International Journal of Intelligent Computing and Technology
ISSN: 2457-0249 (Online)
Website: https://www.ijict.com January (2023) - Vol. 6, Iss.2 Pages:1-07

Evaluation of PPG feature values toward biometric authentication against presentation attacks

[1] Dr P Pandiselvi, [2] S Gobika
[1]Assistant Professor, [2]PG Student,
Mangayarkarasi College of Arts and Science for Women, Paravai, Madurai

Article History- Received: January 2023; Published: January 2023

Abstract

Recently, physiological signal-based biometric systems have received wide attention. Unlike traditional biometric features, physiological signals cannot be easily compromised. Photo plethysmogram (PPG) signal is easy to measure, making it more attractive than many other physiological signals for biometric authentication. However, with the advent of remote PPG (PPG), un observability has been challenged when the attacker can remotely steal the PPG signals by monitoring the victim's face, subsequently posing a threat to PPG-based biometrics. In PPG-based biometric authentication, current attack approaches mandate the victim's PPG signal, making PPG-based attacks neglected. In this process, we proposed a versatile signal processing and analysis framework for (PPG). Within this framework the signals were decomposed into the frequency sub-bands using decomposition method, and then a set of statistical features was extracted from the sub-bands to represent the distribution of wavelet coefficients. Independent components analysis (ICA) and continuous wavelet transform (CWT) is used to extract the features from the decomposed signals, and reduce the dimension of data. Then these features were used as an input to a support vector machine (SVM). The performance of classification process is evaluated by means of the Accuracy, Sensitivity and Specificity.

Keywords: ***Biometric authentication, identity spoofing, photo plethysmogram and presentation attack***

INTRODUCTION

Signal processing is an area of systems engineering, electrical engineering and applied mathematics that deals with operations on or analysis of analogue as well as digitized signals, representing time-varying or spatially varying physical quantities. Signals of interest can include sound, electromagnetic radiation, images, and sensor readings, for example biological measurements such as electrocardiograms, control system signals, telecommunication transmission signals, and many others.

Authentication systems using biometrics are already commonly used in a variety of applications, ranging from mobile phones to border security, because they are easy to use and provide a potentially higher level of security [1]. Instead of memorizing a lengthy password that could be intercepted by a hacker, the user only needs to use their finger or their face to confirm their identity. Despite being commonly used, these biometrics-based authentication systems are still vulnerable to spoofing attacks where an attacker can gain access to the user's unique biometric [2]. A biometric presentation attack (BPA) is a situation in which an attacker has obtained the authentic user's biometric and is using it to fool the biometrics-based authentication system to access the user's devices and accounts. For example, by downloading a picture or a video of the user from their social media page, the attacker may be able to fool the system that relies on face recognition [3]. There have even been cases where attacker's 3D print facial masks or fingerprints can successfully spoof the authentication system [4]. The authors use machine learning algorithms to find discriminative patterns in the frequency spectra that may be difficult to be noticed by a human. The advantage of using the entire frequency spectra directly makes PPG Secure robust to a variety of attacks because we do not have to design what signal features might be discriminative of real live faces which may vary for different methods of fraud.

REVIEW OF LITERATURE

Corey D. Holland et al, presented an objective to evaluate the effects of eye tracking specification and stimulus presentation on the biometric viability of complex eye movement patterns (CEM). Six spatial accuracy tiers (0.5°, 1.0°, 1.5°, 2.0°, 2.5°, 3.0°), six temporal resolution tiers (1000 Hz, 500 Hz, 250 Hz, 120 Hz, 75 Hz, 30 Hz), and five stimulus types (simple, complex, cognitive, textual, random) are evaluated to identify acceptable conditions under which to collect eye movement data.

Corey D. Holland, et al, investigated within the medical field for more than a century to study about brain diseases like epilepsy, spinal cord injuries, alzheimer's, Parkinson's, schizophrenia, and stroke among others [5]. They are also used in both brain computer and brain machine interface systems with assistance, rehabilitative, and entertainment applications. Despite the broad interest in clinical applications, the use of brain signals has been only recently investigated by the scientific community as a biometric characteristic to be used in automatic people recognition systems.

Preben Kidmose, proposed a method for brain monitoring based on measuring the electroencephalogram (EEG) from electrodes placed in-the-ear (ear-EEG) [6]. The objective of their study was to further characterize the ear-EEG and perform a rigorous comparison against conventional on-scalp EEG. This is achieved for both auditory TR U NG Q. LE, CHANGQI NG CH ENG, AKK AR APOL SANGASOONGSONG and visual evoked responses, over steady-state and transient paradigms, and across a population of subjects.

Javad Sohankar, et al, proposed a E-BIAS based pervasive EEG based security system with both identification and authentication functionalities [7]. The main challenges were:1) accuracy, 2) timeliness, 3) energy efficiency, 4) usability, and 5) robustness.

In the title of Wireless Wearable Multisensory Suite and Real-Time Prediction of Obstructive Sleep Apnea Episodes, Obstructive sleep apnea (OSA) is a common sleep disorder found in 24% of adult men and 9% of adult women [8]. Although continuous positive airway pressure (CPAP) has emerged as a standard therapy for OSA, a majority of patients are not tolerant to this treatment, largely because of the uncomfortable nasal air delivery during their sleep.

METHODOLOGY

Various steps involved to generate the model is as follows: Input signal, pre-processing, feature extraction, feature matching and performance Analysis.

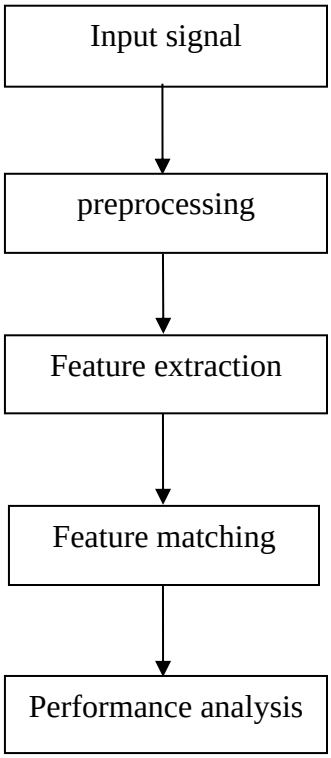

Fig 1 Module Description

Input Signal

PPG is a test that detects abnormalities in brain waves, or in the electrical activity of brain. During the procedure, electrodes consisting of small metal discs with thin wires are pasted onto the scalp. The electrodes detect tiny electrical charges that result from the activity of the brain cells. The technician will put a sticky gel adhesive on 16 to 25 electrodes, and attach them to spots on the scalp. Once the test begins, the electrodes send electrical impulse data from the brain to the recording machine. This machine converts the electrical impulses into visual patterns that appear on a screen. A computer saves these patterns. The technician may instruct to do certain things while the test is in progress. They may ask to lie still, close the eyes, breathe deeply, or look at stimuli (such as a flashing light or a picture).After the test is complete, the technician will remove the electrodes from the scalp. During the test, very little electricity passes between the electrodes and skin.

Pre-processing

Pre-processing is done by Bandpass filter and IIR filter. Filters are networks that process signals in a frequency-dependent manner. Signal distortion is the term often used to describe a systematic undesirable change in a signal and refers to changes in a signal from the non-ideal characteristics of the communication channel, signal fading reverberations, echo, and multipath reflections and missing samples. A bandpass filter is an electronic device or circuit that allows signals between two specific frequencies to pass, but that discriminates against signals at other frequencies. IIR filters are one of primary types of digital filters used in Digital Signal Processing. The impulse response is “infinite” because there is feedback in the filter; if put in an impulse (a single “1” sample followed by many “0” samples), an infinite number of non-zero values will come out (theoretically.)

Feature Extraction

Independent component analysis (ICA) is a feature extraction method that transform multivariate random signal into a signal having components that are mutually independent. Independent components can be extracted from the mixed signals by using this method. In this manner, independence denotes the information carried by one component cannot be inferred from the others. Statistically this means that joint probability of independent quantities is obtained as the product of the probability of each of them.

Feature Matching

The features extracted from the previous step were used as an input to a support vector machine (SVM) with two discrete outputs: epileptic seizure or not. Support Vector Machine : A Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyperplane. In two dimensional space this hyperplane is a line dividing a plane into two parts where in each class they lay on either side. The support vector classifier has many advantages. A unique global optimum for its parameters can be found using standard optimization software. Nonlinear boundaries can be used without much extra computational effort. Moreover, its

performance is very competitive with other methods. A drawback is that the problem complexity is not of the order of the dimension of the samples, but of the order of the number of samples.

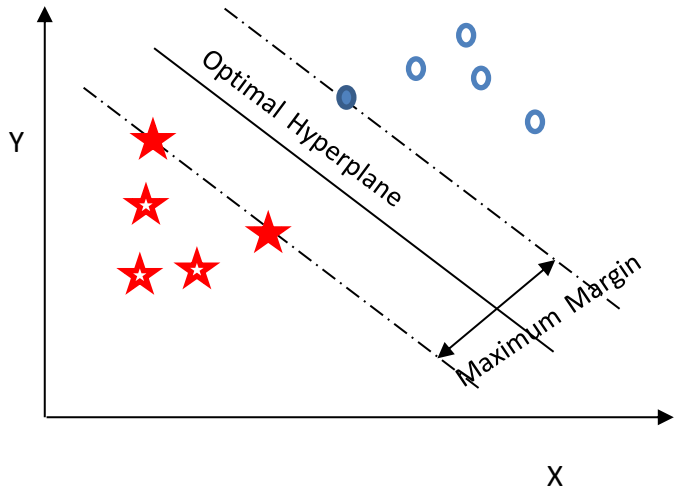

Fig 2 Represent the feature matching

K-Nearest Neighbour

K-Nearest Neighbour is one of the simplest Machine Learning algorithms based on Supervised Learning technique. K-NN algorithm assumes the similarity between the new case/data and available cases and put the new case into the category that is most similar to the available categories. K-NN algorithm stores all the available data and classifies a new data point based on the similarity. This means when new data appears then it can be easily classified into a well suite category by using K- NN algorithm. K-NN algorithm can be used for Regression as well as for Classification but mostly it is used for the Classification problems. K-NN is a non-parametric algorithm, which means it does not make any assumption on underlying data. It is also called a lazy learner algorithm because it does not learn from the training set immediately instead it stores the dataset and at the time of classification, it performs an action on the dataset.KNN algorithm at the training phase just stores the dataset and when it gets new data, then it classifies that data into a category that is much similar to the new data.

Performance Measure

The performance of the process is measured in terms of performance metrics like Accuracy, Sensitivity, Specificity. Terms associated with performance measures are:

- TP- True Positive (correctly identified)
- TN-True Negative(correctly rejected)
- FP-False Positive(incorrectly identified)
- FN-False Negative(incorrectly rejected)

Accuracy : Accuracy in classification problems is the number of correct predictions made by the model over all kinds predictions made.

$$Accuracy = (TP + TN) / (TN + TP + FN + FP)$$

Sensitivity: The ability of a test to correctly identify those with the disease (true positive rate).Measures the proportion of actual positives that are correctly identified.

$$Sensitivity = TP / (TP + FN)$$

Specificity: The ability of the test to correctly identify those without the disease (true negative rate). Measures the proportion of actual negatives that are correctly identified.

$$Specificity = TN / (TN + FP).$$

RESULTS & DISCUSSION

To evaluate the performance of PPG Secure the authors used a publicly available dataset, Replay-Attack [13] with video and photograph biometric presentation attacks. The dataset contains 360 x 240 pixels video recordings, recorded at 25 fps with a total of 1300 videos of 50 different people. The dataset has videos of authentic live users, and video and photo presentation attacks, in controlled and adverse lighting conditions. The photo and video attacks were recorded in the form of the attack fixed and handheld in front of the camera causing small motion. The results of the proposed method was computed separately on handheld and fixed attacks and separately on photo and video attacks. Based on the Table 1, it appears that the method being evaluated has a high level of accuracy (98%), meaning that it is able to correctly identify the target outcome in a large majority of cases. Additionally, the sensitivity of the method is also high (97.9798%), indicating that it is able to correctly identify most positive cases. The specificity of the method is also high (99.9796%), indicating that it is able to correctly identify most negative cases. Overall, these performance metrics suggest that the method being evaluated is very effective at accurately identifying both positive and negative cases of the target outcome.

Table 1 Performance Table

Methods	Performance
Accuracy	98%
Sensitivity	97.9798%
Specificity	99.9796%
Precision	97.9798%

CONCLUSION

This paper integrated CWT, k means and SVM algorithms for accurate filtering of eye-blink arti-factual IC without any loss of neural information. Furthermore, the SVM based classifier developed with two simple time domain features showed accuracy greater than 99% in the detection of eye-blink artifacts ICs. Performance of the proposed method is evaluated on one synthetic and two real PPG datasets under different PPG channels setting. Results show that unlike existing methods, the performance of proposed method in terms of mean RRMSE and CC in time domain and the mean PLV in the frequency band $1 - 8H z$ is consistent for different number of PPG channels setting.

REFRENCES

1. Yarrabothu, R. S., & Thota, B. (2015). Abhaya: An Android App for the safety of women. Annual IEEE India Conference (INDICON), ISSN: 2325-9418.

2. Harini, R., & Hemashree, P. (2019). Android App for Women Security Application. International Journal of Computer Science and Mobile Computing, 8(10), 54-59.

3. Nirmalrani, V., Saravanan, P., & Kalpana, S. (n.d.). SheSecure Safety App- The Hexa Umbilical Cord, 5.

4. Mandapati, S., Pamidi, S., & Ambati, S. (2015). A Mobile Based Women Safety (I Safe Apps). IOSR Journal of Computer Engineering (IOSR-JCE), 17(1), 29-34.

5. Pawar, V., Wankhade, N. R., Nikam, D., Jadhav, K., & Pathak, N. (2014). SCIWARS Android App for Women Safety. International Journal of Engineering Research and Applications, 4(3), 823-826.

6. Mane, I. A., Babar, J. R., Patil, S. S., Pol, S. D., & Shetty, N. R. (2016). Stay Safe. International Research Journal of Engineering and Technology (IRJET), 3(5), 2455-0056.

7. Naik, Y., Vagga, V. K. K., & Deepa, S. (2016). Sthree Raksha -An Android App. International Journal of Recent Trends in Engineering & Research (IJRTER), 2(10), ISSN: 2455-1457.

8. Singh, N., Pawar, H., Rukari, S., Raut, S., & Jadhav, B. V. (2018). Self Defence Application for Women Safety with Location Tracking and SMS Alerting. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 6(2), ISSN: 2321-9653.

How to cite this article:
Dr P Pandiselvi, S Gobika, “Evaluation of PPG feature values toward biometric authentication against presentation attacks”, International Journal of Intelligent Computing and Technology (IJICT), Vol.6, Iss.2, pp.1-7, 2023