FACE ANTI-SPOOFING USING BLOCK AVERAGE LOCAL BINARY PATTERN

Project Reference No.: *48S_BE_2749*

College : Jawaharlal Nehru New College of Engineering, Shivamogga
Branch : Department of Information Science and Engineering
Guide : Dr. Raghavendra R J
Student(s) : Ms. Akshatha J S
Ms. Ananya S
Ms. Nanditha A L
Ms. Nidhishritha B M

Keywords:

Face anti-spoofing, Local Binary Pattern, Block Average Local Binary Pattern, Texture analysis, Information security.

Introduction:

Face anti-spoofing is a critical technology in face recognition systems, designed to determine the authenticity of a detected face and prevent spoofing attacks. Spoofing attacks involve an intruder attempting to gain unauthorized access by presenting a fake representation of a user's face, such as a photo or video . Early face recognition research focused on face matching, often overlooking the importance of verifying the liveness of the presented face. However, the vulnerability of face recognition systems to presentation attacks (PAs), including 2D printing and 3D masks , has become increasingly apparent. As human faces are widely used biometrics in AI systems, robust face anti-spoofing measures are essential.

Texture-based methods are a significant area of research in face anti-spoofing. These methods leverage the difference in texture between a real face and a spoofed image. Real faces possess more detailed appearance information, while spoofing attacks often suffer from information loss due to imperfect reproduction by spoofing media]. Researchers have explored various texture descriptors to capture these differences. For instance, Tan used the surface roughness of an attack image and a real face to detect attacks with printed photographs. Maatta explored micro-textures for spoofing detection using Local Binary Pattern (LBP). To address the limitations of LBP, such as

its lack of global spatial information, researchers have proposed improved descriptors like LBP variance (LBPV) and Local Ternary Pattern (LTP)]. LTP, for example, is designed to be insensitive to illumination variations and preserves essential appearance details.

Objectives:

1. Collection of face anti-spoofing dataset.
2. To detect the face in given image using viola-jones face detector.
3. To develop a novel face anti-spoofing descriptor called Block Average Local Binary Pattern (BALBP).
4. To extract the features using BALBP descriptor.
5. To classify given test image as a real or spoof image.

Methodology:

The proposed system employs the following methodology to detect face spoofing, figure 1 depicts the architecture of our proposed work:

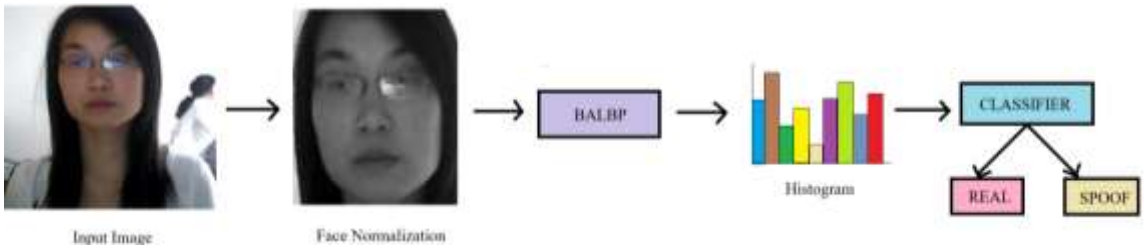

Figure 1: Architecture of proposed method

- Image Acquisition and Pre-processing: Initially, an image or video is captured as input. Pre-processing techniques are then applied to enhance the quality of this input. This involves normalizing lighting conditions, adjusting contrast, and correcting colours variations to ensure consistency across different inputs.
- Face Detection and Alignment: The Viola-Jones face detector is used to locate faces within the image. This robust and efficient algorithm identifies potential face regions. The detected faces are then aligned to a standard position and scale. This alignment is crucial for ensuring that subsequent feature extraction is consistent and accurate.
- Feature Extraction: This is a critical step where distinguishing characteristics between real and spoofed faces are identified and extracted. The system uses

a novel descriptor called Block Average Local Binary Pattern (BALBP). The input image is divided into smaller, overlapping blocks. Within each block, Local Binary Pattern (LBP) codes are computed. These LBP codes capture the local texture patterns within each block. The LBP codes within each block are then averaged to produce a more robust representation. A histogram of these averaged LBP codes is then generated. This histogram represents the distribution of texture patterns across the face image. BALBP is designed to be robust to variations in lighting and noise, which are common in spoofing attempts.

- Classification: The extracted BALBP feature histogram is then fed into a classifier. Machine learning models, such as Support Vector Machines (SVM) or K-Nearest Neighbour (KNN), are trained on a dataset of real and spoofed faces. The classifier learns to recognize the subtle patterns in the BALBP histograms that differentiate between genuine and fake faces. The trained classifier then categorizes a given test image as either "Real" or "Spoof."

Result and Conclusion:

In conclusion, Evaluation of Block Average Local Binary Pattern (BALBP) method is done through a series of experiments. These experiments employ standard metrics, including precision, recall, F1-score, and Average Recognition Rate (ARR), to assess the system's ability to accurately classify real and spoofed faces. The evaluation is conducted on four publicly available and diverse face anti-spoofing datasets—NUAA, MSU-MFSD, Replay-Attack, and Replay-Mobile—ensuring a robust assessment across various conditions and spoofing attack types. The results demonstrate that BALBP achieves a higher recognition rate than both Local Binary Pattern (LBP) and Local Ternary Pattern (LTP) across these datasets, indicating its superior effectiveness in capturing the subtle texture differences between real and spoofed faces. In summary, the experimental results confirm that BALBP is a valuable advancement in face anti-spoofing, exhibiting improved performance compared to existing texture-based methods.

Future Scope:

The future scope of this project includes:

1. BALBP can experiment with other standard face anti-spoofing datasets.
2. Work can be enhanced by taking different pixel sizes.