6. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," in European Conference on Computer Vision, 2010, pp. 504–517.
7. Bruno Peixoto, Carolina Michelassi, and Anderson Rocha, Face Liveness Detection Under Bad Illumination Conditions, Image Processing (ICIP), 2011 18th IEEE Conference, pp 3557-3560, Sep-2011.

8. Gahyun Kim, Sungmin Eum, Jae Kyu Suhr, Dong Lk Kim, Kang Ryoung Park, Jaihie Kim,Face liveness detection based on texture and frequency analyses, Biometrics (ICB),2012 5th IAPR, pp 67-72, April 2012
9. Jukka Matta et al uses the micro texture analysis of Face Image for spoofing detection [9].
10. Peixoto, C. Michelassi, and A. Rocha, "Face Liveness Detection under Bad Illumination Conditions," in IEEE Intl. Conference on Image Processing, Sep. 2011, pp. 3557–3560.
11. Aruni Singh, Shrikant Tiwari and Sanjay Kumar Singh, Face Tampering Detection from Single Face Image using Gradient Method, International Journal of Security and Its Applications Vol. 7, No. 1,pp. 17-30, January, 2013
12. W. Bao, H. Li, N. Li, and W. Jiang, "A Liveness Detection Method for Face Recognition Based on Optical Flow Field," in IEEE Intl. Conference on Image Analysis and Signal Processing, 2009, pp. 233– 236.
13. K. Kollreider, H. Fronthaler, and J. Bigun, "Non-Intrusive Liveness Detection by Face Images," Elsevier Image and Vision Computing, pp. 233–244, Feb. 2009
14. W. R. Schwartz, A. Rocha, and H. Pedrini, "Face Spoofing Detection through Partial Least Squares and Low-Level Descriptors," in Intl. Joint Conference on Biometrics, Oct. 2011, pp. 1–8.
15. G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," in IEEE Intl. Conference on Computer Vision, 2007, pp. 1–8.
16. J.-W. Li, "Eye Blink Detection Based on Multiple Gabor Response Waves," in IEEE Intl. Conference on Machine Learning and Cybernetics, 2008, pp. 2852–2856.
17. G. Pan, Z. Wu, and L. Sun, Recent Advances in Face Recognition. InTech, 2008, ch. Liveness Detection for Face Recognition, pp. 235–252.
18. Penev, P.S. 1998. Local feature analysis: A statistical theory for information representation and transmission. Ph.D. Thesis, The Rockefeller University.
19. Wolff, L.B., Socolinsky, D.A., and Eveland, C.K. 2001. Quantitative measurement of illumination invariance for face recognition using thermal infrared imagery. In Proc. IEEE Workshop on Computer Vision Beyond the Visible Spectrum.
20. Socolinsky, D.A., Selinger, A., and Neuheisel, J.D. 2003. Face recognition with visible and thermal infrared imagery. Computer Vision and Image Understanding, 91(1–2):72–114.
21. Prokoski, F. 2000. History, current status, and future of infrared identification. In Proc. IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications, pp. 5–14.
22. Hall, D.L. and Llinas, J., *Handbook of Multisensor Data Fusion*. CRC Press, 2001.