International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Hidden Markovian Model Combined with Dynamic Mode Decomposition for Detecting Deception in Videos

Shyama V S[1], Mary Linda P A[2]

[1, 2]Department of Computer Science and Engineering, KMCT College of Engineering, Calicut, India

Abstract: ***Biometric authentication systems can be deceived in one way or other. Spoofing attacks to these biometric systems has greatly effected in verifying the identity of an individual. Detection of the spoofing attacks is a serious problem whereas face recognition systems and voice authentication systems are mostly vulnerable to spoofing. Traditional spoofing detection methods are not up to the mark due to the rapid increase in the hacking methodologies. Several spoofing attack detection methods have been proposed but each of them has its own drawbacks. The basic method used in detection of spoofed video uses prior knowledge regarding live face images such as eye blinking and lip movements since attack types are often unknown and very different from each other. Due to the lack of efficiency and accuracy whereas handling excessive attacks, specific cue which is peculiar to the attack must be developed. Thus a data driven approach with high accuracy and efficiency was developed. A combination of Dynamic Mode Decomposition, Principle Component Analysis and Hidden Markovian Model was introduced to provide a better security for the biometric authentication systems in videos. The project focus on both facial spoofing detection and voice spoofing detection in videos simultaneously. Principle Component Analysis and Dynamic Mode Decomposition together helps in the facial biometric authentication and Hidden Markov Model helps in the voice authentication. It considers various facial expressions, and even tilted angled faces in the spoofed samples. Local Binary Patterns, and Support Vector Machine were introduced for identifying print attacks, cut photo attacks and replay attacks. It results in better security, scalability, efficiency and accuracy.***

Keywords: Dynamic Mode Decomposition, Hidden Markov Model, Local Binary Patterns, Replay Attacks

1. Introduction

Biometrics is a technology that can measure and analyze the human body characteristics. It involves both Physical characteristics such as fingerprints, faces or iris patterns and behavioral characteristics such as voice, signature. One of the main challenge that the biometric recognition systems faces today is the unauthorized access of the individuals and thereby the efficiency, accuracy and effectiveness of the system is hampered. Spoofing attacks is one among the cause for illegitimate actions in the biometric systems. Spoofing attacks can be defined as the method of falsifying the biometric system by an unauthorized system such as the use of artificial fingers, contact lens with retinal patterns and recorded voice etc. Spoofing attacks are considered as a major threat because they are implemented with the sole purpose of fooling the system while obtaining the required authentication information from the user. Preventing such spoofing attacks is of primary importance so that it makes people more confident that their information is secure [1]. A photograph of a valid user can be bent, rotated, and/or shifted accordingly before the camera to spoof the authentication system. That makes the photographic spoofing a simple and cheap way of fooling the facial recognition system. Among them liveness facial biometrics [2] based spoofing detection is to be considered seriously as it is highly prone to spoofing attacks. It involves placing genuine photographs or dummies, playing video recording etc. in front of the camera.

Face authentication is proven to be very useful to providing user authentication which helps one to protect information. The facial recognition uses digital image or video processing techniques for authentication. In spite of the fact that the complex algorithms are required for processing images and videos, facial recognition techniques have proven to be very useful for contemporary security applications. Liveness face detection can be either positive class or negative class. Positive class have limited variations and negative class includes the spoofed faces on photographs, dummy or recorded videos. Detection may be influenced by the picture quality, improper lighting, viewing angles, and spoofing alerts. Other than these limitations, in liveness detection for facial biometrics, there are limitations such as lack of accuracy and efficiency in identifying the presentation attacks, replay attacks and print attacks, lack of extracting the unique features that distinguish a valid and spoofed videos, lack of providing the three dimensional (3D) information.

For the past few years, many algorithms have been provided to identify spoofing attacks. Many of such theories have been successful in identifying photograph spoofing with great accuracy. The same could not be said in the case of video spoofing. Facial Recognition in video spoofing, poses a greater threat than any other spoofing techniques as it provides many physiological clues to the system like blinking, head movement, etc. When a video clip of a valid user is placed in front of a camera, it can easily deliver the necessary data to measure the nodal points of a face which makes it a challenge to identify such spoofing attacks. The lack of verification is misused and utilized for spoofing. If a proper security layer is added for better verification of the user, the threats of spoofing can be minimized. Existing technologies do not provide the reliability that the users expect.

In the proposed project, a data driven approach called

Dynamic Mode Decomposition [3] accompanied by Hidden Markovian Model [4] would eliminate the existing flaws in detecting the spoofing possibilities. The work also make use of Local Binary Patterns [5] Principle Component Analysis and [6] Support Vector Machine [7] so as to provide efficient liveness detection of the facial biometrics. These algorithms could help in the extraction of the unique features and relevant modes from videos and can provide a good separability between valid videos and the spoofed ones. DMD has the capability of capturing and discovering the important signs of valid face videos and at the same time artefacts of spoofed videos such as moiring and planar effects are also being extracted. Thus it is computationally efficient in handling the large sized videos as it considers the deep and accurate complex flow behavior of the features that can tackles both photo based and video based spoofing attacks.

2. Related Works

Many researches has been done in the area of biometrics and thereby the developments. In last few years various efficient methods have been proposed for spoofing. Most of the work on the facial spoofing detection focus on the outline structure of facial expressions such as eye blinking, lip movement, and head movement. Some noticeable work in area of data hiding are as follows:

Most of the face liveness detection algorithms require user cooperation for adopting the behavioral features. Z. Zhang [8] proposed a system of multispectral face liveness detection method which does not require the user cooperation. In this method, the multispectral properties of the human skin versus non skin are analyzed by using Lambertian model. After that two discriminative wavelengths are extracted. Zhang also used trained SVM classifier for identifying the genuine and fake images. The advantages of this proposed method is that it makes the liveness detection more user friendly and fast. Also it considers the user system distance factor which results into better performance. But this method faces major drawbacks as it does not adopt time consuming and user unfriendly interactions. Also it does not detect the mask faces and thereby the accuracy of the algorithm is reduced.

G. Pan [9], [10] established a method for the liveness detection especially for the eye blink sequences. In this method spontaneous eye blink is detected and modelled as the inference in a Conditional Random Field (CRF) [11] framework which contains variable nodes and factor nodes. For the computational efficiency and accuracy a discriminative measure known as the eye closity is derived and it is enclosed in to the contextual model. The major advantages of this method is that it does not require extra hardware other than a webcam, it is a non intrusion method and Pan proved that it has high performance in detecting the spoofed facial images. But on the other side it holds various disadvantages such as the spoofing detection is highly affected by strong glasses reflection that can cover the eyes partially or fully, also this algorithm does not works for the video spoofing.

Two dimensional facial spoofing attack detection were studied by R. Tronci [12] as a combination of both static and dynamic (video) analysis of the scenes. The static analysis considers to work upon the photo attack and the noise introduced during those attacks. In the case of dynamic analysis, it examine the human facial physiological characteristics this method can easily identify the features about the motion, texture and the liveness of the input scenes.

In this proposed method, each image is represented with feature spaces by using JPEG histogram, texture histogram and many others so that the dynamic features are extracted accurately. After obtaining the features a classifier is trained so that for each frame of a video, a score is obtained. By comparing these scores with the threshold values the method easily detects whether the input sample is a spoofed sample or actual sample. Here for N frames it has N scores and N number of visual features are being used.

This method proves to have better performance but it also faces various disadvantages such as detection of the photo within the context of automatic face verification system is difficult. It is a time consuming process and could not be applied on three dimensional attacks for face spoofing.

W. R. Schwartz [13] proposed an anti-spoofing method to discriminate the valid and non valid videos by considering both spatial and temporal informations with the help of Partial Least Squares regression method. Firstly, a video containing N frames are divided into m parts such that the feature extraction process is done at every ith frame. Descriptors are extracted from each frame and are concatenated to form the resultant feature vector. This methods uses various databases and the sample videos are being trained and tested. In the training stage, the face regions are analyzed from the videos. The color frequency, histogram of oriented gradients, and histograms of shearlet coefficients of the image are integrated to yield better performance. Upon this integrated component, Partial Least Squares Regression method is carried out and thereby, the samples are being tested and the spoofed ones are detected. The major drawback of this method is that it does not focus on the specific features of a face image like eyes, lips etc. an overall face image is considered from a video and it is being processed.

A. da Silva Pinto [14] proposed a method in detecting the video based spoofing attacks based on the visual dynamics. Firstly noise signatures of every videos are extracted and then the Fourier Spectrum on logarithmic scale is computed for each and every frame. In the next stage the visual rhythms for each video is created and training is provided to the classifier by using pixel intensities or gray level occurrence matrices. In the testing phase a visual dynamic for a given video under examination is taken out and discriminated whether it is a valid access or spoofed access. This method has a disadvantage that it cannot extract the unique features that are included in the facial images.

Security is a major concern in case of biometrics. Spoofing attacks to the biometric systems have been increasing day by day and thereby unauthorized access to these systems cause a major security problem. There are several existing methodologies to handle these security issues. But every

method has its own drawbacks. Considering all the existing drawbacks, Dynamic Mode Decomposition algorithm has proposed along with Hidden Markov Model to recognize the spoofed videos. The characteristic features of using these algorithms is that it can effectively and efficiently identify the spoofed videos by analysing the unique characteristics of facial features and also the voice in the videos.

Existing methods cannot extract the unique facial features and thus it lacks efficiency. The existing systems effectively deals with the spoofing detection of the images rather than videos. Different algorithms were implemented to detect the spoofed samples. But the drawback is that none of the algorithm could efficiently detect the facial spoofing. Time consumption, lack of efficiency, lack of handling illumination changes etc. Existing method cannot even extract the unique facial features. In order to provide a better authentication to biometric systems, a combined authentication scheme of DMD and HMM is proposed. DMD accompanied by PCA is used for the spoofed facial detection even in the case of tilt angles, different facial expressions, tilt angles etc. At the same time voice authentication using Hidden Markov Model is also used. Kernel based SVM classifier is used to identify the spoofed samples. This can efficiently handle the biometric system by considering facial as well as voice authentications.

3. DMD combined with HMM Model

Detection of the spoofing attacks in videos by using Dynamic Mode Decomposition accompanied by Hidden Markovian Model improves the identification task. Principle Component Analysis can help to detect the spoofing of facial spoofing in case of tilt angles, occlusions and different facial expressions. Existing spoofing attack detection method concentrate only on either the facial videos or the voices. Hidden Markovian Model combined with Dynamic Mode Decomposition and Principle Component Analysis is proposed to detect the facial videos and voice recognition simultaneously.

The Hidden Markovian Model combined with Dynamic Mode decomposition is proposed as a solution to the limitations of the existing biometric systems. The proposed method is an attempt to discriminate the spoofed samples and the valid videos.

Dynamic Mode Decomposition has the ability to extract the unique facial features and thereby the security for the biometric system can be efficiently and effectively handled. Along with DMD, HMM PCA also implemented for examining the spoofing in case of different facial expressions, tilt angles and occlusions

Hidden Markov Model provides a method of storing the voiceprints of individuals uniquely. This is different from the speech recognition. The voiceprint will then be used for voice authentication, using text independent speaker recognition methods in which the system does not have belief in on special wording being talked, but one and only on the voice of the speaker. The method explains more about the user training phase detailing how the voice print of an individual is stored in the system by extracting certain features especially Cosine Normalized Phase and Modified Group Delay Phase of the waveform using HMM.

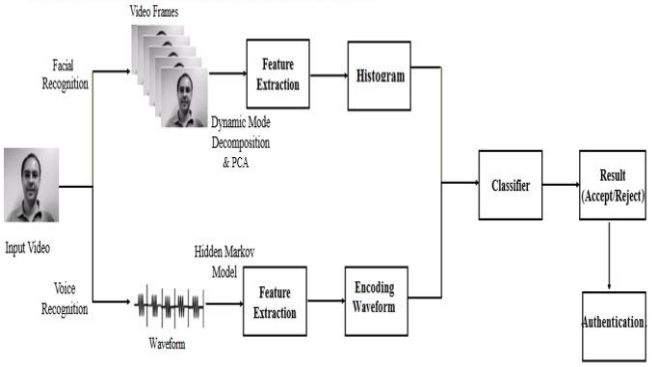


Figure 1: The Framework of HMM based Spoofing Detection

Figure 1 shows the framework of the proposed system. In this system, DMD is effectively used for countering spoof attacks in face recognition. Since DMD has not been used with classification of video sequences, a system is proposed which consists of pipeline including DMD, Local Binary Patterns and SVM. This combination is ideal because DMD captures the visual dynamics in the form of a fixed-size image, LBP can effectively capture the dynamic patterns, and SVM is known to be an ideal general-purpose classier that minimizes the empirical risk of classification error. In this modified DMD, the absolute value of the complex modes when rendering the "DMD image" is considered. The optimal mode is selected from the DMD modes using the zero phase angle criteria.

The pipeline of the proposed system consists of DMD, Local Binary Pattern histograms and a kernel based Support Vector Machine (SVM) classier for facial spoofing detection and for the voice authentication system, Hidden Markov Model is used. First, a video is processed using the DMD algorithm in order to output dynamic mode images. From which, we select a single dynamic mode image corresponding to eigenvalue whose phase angle is = 0 or closest to it. Second, LBP histogram features are computed for this dynamic mode image. Finally, the produced LBP code is fed into a trained SVM classier in order to classify whether the processed video is a valid access or spoof. Half Total Error Rate (HTER) [15] is used to evaluate the performance measure. To validate our DMD pipeline Principle Component Analysis (PCA) based on snapshot approach as a baseline method.

In HMM, the voiceprints of the individuals are considered and unique features are being described and extracted. Modified Delay Group Function and Cosine Normalized Functions are the major parameters involved in feature extraction. The first step is to capture the sound waves of the voice of the speaker. This process will be done by using the microphone. A microphone is used to record the voice. The ultimate output of this step will be a formatted .wav file. In the training phase the .wav files are user utterances of individual phonemes. After capturing the sound, it must be validated to see if it is free from defects. The objective of this step is to remove any noise that may be remaining in the sound waves in small amounts. The next step is to model a

Hidden Markov Model for each phoneme that is trained and using a classifier it identifies whether the captured voice is a spoofed one or not.

Different facial expressions, and tilt angles in the videos were also analysed. It is done by using PCA algorithm. Here at first an input image frame is considered from a video. Next step is to perform PCA upon this and finally recognition takes place. Mean and Gaussian Curvature analysis were also examined to identify the facial features in depth.

The proposed project can effectively discriminate the spoofed samples and original sample. Authentication can be made efficient by using the DMD, PCA and HMM algorithms. Comparing to the existing algorithms, these methods outperforms well. These has the capability to analyses the unique characteristics of the facial features and also the voiceprints. Thus an effective efficient and well performed authentication can be assured.

3.1 Dynamic Mode Generation

An efficient Dynamic Mode Decomposition algorithm is used for the mode selection. DMD algorithm has the capability to identity both moiring and planar effects along with eye blinking head movements. A test video is given as an input to the system and (1−N) video frames are generated. On applying the Dynamic Mode Decomposition algorithm, these (1...N) video frames are converted into (1…(N-1)) dynamic modes. From these generated dynamic modes, a single mode is being selected. This is done on the basis of the Eigen value for the dynamic modes. After calculation of the Eigen values, the phase angle equal to zero or close to zero is selected as the final dynamic mode. In this stage three algorithms are used: Dynamic Mode Decomposition, Euclidean Distance Algorithm for finding the distance between two points in the Euclidean space [16], and Singular Value Decomposition [17] for matrix factorization.

3.2 Feature Extraction

DMD has the ability to extract the unique facial features combined with eye blinking, head movements, lip movement. In order to extract the different facial expressions with tilt angles, Principle Component Analysis (PCA) is used. DMD along with PCA can effectively extract the features in which it can uniquely examine the different characteristics facial features. Histograms corresponding to the generated mode is built on the basis of features extracted.

3.3 Histogram Creation

Histogram is created for the corresponding selected mode after applying dynamic mode decomposition and principle component analysis. The image is divided into different blocks. Local Binary Pattern histogram s created from each blocks. All the histograms created are concatenated to form feature histogram.

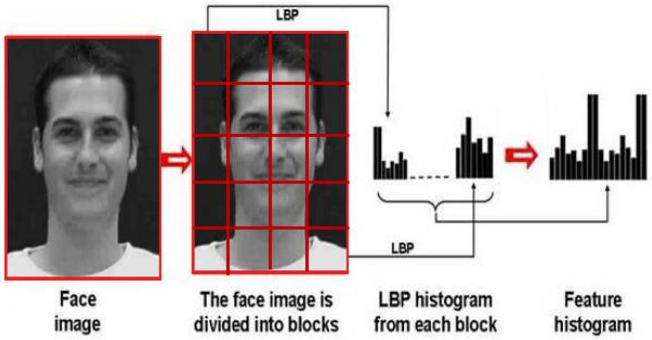


Figure 2: Histogram Creation

3.4 Voice Authentication

Hidden Markov Model is an effective model for examining the voiceprints of an individual since it has a well defined mathematical structure. It does not require expert knowledge about speech signal. Errors in the analysis don't propagate and accumulate. Temporal property of speech is accounted. Hidden Markov Model contains HTK (Hidden Markov Model Tool Kit) that is capable of describing the waveform by itself with given parameters.

In identifying the voiceprints, firstly the voiceprints of an individual is stored and trained. The voice validation and noise reduction is then done by using the algorithm MMSE (Minimum Mean Square Error) [18] algorithm. Cosine Normalised Phase (Cos-Phase) and Modified Group Delay Phase (MGDF) [19] is used to identify the converted speech. MFCC (Mel Frequency Cepstral Frequency) [20] algorithm is also used for extracting the voice features. MFCC algorithm is generally preferred as a feature extraction technique to perform voice recognition as this involves the generation of coefficients from the voice of the user that are unique to every user. The waveform is then encoded and parameterized for authentication. Figure 3 shows the voice authentication process. Figure 4 shows the block diagram for obtaining the Mel Frequency Cepstral Coefficients.

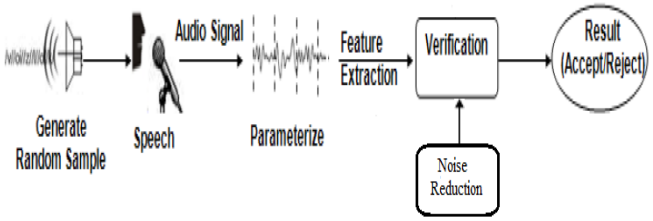


Figure 3: Voice Authentication

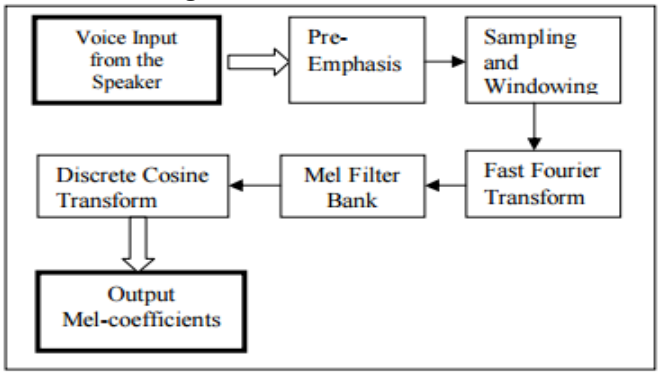


Figure 4: Block diagram for obtaining MFCC

The following equation represents the filter bank in the feature extraction stage with M (m=1, 2, 3…..M) filters, where m is the number of triangular filter in the filter bank [2

$$Hm(k) = \begin{cases} 0, \text{for } k < f(m-1) \\ \dfrac{k - f(m-1)}{f(m) - f(m-1)}, \text{for } f(m-1) \le k \le f(m) \\ \dfrac{f(m+1) - k}{f(m+1) - f(m)}, \text{for } f(m) \le k \le f(m+1) \\ 0, \text{for } k > f(m+1) \end{cases}$$

Each triangular filter in the filter bank satisfies the following equation. After that the logarithm of the sum of filtered components for each filter is computed [21] and thereby the features are extracted in the form of coefficients.

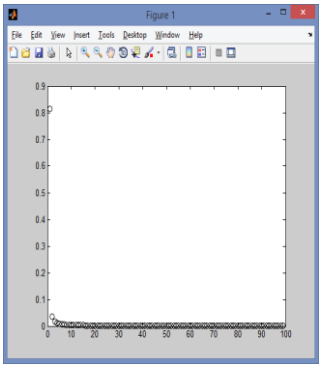
$$\sum_{m=0}^{M-1} Hm(k) = 1$$

3.5 SVM Training and Classification

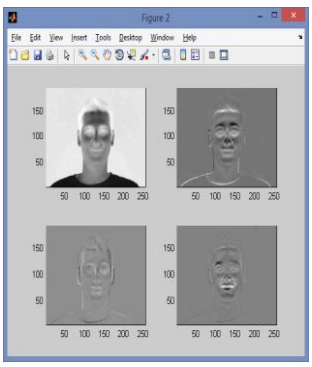
Support Vector Machine classifies whether the given video is a spoofed sample or not by considering both facial features and voice features. Training is using the datasets available online. SVM classifies the videos based on the histograms generated for the facial features. In the case of voice authentication the encoded waveforms are examined by the SVM classifier for classifying the spoofed voice and original sample.

4. Implementation and Analysis

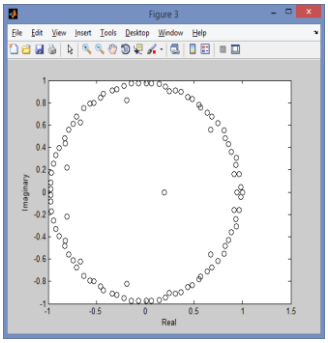
The HMM combined with DMD is implemented using Matlab. The proposed method is tested on CASIA-FASD dataset. The dataset consists of 600 videos including 150 valid-access and 450 attacks. The training set contains 240 videos and testing set include 360 videos. Voice testing is done by using various human voices. A video is provided as an input and classifies whether it is a spoofed video or not. It classifies by considering the facial expressions as well as the voice variations. After classification, the systems checks for the user authenticity.



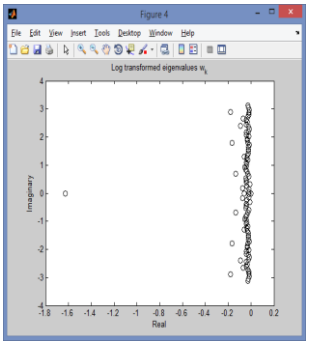
(a)



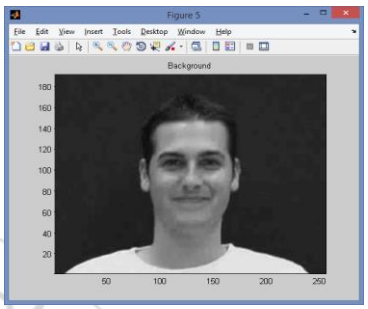
(b)



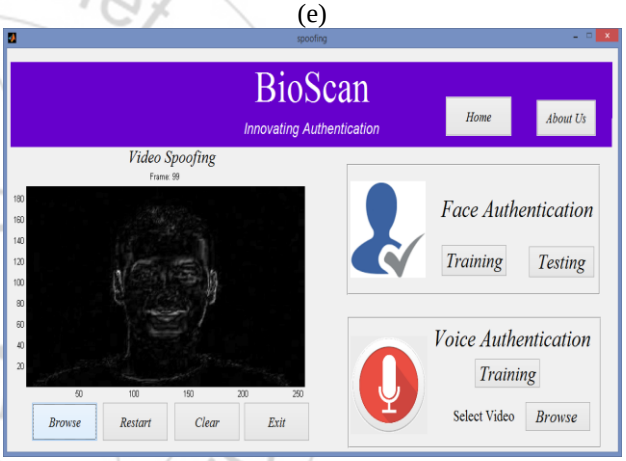
(c)



(d)

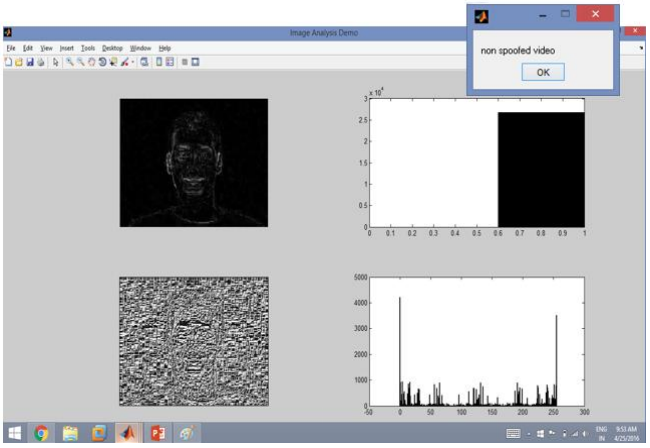


(e)



(f)

Figure 5: (a) Singular Value Decomposition Plot, (b) Frame Selection Modes, (c) Eigen Value Plot, (d) Transformed Eigen Value Plot (e) Background, (f) Frame Reading



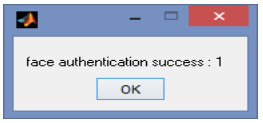


Figure 5: Classification and Authentication

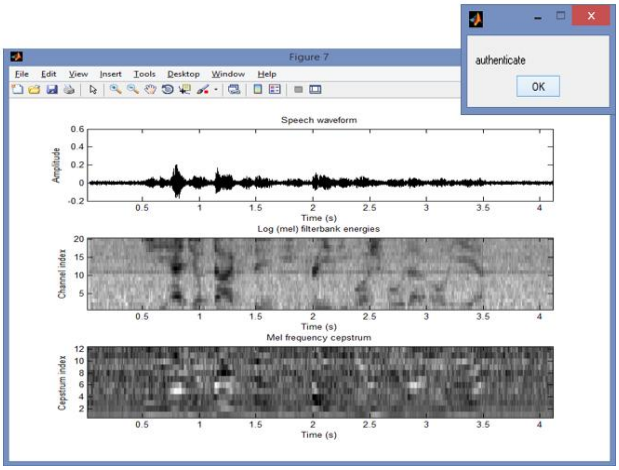


Figure 6: Voice Spoofing Detection

By comparing with the existing similar methodologies, the proposed system performs more efficiently. It results in good accuracy and has high performance.

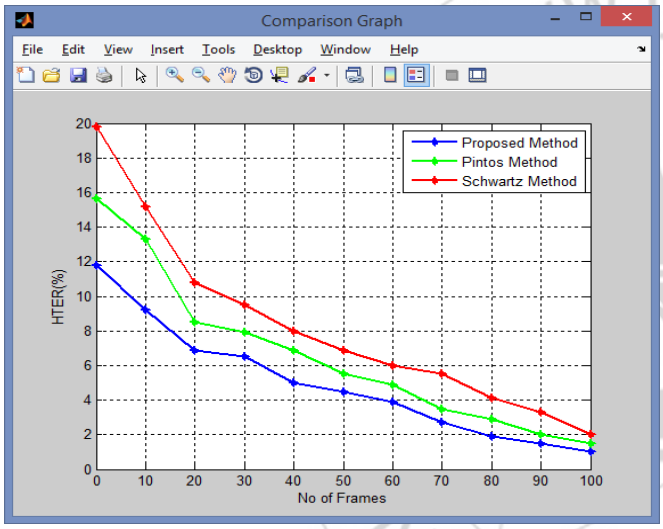


Figure 7: Comparison Graph

A comparison graph is plotted with Half Total Error Rate (Average of False Acceptance Rate and False Rejection Rate) against No of Frames. The proposed system is compared with two other existing systems i.e., Pintos Method and Schwartz Method. Finally the proposed method outperforms well. It has a reduced error rate compared with the other systems.

5. Conclusion

Dynamic Mode Decomposition (DMD) in combination with Hidden Markov Model (HMM), Linear Binary Patterns (LBP), Principle Component Analysis (PCA) and Support Vector Machine (SVM) performs well for identifying the spoofed videos and valid videos. It has the capability to simultaneously extract the liveness characteristics and attack specific artefacts. The dynamic mode decomposition helps in extracting the unique features of the facial expressions in the video frames and easily discriminates the valid video from the spoofed video. The principle component analysis approach can effectively identify the different facial expressions and tilt angles and helps in the user authentication. Hidden Markov model helps in authenticating the voice of a user. Hmm with the help of Mel Frequency Cepstral Coefficients (MFCC) and Minimum Mean Square Error (MMSE) algorithm helps in the voice authentication and helps in providing more security to the biometrics. The proposed project has an advantage of providing better security, efficiency, performance and accuracy. As a future work, the typing behavior or scrolling behavior characteristics of individuals can be examined in order to provide a better security to the biometric systems.

.References

[1] Detection of Face Spoofing Using Visual Dynamics Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony T.S. Ho, IEEE Transactions on Information Forensics and Security, IEEE, 2015
[2] Biometrics: A Tool For Information Security Anil K. Jain,Fellow, Ieee, Arun Ross,Member, Ieee, And Sharath Pankanti,Ieee Transactions On Information Forensics And Security, Vol. 1,June 2006
[3] P. J. Schmid, K. E. Meyer, "Dynamic mode decomposition and proper orthogonal decomposition of flow in a lid driven cylindrical cavity," in 8th International Symposium on Particle Image Velocimetry, pp. 25–28, 2009.
[4] The Application of Hidden Markov Models in Speech Recognition Mark Gales1 and Steve Young Foundations and Trends in Signal Processing Vol. 1, No. 3, 2007, 195–304
[5] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti spoofing," in Biometrics Special Interest Group (BIOSIG), IEEE 2012 BIOSIG- Proceedings of the International Conference of the,pp ,1-7, IEEE, 2012
[6] Modular Image Principal Component Analysis for face recognition Pereira, J.F.; Cavalcanti, G.D.C.; Tsang Ing Ren Neural Networks, 2009. International Joint Conference on Neural Networks, Atlanta, Georgia, USA, June 14-19, 2009, Pages: 2481 - 2486
[7] N. Cristianini and J. Shawe Taylor, An introduction to support vector machines and other kernel based learning methods, Cambridge university press, 2000.
[8] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li. Face liveness detection by learning multispectral re- flectance distributions in International Conference on Face and Gesture, pages 436–441, 2011.
[9] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eye blink based anti-spoofing in face recognition from a generic web camera," in Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on, IEEE, 2007.
[10] G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," Recent advances in face recognition, pp. 109–124, 2008
[11] K.Zuiderveld,"Contrast limited adaptive histograph equalization.," Graphic Gems IV, pp. 474–485, 1994
[12] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli, "Fusion of multiple clues for photo attack detection in face recognition

systems," in Biometrics (IJCB), 2011 International Joint Conference on, pp. 1-6, IEEE, 2011
[13] W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low level descriptors," in Biometrics (IJCB), 2011 International Joint Conference on, pp. 1–8, IEEE, 2011.
[14] A. da Silva Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video based face spoofing detection through visual rhythm analysis," pp. 221–228, IEEE, 2012
[15] Kar-Ann Toh, Jaihie Kim, Sangyoun Lee, "Biometric Scores fusion based on total error rate minimization", Biometrics Engineering Research Center,2007
[16] A. Meijster, J.B.T.M. Roerdink And W.H. Hesselink, "A General Algorithm For Computing Distance Transforms In Linear Time", 2009
[17] Alan Kaylor Cline The University of Texas at Austin Inderjit S. Dhillon The University of Texas at Austin, "Computation of Singular Value Decomposition".
[18] Dong Yu, WA Li Deng "Robust Speech Recognition Using a Cepstral Minimum-Mean-Square-Error-Motivated Noise Suppressor", Ieee Transactions on Audio, Speech and Language Processing, Volume:16 , Issue: 5, 2008
[19] Zhizheng Wu, Haizhou Li "Voice conversion and spoofing attack on speaker verification systems",Singapore , 2013
[20] Koustav Chakraborty , Asmita Talele, "Voice recognition using MFCC Algorithm", 2014
[21] Siddhant C. Joshi, Dr. A.N.Cheeran, "MATLAB Based Feature Extraction Using Mel Frequency Cepstrum Coefficients for Automatic Speech Recognition", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 6, June 2014

Author Profile

Shyama V S is pursuing her M.Tech degree in Computer Science and Engineering from KMCT College of Engineering, Calicut University. She obtained her B.Tech Degree in Computer Science and Engineering from Calicut University Institute of Engineering And Technology, in 2014.

Mary Linda P.A. is Assistant Professor, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University. Her research focuses on Image processing, Internet security. She obtained her B.Tech degree in Information Technology from KMCT College of Engineering in 2007. She completed her M.Tech degree in Image processing from Model Engineering College, CUSAT in 2012.