Detection of Fake Biometrics: Assessment of Image Quality in Face, Fingerprint

J. Madhavi¹, Giri Babu K²

¹Assistant Professor, TKR College of Engineering And Technology
²Assistant Professor, CVR College Of Engineering And Technology

Abstract:
Biometric authentication is difficult because it is difficult to distinguish between a genuine trait and a fake, self-made synthetic, or reconstructed sample. This calls for new, more effective protection measures. This paper describes a software-based fake detection method that can be used in multiple biometric systems to detect fraudulent access attempts. This system adds liveness assessment to biometric recognition systems in an easy-to-use, non-invasive way. It is intended to increase security. This method is easy to use and can be used in real-time. It works by combining 25 image quality features (i.e. it uses 25 general image quality features from one image (i.e., the same image used for authentication) to differentiate legitimate samples from counterfeit ones. The proposed method is superior to other state-of-the-art methods, according to experiments that used publicly available data for fingerprint, iris, and 2D faces. The analysis of biometric samples' general quality revealed valuable information that can be used to identify genuine traits from fake ones.

Keywords: Image quality assessment, biometrics, security, attacks, countermeasures.

INTRODUCTION:
Biometrics refers to the science and technology that measures and analyzes human body characteristics, such as fingerprints. Eye retinas and iris patterns, voice patterns, facial patterns, hand measurements, and voice patterns. It is used primarily for authentication. Many initiatives have been developed to ensure the security of the biometric systems. These initiatives reflect the importance of all parties involved in developing security systems to allow the rapid development of technology into practical use. This will allow them to fraudulently access the biometric system. Digital protection mechanisms that are used are ineffective as attacks are done in analog domains and interactions with the device are done using regular protocol.

For image processing applications like recognition, retrieval and classification, compression, restoration, and other similar fields, it is important to measure the quality of images. Images can be affected by different distortions. It is important to accurately rate the quality of the image. The traditional subjective rating method used to assess the image's quality was based on the time requirements. Experts are needed to evaluate image quality. This can be costly and time-consuming. Many image quality assessment algorithms exist today to determine the quality.
The image may not look the same as the original when it is displayed to the user. This happens because it has gone through multiple processes. There are many possible sources of distortion, including motion blurring, Gaussian Noise, sensor inadequacy and compression. It is also possible that the image has been subject to error during transmission. Images before they are stored or transmitted. A variety of methods have been developed to assess the quality of videos and images.

**LITERATURE SURVEY**

Paper Javier (Galbally Z.Wei 2014) introduced a new software-based multibiometric and multi attack protection method that aims to overcome some limitations. It cannot operate under diverse biometric systems or for different spoofing scenarios. The paper by Poonam Dabas Z.Wei (2013) introduced objective methods to measure the quality of images. The paper presented a method that focused on quality measures and an algorithm for modeling HVS (Human Visual System). The properties of HVS include perceived brightness and frequency response. HVS is used for processing input images.

This paper's Approach [9] is based upon the fact that digital media hide information by altering signal properties to introduce some degradation. This paper shows how adding a message or watermark to a digital media file can create unique artifacts that are detectable using Image Quality Measures. This paper shows that image quality assessments can be used to distinguish between stego-images and cover images.

**IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION**

Image quality refers to the image's perceived image degradation. Imaging systems can introduce distortions or artifacts into the signal. This makes quality assessment a critical problem. Image quality can be measured in two ways. The subjective image quality assessment uses the mean opinion score (MOS). While algorithms evaluate quality, they are based on subjective evaluations. This is how an image is perceived by viewers. This is why the human visual system has a high degree of adaptation. The measurement of structural distortion must be accurate to approximate the perception of image distortion. This will make them more useful in real-world situations. Image quality can be measured in two ways.

The subjective image quality assessment uses the mean opinion score (MOS), which is a human-based method of evaluating quality. Algorithms are used to objectively evaluate quality. The diagram for IQA can be found. The measurement of structural distortion must be accurate to approximate the perception of image distortion in real-world situations.
IMAGE QUALITY ASSESSMENT TECHNIQUES

1. Subjective Methods
Images are presented to several observers for subjective quality assessment. Each image is displayed to an observer who is asked to rate the image on a scale of 1-5. The subjective quality test takes into consideration three factors: illumination, viewing distance from the observer to display, and display properties.

2. Objective Methods
An objective method uses two images to determine the image quality. It is a quantitative approach that takes into account the intensity of two images, reference and distorted types. An objective method can be divided into three types: full-reference (reduced-reference), and no-reference (no-reference) based on the availability of a reference image. This allows us to calculate a number that indicates the image quality.

Reduced Reference (RR) models: This method does not use the original reference image center side by side. Some features from the original reference images are however extracted and used by the quality assessment system. This allows the assessment system to quantify the image's quality and help it evaluate its quality.

PROPOSED METHOD
The proposed system aims to improve the security of biometric recognition systems by adding liveness assessment quickly, easily, and without any intrusion, using image quality assessment.

Fig.2. Liveness detection

Fig.3. Architecture diagram for real-time recognition from a web camera
Face Recognition
This step allows us to determine who a person is based on a single facial image. We have used the Fisher algorithm to recognize faces. To recognize faces, the OpenCV function was used in the proposed system. OpenCV has many FaceRecognizer algorithms. We used the Fisher algorithm to recognize faces in our system. To verify the accuracy of the prediction or to determine if it is a mistake, face verification can be performed. Facial verification can be achieved by reconstructing facial images, then calculating the similarities between the reconstructed and input images. To perform these steps, we use OpenCV functions. We have thus used the Fisher faces algorithm. It requires a higher threshold, so we used a threshold of 0.7.

Proposed Fingerprint recognition method: Another biometric check is fingerprint. We have used OpenCV to fingerprint in the proposed system. We take the fingerprint of the person [18] at registration and verify it at verification time.

VI. EXPERIMENTAL RESULTS
Proposed Face Recognition
The proposed system consists primarily of the following three steps for face recognition:
1. First, we need to create a database with multiple images of faces for each person.
2. Next, we will use the images from the database to identify faces and train the face recognition program.
3. The third step is to verify that the facial recognition software can recognize faces it was programmed for.

Dataset:
We used the publicly accessible AT &T "The Database of faces", also known as "The ORL Database of faces" in our proposed system. The database contains ten images of each subject. Images were taken at various times and with different lighting conditions. The facial expressions of the subjects (smiling or smiling open or closed eyes), as well as facial details like glasses or without glasses, were varied. The dark background was uniform and subjects were in front and upright positions.

Fig 4: Architecture Diagram of Offline Recognition

Fig 5: Images of Fingerprint Dataset:
Face Recognition:
We recommend that we take at least 15 images using the web camera to achieve better performance. The proposed system recognizes the face of the image taken by the camera with a similarity 93%. Fingerprint authentication was also successfully performed.

Conclusion
It is clear that biometric security has been an active area of research over the past few years. The proposed system was evaluated using biometric modalities like fingerprint and face. This includes the use of publicly available databases as well as face images captured by webcam and fingerprint scanners with well-defined associated protocols. The system was successfully developed and tested using both offline and real-time recognition. The system was successfully tested and evaluated. The system uses publicly accessible data. Different algorithms are used to recognize different biometrics. Future work will be possible with the proposed work, such as using video quality measures to detect video attacks and further evaluation of other image-based modalities, like palm print.
REFERENCES: