electronics

MDPI

Article

Auditory Perception Based Anti-Spoofing System for Human Age Verification

Muhammad Ilyas, Alice Othmani, Régis Fournier and Amine Nait-ali *

LISSI, Université Paris-Est, UPEC, 94400 Vitry sur Seine, France; ilyaskhantmg@hotmail.com (M.I.); Alice.othmani@u-pec.fr (A.O.); rfournier@u-pec.fr (R.F.)

* Correspondence: naitali@u-pec.fr

Received: 27 September 2019; Accepted: 5 November 2019; Published: 8 November 2019

Abstract: Biometric systems are considered an efficient component for identification in the developing modern technologies. The aim of biometric systems is to verify or determine the identity of a user through his/her biological and behavioral characteristics. The threat of spoof attacks is always an important issue in biometric verification and authentication, which requires an updated and stronger protection system. In this article, we propose an anti-spoofing system based on auditory perception responses. To the best of our knowledge, this is the first time that an auditory perception based anti-spoofing system has been presented for age verification. The proposed auditory perception based anti-spoofing system was evaluated with 770 trials conducted by many subjects of each gender and age range (12–65 years of age). The results achieved are encouraging, as the auditory perception based system showed the lowest Equal Error Rate (EER) value of 5.5%.

Keywords: auditory perception; anti-spoofing measure; biometrics; forensics age estimation

1. Introduction

Biometric systems allow us to identify a person and provide authentication based on an identifiable and verifiable dataset, which is uniquely specific to the person. It can be used for surveillance, access control, and security systems [1]. Due to scientific growth and technological advancement, in the fields of pattern recognition, computer vision, machine learning, data storage, data processing, and data acquisition, it is now very much possible to identify and verify a subject. Several biometric modalities such as face, iris, fingerprint, veins, blood flow, and auditory perception can successfully allow a subject's identification and authentication. In parallel, several spoofing techniques have also been introduced to crack such biometric systems.

In the present era, the threat of malicious actions is among the major challenges that biometric systems confront. The main type of malicious action uses a conventional type of attack, known as "spoofing", to trick a biometric system. Biometric spoofing is a technique to deceive a biometric system. In this technique, a false object such as a fingerprint mold made of artificial material that copies the unique biological features of a subject is presented to the biometric scanning tool. The system computes the features in a manner that the biometric system will otherwise not be able to recognize the artifact from the genuine biological target. Therefore, the aim of spoofing a biometric system is to present the spoof attacker as a real user by producing a fake identity to fool the biometric sensors. Anti-spoofing systems thus are required in order to reject the spoofing attacks [2]. Biometric systems without an anti-spoofing system pose a greater threat to the security of users' data [3,4]. In previous studies, eight different points have been highlighted regarding spoofing attacks [5,6], and they are categorized into two major groups such as direct attacks and indirect attacks.

Direct attacks [6] are possible by generating synthetic samples, and this is the first unsafe point at the sensor level of a biometric security system. For direct attacks, no particular information is needed

about the system such as the matching algorithm, feature extraction, the format of data, etc. It works in the analog domain, outside of the digital boundary of the system. Therefore, digital protection techniques like digital signatures and watermarking are not useful. For direct spoofing, the attacker targets the sensors typically. Several biometric modalities can be constructed by using common types of equipment to copy actual biometric readings such as printers, audio recorders, and stampers. As concerns that, the biometrics community has proposed spoofing benchmarks. Benchmarks allow the biometric systems to work on the concepts of anti-spoofing systems. For example, face, iris, and fingerprint are some important modalities for which spoofing detection has been investigated. Each of them shares a common characteristic for benchmarks such as video based or images. For iris, spoofing attacks usually occur with printed iris images [7] or cosmetic contact lenses [8–10]. For faces, a digital video or photograph can be used for a spoof attack [11]. A 3D mask is also a logical option for a face spoof attacker [12]. However, for fingerprints, artificial replicas are modeled in a supportive way for spoofing [13]. A mold of the fingerprint of an authentic user can also duplicate the real user in a specific material such as silicon, play dough, gelatin, etc.

Indirect attacks require all the information and knowledge about the system to trick it. In order to manipulate a biometric system, indirect attacks require knowledge about specific feature extraction procedures, the matching algorithm used, possible weak links in the communication channel, and database access. In a biometric system, indirect attacks are like bypassing the feature extractor or the comparator, manipulating the biometric references in the biometric reference database, by taking advantage of the weak points in the potential interaction channel [14]. The security of a biometric system depends on information regarding data acquisition in a secure environment. Even a small modification in the system needs to reconstruct the whole system from scratch.

Threats to biometric system regarding spoofing attacks are now acknowledged by researcher. However, the anti-spoofing systems are still facing challenges to handle spoof attackers. They can minimize the chances of spoofing, but they can also end up rejecting access to genuine subjects. In the future, anti-spoofing systems will require more intensive study and attention.

Human age estimation and classification based on auditory perception responses were presented for the first time in 2017. In this article, we present an anti-spoofing system for a pre-existing biometric system for age estimation and classification based on auditory perception [15].

The article is organized as follows: In Section 2, several anti-spoofing systems based on different biometric traits are discussed. In Section 3, we describe auditory perception based on the human age estimation/classification system and its potential vulnerabilities to spoofing. The anti-spoofing system based on auditory perception responses is explained in Section 4. The performance and evaluation methodology of the anti-spoofing system will be discussed in Section 5. A summary of our proposed methods is presented in Section 6, while the work will be concluded in Section 7, together with some ideas for future research.

2. Related Work

In this section, a review about anti-spoofing systems is given for different biometric modalities.

2.1. Fingerprint

In the modern authentication and verification systems, spoof attacks are highly observed, using several kinds of materials such as wood glue, printed fingerprints, gelatin, and silicone [16]. For a specific spoofing technique, a special anti-spoofing system is designed that cannot be used globally. Dubey et al. [17] proposed a method of combining multiple techniques for feature extraction such as the SURF method for the detection of the local point of interest, the pyramid multi-scale characteristic of the Histogram of Oriented Gradients (HOG), and the Gabor texture characteristic. They combined all the characteristics to identify the spoof and separate it from genuine subjects. This technique was tested in fingerprint Liveness Detection competition (LivDet2011)and an Average Equal Error Rate (AEER) of 3.95% was achieved, while the Average Classification Error Rate (ACER) was 2.27%.

Rattani et al. [18] also presented a fusion of features (a Histogram of Oriented Gradients (HOG) and Grey Level Co-occurrence Matrix (GLCM)) based system for liveness detection by using different materials and a material detection scheme, which obtained an average correct detection rate up to 74%. Recently, researchers have been inspired by some techniques based on deep learning feature extraction (e.g., Convolution Neural Network (CNN)) to propose more precise methods for the detection of spoof attackers [19].

2.2. Iris

Iris recognition/verification has gathered significant attention due to its well established architecture, with high precision and operational performance. The viability of spoofing attacks was recognized for the first time by Daugman [20]. He used fast Fourier transform for the verification of high frequency spectral measures inside the frequency domain. In the literature, several solutions are available to detect the liveness of iris, which rely on special acquisition hardware [21–23], as well as software based solutions that use the pattern of someone's iris on contact lenses to analyze the textural effects of the spoof attacker [24]. Software based solutions have also investigated pupil construction [25], cosmetic contact lenses [8,26,27], and multiple biometrics, EEG and iris together [28].

Hsieh et al. [29] used a system for the detection of spoof attacks of subjects having Cosmetic Contact Lenses (CCL). They used a spectral imaging system to capture the iris images of the subjects wearing CCL. By using the technique of independent component analysis, they achieved promising results with the value of the false rejection rate from 10.52% to 0.57%.

For image quality measures such as motion, occlusion, focus, and pupil dilation, 22 images were used by Galbally et al. [30]. Sequential floating feature selection was used for the best features' selection and then forwarded to a quadratic discriminant classifier [31]. To analyze pattern regularities in irises, some peak values inside the frequency spectrum are a concern with respect to spoof attackers. Iris anti-spoofing methods investigate strong features through texture patterns, bags of visual words, and image quality metrics. A strong variation has been found from dataset to dataset concerning the performances [2] and has shown an accuracy of 99.84%.

2.3. Face

The face based anti-spoofing techniques are categorized into four different groups [32] such as user behavior modeling, data driven characterization methods, relying on user corporation, and relying on extra devices. Users' behavior modeling concerns the behavior of a user in front of the camera, and some researchers considered motion detection such as the unintentional movement of different parts of the head and face [33,34] and eye blinking [35]. These methods rely on extra devices such as allowing a user to utilize specific anti-spoof hardware, and thermal or infrared images could be deployed [36]. Multiple 2D cameras or 3D cameras have been used, which can also provide additional protection [37]. The physical characteristics of materials relating to their unique reflective qualities have also been presented as a measure of distinction between a real face and a printed face on paper as a 2D image. Polarized light (light that vibrates in one direction) can be utilized to distinguish reflections. Stokes' parameters have been applied to generate Stokes images, which have then been utilized to create the final picture, known as the Stokes Degree of Linear Polarization (SDOLP). Statistically, the strength of an SDOLP image has been studied, and promising results have been demonstrated between skin and a paper mask in the material classification [38].

From many decades, people have been wearing masks or facial disguises so as not to be identified. In the present era, the use of plastic surgery is a newer trend to modify one's appearance. The procedure of plastic surgery is performed because of its cost and time effectiveness to achieve perfection. Despite all this, recently, a robust algorithm was designed to detect the facial surgery changes [39–41]. However, the problem of face recognition after going through an operation of plastic surgery is still a challenging task [42]. Even without going through a permanent treatment, temporary make-up can also affect the efficiency of a face based biometric system [37]. Adaptive Gradient Location and Orientation

Histogram (AGLOH) based extraction features have also been introduced for successful plastic surgery face recognition. The features indicated have been omitted from the granular region of the face [43]. All the above techniques mentioned such as face masks, make-up, and plastic surgery are used to hide the identity of a person. Adults try to impersonate a child; males can try to impersonate females, etc. It has also been demonstrated that a female intruder can impersonate a male successfully by wearing some make-up [44].

2.4. Gait

For gait recognition, spoof attacks have not been studied as intensively as needed. High quality video of a legitimate volunteer replayed in front of the camera can affect the system. Gait is a behavioral trait, and it may not remain the same, especially over a longer period of time, due to changes in body weight, and particular injuries [7]. Synthetic attacks cannot affect the performance of gait biometrics.

Meanwhile, four different spoofing mechanisms have been explored. The gait motion has been captured through an accelerometer sensor, which provided the gait signature. Traditional approaches such as a vision based gait recognition system have more potential and are more practical compared to a sensor based approach.

The first spoofing attack for gait signature is that an individual can walk behind the genuine target by copying his/her moves. This kind of spoofing can be identified as a spoofing attempt that has a lower match score in comparison to the genuine gait. The second spoofing attack is related to the reaction of an accelerometer sensor connected to the leg, which is projected on a wall. A spoof attacker can visualize and try to match the moves of the target, and this is used for identification. This technique has an accuracy of 60% to trick the gait biometric system. For the third spoofing attack, an accelerometer is used like the previous approach and focused on one's performance achieved via practice. Only those spoof attackers were found to be successful that were closely matched to the genuine signature gait of the target, and with practice, the performance of the signature gait can affect the system. The fourth study showed how a an attacker impersonated the clothing of a genuine subject to trick the gait recognition system. It is among one of the most straightforward and robust methods used for spoofing. It was used to enter a secure environment where formal types of dress or uniforms are common. Impersonation of clothes is also one of the most efficient techniques used to spoof gait signature [45].

Using targeted attacks and clothing impersonation can trick a gait recognition system. No artificial detection exists for such kinds of attacks, and this is especially extremely challenging.

2.5. Multimodal

Multimodal biometrics can also be defined as a fusion of a matcher and liveness detector or multiple biometric systems without liveness detection [46]. Multimodal biometric systems are considered more secure as compared to unimodal systems by making it difficult for the intruder to spoof the trait of a genuine subject [47]. Ricardo et al. [48] considered a biometric system combining face and fingerprint modalities, and the likelihood rate and weighted sum were used as score fusion rules. The performance evaluation results showed a lower value of false acceptance rate (4.33% and 4.71%).

An anti-spoofing system extracted different kinds of features for each biometric trait. Ridgelets was used to extract features from the face, while from fingerprint Level 1 such as local orientation and frequencies and Level 2 (minutiae) extracted the required characteristics. The local ternary pattern was calculated for iris. Finally, all the features were fused and fed to the classifier for classification. A multimodal biometric system with the fusion of three biometric modalities (face, fingerprint, and iris) was also designed based on a convolutional neural network with promising results [49].

For all biometric modalities such as iris, face, gait, etc., there are spoofing detection methods. All the existing systems are based on a deep feature extraction and provide a solid direction that allows

us to develop a more efficient anti-spoofing system. In this paper, we present an anti-spoofing system for auditory based human age estimation and classification.

3. Age Estimation Using Auditory Perception and Its Potential Vulnerabilities

In this section, we will explain the mechanism of the existing system for human age estimation using auditory perception and its vulnerability to spoof attacks.

3.1. Age Estimation Based on Auditory Perception

The ability of a human to receive and interpret different sounds that reach the ears or the human auditory system through audible frequency waves transmitted through air or other means is known as auditory perception [50]. Auditory perception has a high correlation with human age. The auditory perception response varies with age; for example, as age increases, the highest audible range of frequency decreases. The decrease in the highest audible frequency leads to hearing loss.

The flowchart of the proposed auditory perception based age estimation and classification approach is shown in Figure 1. First, the auditory system is stimulated via dynamic frequency sound waves. The audible frequencies are registered and utilized for age estimation of a person. After, the responses of the auditory perception are registered in a dataset to analyze the separability between the different age groups, to classify the perceived responses into an age group, and estimate the age of the subject.

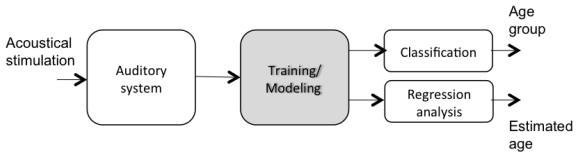

Figure 1. Flowchart of the proposed auditory perception based age classification and estimation approaches.

3.2. Protocol of Stimulation

By generating dynamic frequency sound waves, the human auditory system is stimulated according to the following model:

$$\begin{aligned} x(t) &= A_0.sin(2\pi.\phi(t).t), \\ where \phi(t) &= \alpha.t + \phi_0, \end{aligned} \tag{1}$$

A_0 stands for the sound amplitude, t for time, ϕ_0 the initial frequency, and α the speed of frequency.

The dynamic frequency sound is generated according to proposed Formula (1) with the time duration of t = 20 s. A test subject has to interact with the system in real time. The subject should respond when he/she stops hearing the sound for the first test and respond while he/she starts hearing the sound for the second test. The subject should conduct two tests:

- First test: The sound is generated from lower frequency (20 Hz) to higher frequency (20,000 Hz). The subject can complete the first test (e.g., keyboard action) once the subject is unable to detect the sound,
- Second test: The second test starts automatically. In this case, the sound is generated from higher frequency (20,000 Hz) to lower frequency (20 Hz). The subject can complete the second test (e.g., keyboard action) once the subject starts detecting the sound.

Both frequencies are registered in a database, and the system then calculates the mean of the two frequencies (first test frequency and second test frequency). The three frequencies are the feature vectors, which are used to describe the response of auditory perception for every test subject. While performing this experiment, two objectives were achieved:

- Human age classification using auditory perception
- Human age estimation using auditory perception.

Human age estimation and classification was achieved by using the random forest regression and classification model [51].

3.3. Performance and Vulnerabilities to Spoofing

In this section, the performance of human age estimation and classification is briefly explained along with the vulnerability of the system to spoof attacks. The proposed approach of human age classification based on auditory perception showed a good classification rate of 92% and 86% for three to five age groups, respectively. A robust regression model was also designed for human age estimation, and it had a root mean square of error value of 2.6 years.

The auditory perception-based system for age estimation and classification showed promising results. Although it was very sensitive to spoof attacks, a subject could easily fool the system with respect to age. Two scenarios exist to trick the system:

- An old subject can impersonate a young one just by finishing the experiment with a high frequency in the first test and respond after some seconds as the second test of the experiment.
- A young subject can impersonate an old one by finishing the first test with lower frequency and respond with a higher delay for the second test.

To check the vulnerability of the auditory perception based system for human age estimation and classification, it was tested under two scenarios:

- The licit scenario for evaluating the baseline performance (no spoof attacks and no anti-spoofing system) utilizing genuine and zero-effort imposter trials.
- The spoof scenario for evaluating the baseline performance of the same system under spoof attack.

The comparison of the human age estimation system under the licit scenario and spoof scenario is shown in Figure 2. The efficiency of a biometric system can be evaluated by calculating the Equal Error Rate (EER). The lower value of ERR indicates the higher accuracy of the biometric system, while a higher value of EER indicates worse performance. The EER value for the human age estimation system under the licit scenario was nearly 2%, while under the spoof scenario, it increased to 60%. We concluded that the existing system for human age estimation was vulnerable to spoofing and required a strong anti-spoofing system to overcome this challenge.

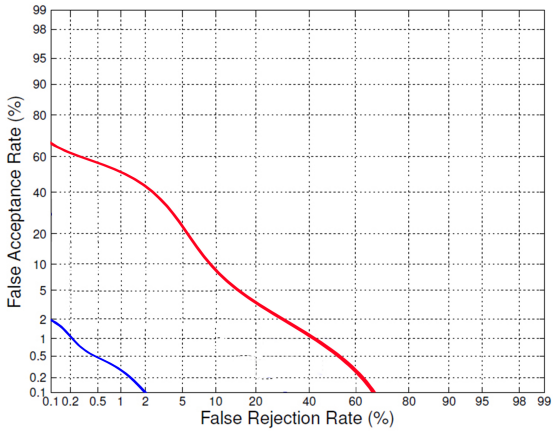

Figure 2. Licit scenario vs. spoof scenario of the biometric system for auditory based human age estimation.

4. Proposed Anti-Spoofing System

The biometric system for age estimation and classification based on auditory perception was vulnerable and easy to spoof, as briefly explained in Section 3. Therefore, we present an anti-spoofing system based on auditory perception responses, and the flowchart of the proposed system is shown in Figure 3.

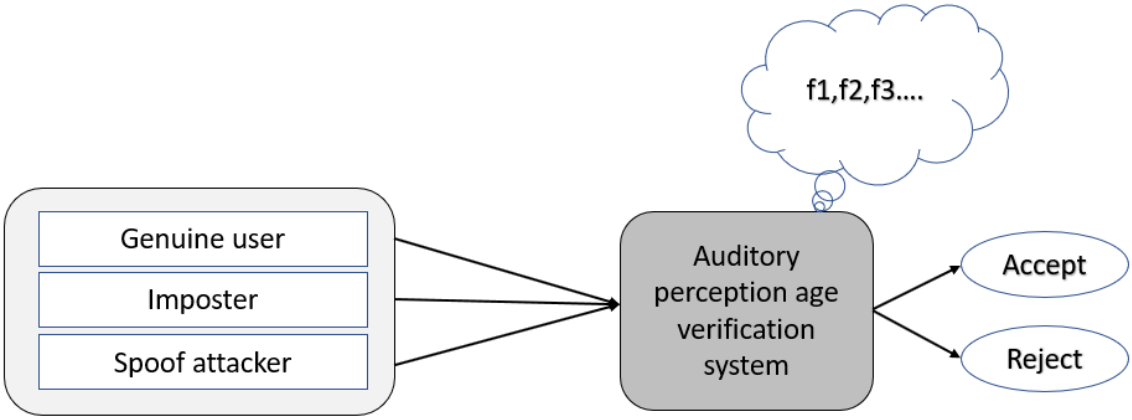

Figure 3. Auditory perception based anti-spoofing system.

Experimental design: a test subject was required to take the test for age estimation using auditory perception, as shown in Figure 1. As the auditory perception based system estimated the age, our proposed anti-spoofing system would verify the age of the test subject. A system was designed to generate ten random frequencies of sound according to our standard database by taking the estimated age of the subject as an input. Among these ten sound frequencies, some were audible and some were inaudible for the test subject. To make it more secure against spoofing attacks, some of the audible frequencies were repeated to ensure that the test subject provided the same feedback. According to our previous study, the minimum and the maximum values of audible and inaudible sound frequencies for each age were assigned from a reference database. It was hard for a spoof attacker to guess the audible and inaudible sound frequencies in the set of generated sound frequencies. Every feedback for each generated sound frequency had a value of $1/b$ to calculate the final score, where b is the total number of randomly generated sound frequencies, as shown in Algorithm 1. The final score must be greater than a decision threshold τ to prove that the subject is genuine and verify the input age.

The value of decision threshold τ was chosen according to the evaluation standards given by:

$$\tau^*_{EER} = arg.min|FAR(\tau, D_{dev}) - FRR(\tau, D_{dev})| \quad (2)$$

Here, the decision threshold τ was set in order to equalize the False Rejection Rate (FRR) and the False Acceptance Rate (FAR). FRR is defined as the ratio of the number of false rejections divided by the number of verification attempts; while FAR is defined as the ratio of the number of false acceptances divided by the number of verification attempts. The baseline performance of the algorithm can also be illustrated as a function of the decision threshold τ_{EER}.

As FRR and FAR are inversely related, the decision threshold can be fixed to equalize the ratio of FAR and FRR. Therefore, the a posteriori performance criterion to minimize can be the value of the Half Total Error Rate (HTER):

$$\tau^*_{EER} = argmin.HTER(\tau, D_{dev}) \quad (3)$$

$$HTER(\tau, D_{dev}) = \frac{FRR(\tau, D_{dev}) + FRR(\tau, D_{dev})}{2}) \quad (4)$$

D_{dev} is the development dataset used to determine the decision threshold by using the proposed anti-spoofing system. More details about the algorithm are given in Algorithm 1.

Algorithm 1 Auditory perception based anti-spoofing system for age estimation system.

procedure OUTPUT: AGE VERIFICATION
  a = *real-age*,
  b = *nbr-freq*,
  c = *nbr-random-hearable-freq*,
  d =*nbr-repetition-hearable-freq*,
  Input: *a*, *b*, *c*, *d*, *e*(τ_{EER})
  a ← *insert()*
  F3, *F4* = [*min-f(a)*, *max-f(a)*]
  F1, *F2* = [*min-f(a)*, *max-f(a)*]
  TAB : *rand-f(b)*
  for *i* = *1*:*b* **do**
    TAB[i] = 0
  end for
  hearable-indices [ ] ← *c*
  for *i* = *1*:*length(hearable-indices)* **do**
    TAB[hearable-indices(i)] = (F1,F2)
  end for
  for *i* = *1*:*d)* **do**
    d ← *rand[ ]*
    d = TAB[position]
  end for
  for *i* = *1*:*b)* **do**
    if *TAB[i]* $\neq$ 0
    TAB[i] = (F3,F4)
    endif
  end for
  for *i* = *1*:*b* **do**
    play sound(<TAB[i])
    user feedback[i] ← *ask user feedback* >
  end for
  nbr-correct-answers ← *check user feedback(user-feedback[])*
  if *(nbr-correct-answers*$\geq \tau_{EER}$):
  verified-age ← True
  else
  verified-age ← False
  end
end procedure

5. Experiments and Results

In this section, we will discuss the dataset collected for decision threshold optimization and the dataset for testing the anti-spoofing system with the standard value of the decision threshold.

5.1. Datasets Collection

We developed two datasets as shown in Table 1 under two different scenarios, the licit scenario and the spoof scenario, by using Algorithm 1:

The development dataset was utilized to decide the optimization point of the threshold for efficient performance at a specific operational value. The total number of trials for the development dataset was 360, for both genders (male and female).

The anti-spoofing dataset was used to assess the vulnerability of the proposed anti-spoofing system with the required threshold τ value, and 410 trials were conducted for the anti-spoofing dataset.

Table 1. Datasets collected for different scenarios.

Datasets	**Development Dataset**		**Anti-Spoofing Dataset**	
Gender	Male	Female	Male	Female
Licit Scenario	200	80	220	108
Spoofing Scenario	60	20	60	22
Total trials	360		410	

5.2. Decision Threshold Optimization

The development dataset was utilized for optimization of the decision threshold. The performance of the anti-spoofing system was assessed on a licit scenario with genuine and zero-effort imposter trials. The function of the decision threshold (τ) is illustrated in Table 2, and the best threshold that minimized the HTER was set to 80% of all the experiments. As the number of repetitions or experiments was fixed in this work to ten, imposter trials correlating to a score a little higher than eight trials would be misclassified as genuine trials, such that the genuine trials with correct answers fewer than eight trials would be misclassified as imposter trials. The score distribution for the licit scenario is illustrated in Figure 4; still, a small overlap existed between the distribution of genuine and imposter trials. The x-axis determines the value of decision threshold τ, and the y-axis shows the number of trials of the subjects. During the process of decision threshold optimization, the FAR value was higher for the initial values of $\tau = 10\%, 20\%, 30\%, 40\%, 50\%, 60\%$. Thus, the system would not make many errors in distinguishing between genuine and spoof attackers. The behavior of the system for varying decision threshold τ showed a continuous effect in the performance of the anti-spoofing system. The decision threshold τ at 80% showed the minimum misclassification of imposter trials as genuine. The efficiency of the proposed anti-spoofing system could be demonstrated with the Detection Error Trade-off (DET) profile, as shown in Figure 5. Under the licit scenario, the EER value was 2.2% for our proposed anti-spoofing system.

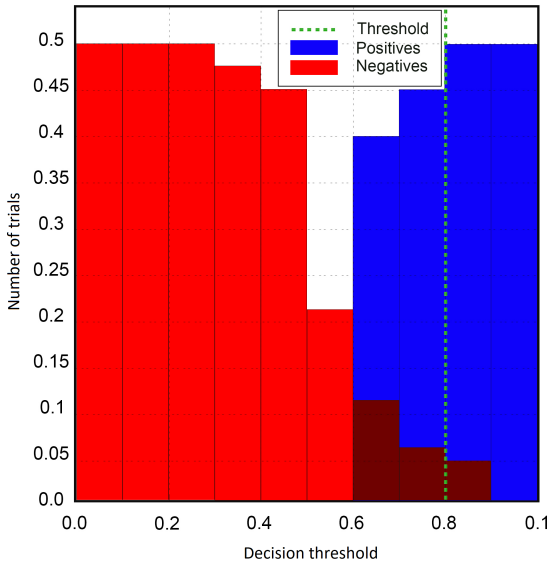

Figure 4. Genuine users' and zero-effort imposters' score distribution while a decision threshold τ was determined with a vertically drawn dashed line, while the x-axis represents the value of decision threshold τ, and the y-axis represents the number of trials.

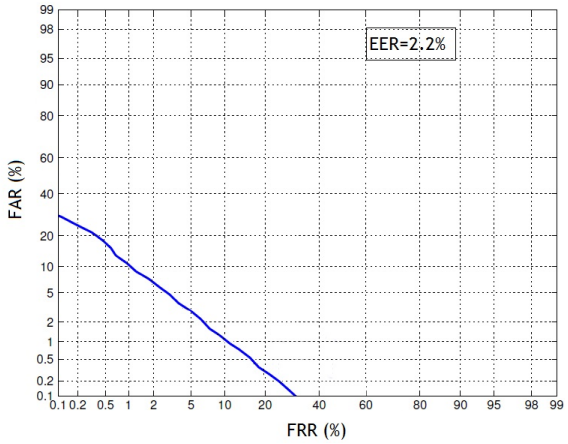

Figure 5. Detection of Error Trade-off (DET) plot showing an Equal Error Rate (EER) of 2.2%. FFR, False Fake Rate; FLR, False Living Rate.

Table 2. Optimization for the decision threshold (τ) for auditory perception. HTER, Half Total Error Rate.

Decision Threshold (τ)	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
FAR	100%	100%	100%	94%	91%	42%	13%	6.8%	5.7%	0%
FRR	0%	0%	0%	5.7%	8.5%	8.5%	3.4%	4.6%	20.5%	25.7%
FAR-FRR	100%	100%	100%	88.3%	82.5%	33.5%	9.6%	2.2%	14.8%	25.7%
HTER	50%	50%	50%	49.4%	49.75%	25.25%	16.4%	5.7%	23.35	12.8

5.3. Performance Evaluation of the Anti-Spoofing System

In the field of biometrics, we consider a binary classification to distinguish genuine and spoof trials. Like other biometric systems, this also gave rise to two other kinds of errors, False Fake Rate (FFR) and False Living Rate (FLR). FFR represents the value of genuine trials misclassified as spoofed trials, while FLR represents the value of spoofed trials misclassified as genuine trials.

In Figure 6, each profile represents a specific configuration profile according to the baseline approach. The blue profile (first line from the bottom) shows the baseline performance (auditory perception based age estimation) of the biometric system under the licit scenario (genuine trials). The black profile (the highest line) shows the efficiency of the system while having the same configuration of the baseline under the spoofing scenario. The cyan profile (second from highest) shows the performance of the baseline system under the licit scenario with zero-effort imposters. The red profile (second from bottom) shows the performance of the baseline system, equipped with auditory perception based anti-spoofing under spoofing attack. In order to quantify how many genuine users were misclassified as spoof attackers and to recapitulate all of the above configurations, we needed to study the system under a complex contact of the integrated system with a spoofing attack.

The overall efficiency of a biometric system is the main concern, and there is always an assessment of unconventional performance. The first configuration (blue line) was specified as the baseline configuration, while the forth configuration (black line) was simple with no anti-spoofing system and open to spoof attacks. A separate configuration needed to be applied which can support the licit scenario under spoof attack. However, the third configuration (cyan line) was the baseline system with zero-effort imposters (attackers with no spoofing background). The second configuration (red line) allowed the system to stay secure under spoof attack and could be evaluated for overall performance.

Hence, the value of FLR/FFR can decide the overall efficiency of a biometric system under the required conditions. The performance depends on the requirement and security of the system such that for some applications, FLR is more important than FRR and vice versa. The EER value for the baseline under the licit scenario, the baseline under the licit scenario with zero-effort imposters, the baseline under spoof attacks, and the baseline with anti-spoofing system was 2.7%, 43%, 60%, and 5.5%, respectively. These results demonstrated that the anti-spoofing system based on auditory perception showed promising accuracy for age verification.

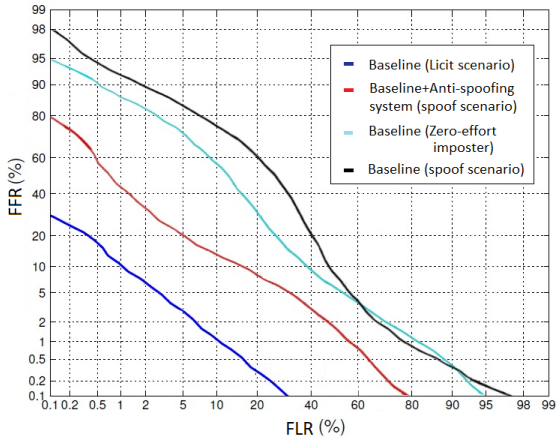

Figure 6. False Fake Rate (FFR) and False Living Rate (FLR) of the proposed biometric system with/without spoof-attack.

5.4. Vulnerabilities to the Proposed Anti-Spoofing System

The performance of the anti-spoofing system based on auditory perception was evaluated with the spoofing scenario such that the subset of zero-effort imposters was replaced by spoofed trials. It can be illustrated from the score distribution that the overlap between spoofed trials and genuine was greater than imposter and genuine trials.

The vulnerability of the system was quantitatively measured and expressed in terms of Spoof False Acceptance Rate (SFAR). SFAR is the percentage value of the spoofed trials that are classified as genuine for a given decision threshold τ. An example is presented in Figure 7, which shows the score distributions for subjects of genuine, impostor, and spoofed trials. It can briefly illustrate the SFAR profile with a threshold function τ. The difference among the impostor and spoofed trial distributions showed the potential impact of spoofing on the quality of biometric verification, and the correlation of genuine and spoofed trial score distributions was significantly greater than that of genuine and impostor distributions. In Figure 8, the DET plot presents both the spoof (SFAR vs. FRR) and licit (FAR vs. FRR) scenarios. Expressing the vulnerability at a certain point is very important; thus, the EER for SFAR and FAR for a common FRR is shown in Figure 8. The FAR under the licit scenario was 2.3% for a baseline system, while SFAR was 5.5% under the spoof scenario, which means there was a chance for nearly five trials to be misclassified among one hundred trials. The results showed that our proposed anti-spoofing system was highly secure and that it was difficult for a spoof attacker to deceive this system.

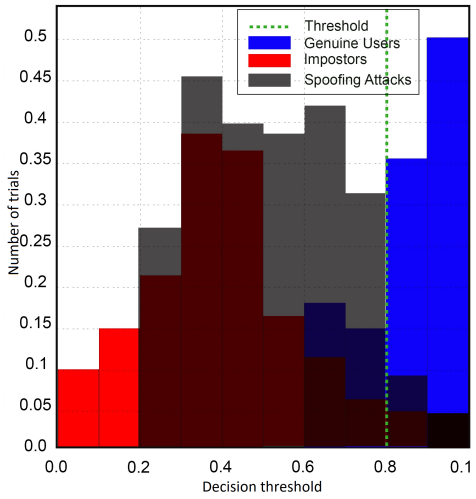

Figure 7. Score distributions of zero-effort imposters, genuine, and spoof attackers with the spoof false acceptance rate; the the x-axis represents the value of decision threshold τ, and the y-axis represents the number of trials.

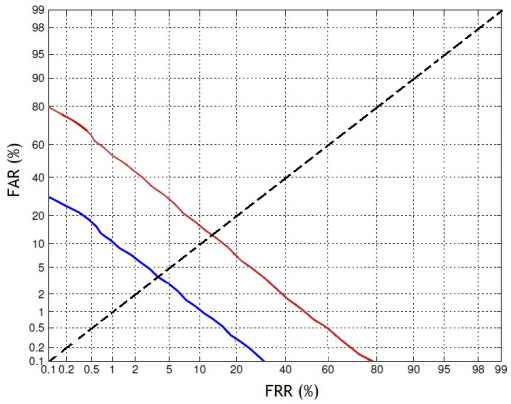

Figure 8. DET determines the Spoof False Acceptance Rate (SFAR); EER on the decision threshold τ illustrated from the development dataset.

6. Summary

The performance evaluation methods presented in this article were based on standard methodologies existing in the state-of-the-art for anti-spoofing systems. In this study, we presented techniques to secure our existing system for human age estimation using auditory perception considering its vulnerability to spoofing.

Baseline system: Human age estimation based on auditory perception responses was presented as the baseline. This baseline system was tested under different scenarios (licit scenario and spoof scenario) to demonstrate its vulnerability to spoofing.

Anti-spoofing system: The proposed anti-spoofing model based on auditory perception consisted of a feature vector that was created as a result of generating different sound frequencies, audible and inaudible. From the feature vector, the value of the decision threshold ($\tau = 80\%$) was calculated for age verification. For global model adaptation, the system was trained in real time with genuine, imposter, and spoof trials. The performance of the system was achieved by observation of the global model against spoofing trials with the predefined decision threshold τ.

Vulnerability: As our purposed anti-spoofing system was well equipped with a solid design, every biometric system shows a weakness for spoof attacks. Although some biometric modalities such as gait, fingerprints, etc., claim more secure behavior as compared to other biometric systems, that does not mean these approaches are reliable in the presence of spoof attackers. Thus, in this article, we also presented a secure anti-spoofing approach, which can be used for other biometric modalities.

Usability: The anti-spoofing system based on auditory perception was easy to use and was more secure as compared to the existing approaches. This depends on the requirement of the system, e.g., some systems are highly secure and accept a higher value of FRR as compared to FAR. Our proposed system is easy to optimize according to the requirements of biometric systems. The anti-spoofing system has not yet been implemented in real-time applications and requires more time for testing.

7. Conclusions and Future Work

For the first time, we demonstrated successfully in 2017 that human age can be estimated using auditory perception responses. As our proposed system for age estimation was working in real-time, it was identified as vulnerable to spoof attacks. For example, an adult can easily fool the system to impersonate himself/herself as a child or a child can impersonate himself/herself as an adult. Hence, we felt the need for an anti-spoofing system to secure the system against spoof attacks.

Until now, all the biometric systems have been facing the mutual issue of spoof attacks. In this article, we introduced an anti-spoofing system based on auditory perception with promising knowledge and a standardized evaluation method. Our proposed anti-spoofing system was tested in real time by different volunteers of different ages and genders. We concluded that our proposed anti-spoofing system was robust by having an EER value of 5.5% under the spoofing scenario. This position contributes to a range of forward-looking study strategies, including merged countermeasures and classification techniques. As it is a new trait, more challenging systems are needed to keep biometric systems safe from spoof attackers. However, it is hard to estimate the effectiveness of an anti-spoofing system without implementing it in a critical situation. This includes not only the capacity to identify spoof attacks, but also the effect on the suitability of the model.

As future work, we are planning to test our proposed anti-spoofing system under different scenarios to enhance its performance. We will also implement our system with other biometric modalities such as face, gait, hand, etc., as a multimodal anti-spoofing system to enhance the performance of age verification systems. We are also planning to test the compatibility of the proposed anti-spoofing system with other biometric traits for age verification in real time.

Author Contributions: Conceptualization, A.N.-a.; Data curation, M.I.; Methodology, A.O.; Resources, M.I.; Visualization, M.I.; Writing—original draft, M.I.; Co-supervision, R.F.; Supervision, A.N.-a.

Funding: This research received no external funding.

Acknowledgments: We thank Hina Rehman for assisting us in database collection.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Reid, D.A.; Samangooei, S.; Chen, C.; Nixon, M.S.; Ross, A. Soft biometrics for surveillance: An overview. In *Handbook of Statistics*; Elsevier: Salt Lake City, UT, USA, 2013; Volume 31, pp. 327–352.
2. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.R.; Pedrini, H.; Falcao, A.X.; Rocha, A. Deep representations for iris, face, and fingerprint spoofing detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 864–879. [CrossRef]
3. Rathgeb, C.; Uhl, A. Attacking iris recognition: An efficient hillclimbing technique. In Proceedings of the IEEE/IAPR International Conference on Pattern Recognition (ICPR), Istanbul, Turkey, 23–26 August 2010; pp. 1217–1220.
4. Christian, R.; Uhl, A. Statistical attack against iris-biometric fuzzy commitment schemes. In Proceedings of the CVPR 2011 WORKSHOPS, Colorado Springs, CO, USA, 20–25 June 2011; pp. 23–30.

5. Galbally, J.; Fierrez, J.; Ortega-garcia, J. Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection. *Database* **2007**, *1*, 1–8.
6. Ratha, N.K.; Connell, J.H.; Bolle, R.M. An analysis of minutiae matching strength. In Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication, Halmstad, Sweden, 6–8 June 2001; pp. 223–228.
7. Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 4–20. [CrossRef]
8. Bowyer, K.W.; Doyle, J.S. Cosmetic contact lenses and iris recognition spoofing. *Computer* **2014**, *47*, 96–98.
9. Yadav, D.; Kohli, N.; Doyle, J.; Singh, R.; Vatsa, M.; Bowyer, K. Unraveling the effect of textured contact lenses on iris recognition. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 851–862. [CrossRef]
10. Yambay, D.; Becker, B.; Kohli, N.; Yadav, D.; Czajka, A.; Bowyer, K.W.; Schuckers, S.; Singh, R.; Vatsa, M.; Noore, A. LivDet iris 2017—Iris liveness detection competition 2017. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 1–4 October 2017; pp. 733–741.
11. Chingovska, I.; Anjos, A.; Marcel, S. On the effectiveness of local binary patterns in face anti-spoofing. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; pp. 1–7.
12. Erdogmus, N.; Marcel, S. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In Proceedings of the IEEE International Conference on Biometrics: Theory Applications and Systems (VISAPP), Arlington, VA, USA, 29 September–2 October 2013; pp. 1–6.
13. Ghiani, L.; Yambay, D.; Mura, V.; Tocco, S.; Marcialis, G.; Roli, F.; Schuckcrs, S. Livdet 2013—Fingerprint liveness detection competition. In Proceedings of the International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–6.
14. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634. [CrossRef]
15. Ilyas, M.; Othmani, A.; Nait-Ali, A. Human age estimation using auditory system through dynamic frequency sound. In Proceedings of the International Conference on Bio-Engineering for Smart Technologies (BioSMART), Paris, France, 30 August–1 September 2017; pp. 1–3.
16. Marasco, E.; Ross, A. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Comput. Surv. (CSUR)* **2015**, *47*, 28. [CrossRef]
17. Dubey, R.K.; Goh, J. Thing, Fingerprint liveness detection from single image using low-level features and shape analysis. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1461–1475. [CrossRef]
18. Rattani, R. Automatic adaptation of fingerprint liveness detector to new spoof materials. In Proceedings of the IEEE International Joint Conference on Biometrics, Florida, USA, 29 September–2 October 2014; pp. 1–8.
19. Sajjad, M.; Khan, S.; Hussain, T.; Muhammad, K.; Sangaiah, A.K.; Castiglione, A.; Baik, S.W. CNN-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognit. Lett.* **2019**, *126*, 123–131. [CrossRef]
20. Daugman, J. Recognizing Persons by Their Iris Patterns. In *Biometrics: Personal Identification in Networked Society*; Kluwer Academic: Dordrecht, The Netherlands, 1999; pp. 103–121.
21. Lee, E.; Park, K.; Kim, J. Fake iris detection by using purkinje image. In *Advances in Biometrics*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3832, pp. 397–403.
22. Pacut, A.; Czajka, A. Aliveness detection for iris biometrics. In Proceedings of the Annual IEEE International Carnahan Conferences Security Technology, Lexington, KY, USA, 16–19 October 2006; pp. 122–129.
23. Kanematsu, M.; Takano, H.; Nakamura, K. Highly reliable liveness detection method for iris recognition. In Proceedings of the Annual Conference SICE, Takamatsu, Japan, 17–20 September 2007; pp. 361–364.
24. Wei, Z.; Qiu, X.; Sun, Z.; Tan, T. Counterfeit iris detection based on texture analysis. In Proceedings of the International Conference on Pattern Recognition (ICPR), Tampa, FL, USA, 8–11 December 2008; pp. 1–4.
25. Huang, X.; Ti, C.; Hou, Q.Z.; Tokuta, A.; Yang, R. An experimental study of pupil constriction for liveness detection. In Proceedings of the IEEE Workshop on Applications of Computer Vision (WACV), Clearwater Beach, FL, USA, 15–17 January 2013; pp. 252–258.
26. Kohli, N.; Yadav, D.; Vatsa, M.; Singh, R. Revisiting iris recognition with color cosmetic contact lenses. In Proceedings of the IAPR International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013.

27. Doyle, J.; Bowyer, K.; Flynn, P. Variation in accuracy of textured contact lens detection based on sensor and lens pattern. In Proceedings of the IEEE International Conference on Biometrics: Theory Applications and Systems (VISAPP), Arlington, VA, USA, 29 September–2 October 2013; pp. 1–7.
28. Kathikeyan, T.; Sabarigiri, B. Countermeasures against iris spoofing and liveness detection using electroencephalogram (eeg). In Proceedings of the International Conference on Computing, Communication and Applications (ICCA), Tamilnadu, India, 22–24 February 2012; pp. 1–5.
29. Hsieh, S.H.; Li, Y.H.; Wang, W.; Tien, C.H. A novel anti-spoofing solution for iris recognition toward cosmetic contact lens attack using spectral ICA analysis. *Sensors* **2018**, *18*, 795. [CrossRef]
30. Galbally, J.; Ortiz-Lopez, J.; Fierrez, J.; Ortega-Garcia, J. Iris liveness detection based on quality related features. In Proceedings of the IAPR International Conference on Biometrics (ICB), New Dehli, India, 30 March–1 April 2012; pp. 271–276.
31. Pudil, P.; Novovičová, J.; Kittler, J. Floating search methods in feature selection. *Pattern Recognit. Lett.* **1994**, *15*, 1119–1125. [CrossRef]
32. Schwartz, W.R.; Rocha, A.; Pedrini, H. Face spoofing detection through partial least squares and low-level descriptors. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 11–13 October 2011; pp. 1–8.
33. Kollreider, K.; Fronthaler, H.; Bigun, J. *Non-Intrusive Liveness Detection by Face Images*; Elsevier: Amsterdam, The Netherlands, 2009; pp. 233–244.
34. Feng, L.; Po, L.M.; Li, Y.; Xu, X.; Yuan, F.; Cheung, T.C.H.; Cheung, K.W. Integration of image quality and motion cues for face anti-spoofing: A neural network approach. *J. Vis. Commun. Image Represent.* **2016**, *38*, 451–460. [CrossRef]
35. Young-Joo, H.; Kim, W.; Park, J. Efficient Eye-Blinking Detection on Smartphones: A Hybrid Approach Based on Deep Learning. *Mob. Inf. Syst.* **2018**, *2018*, 6929762.
36. Soco1insky, D.A.; Selinger, A.; Neuheisel, J.D. *Face Recognition with Visible and Thermal Infrared Imagery*; Elsevier: Amsterdam, The Netherlands, 2003; pp. 72–114.
37. Fladsrud, T. Face Recognition in a Border Control Environment: Non-Zero Effort Attacks Effect on False Acceptance Rate. Master's Thesis, Gjovik University College, Gjøvik, Norway, 2005.
38. Abd, A.A.Z.; Wei, H.; Ferryman, J. Face anti-spoofing countermeasure: Efficient 2D materials classification using polarization imaging. In Proceedings of the 2017 5th International Workshop on Biometrics and Forensics (IWBF), Coventry, UK, 4–5 April 2017.
39. Aggarwal, G.; Biswas, S.; Flynn, P.J.; Bowyer, K.W. A sparse representation approach to face matching across plastic surgery. In Proceedings of the 2012 IEEE Workshop on the Applications of Computer Vision (WACV), Breckenridge, CO, USA, 9–11 January 2012; pp. 113–119.
40. Bhatt, H.S.; Bharadwaj, S.; Singh, R.; Vatsa, M. Recognizing surgically altered face images using multiobjective evolutionary algorithm. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 89–100. [CrossRef]
41. Sun, Y.; Tistarelli, M.; Maltoni, D. Structural similarity based image quality map for face recognition across plastic surgery. In Proceedings of the 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 29 September–2 October 2013; pp. 1–8.
42. Singh, R.; Vatsa, M.; Bhatt, H.S.; Bharadwaj, S.; Noore, A.; Nooreyezdan, S.S. Plastic surgery: A new dimension to face recognition. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 441–448. [CrossRef]
43. Harsing, S.A.; Talbar, S.N. Adaptive GLOH with PSO-trained NN for the recognition of plastic surgery faces and their types. *Bio-Algorithms Med-Syst.* **2019**. [CrossRef]
44. Rasa, T. Tabula Rasa Spoofing Challenge. 2013. Available online: http://www.tabularasa-euproject.org/evaluations/tabula-rasaspoofing-challenge-2013 (accessed on 12 June 2019).
45. Shmuel, G. Anti-Spoofing System and Methods Useful in Conjunction Therewith. U.S. Patent Application No 15/531,229, 1 February 2018.
46. Wild, P.; Radu, P.; Chen, L.; Ferryman, J. Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. *Pattern Recognit.* **2016**, *50*, 17–25. [CrossRef]
47. Fumera, G.; Marcialis, G.L.; Biggio, B.; Roli, F.; Schuckers, S.C. Multimodal anti-spoofing in biometric recognition systems. In *Handbook of Biometric Anti-Spoofing*; Springer: London, UK, 2014; pp. 165–184.
48. Rodrigues, R.N.; Ling, L.L.; Govindaraju, V. Robustness of multimodal biometric fusion methods against spoof attacks. *J. Vis. Lang. Comput.* **2009**, *20*, 169–179. [CrossRef]

49. Devakumar, P.; Sarala, R. An Intelligent Approach for Anti-Spoofing in a Multimodal Biometric System. *Int. J.* **2017**, *7*. [CrossRef]
50. Mills, J.H.; Schmiedt, R.A.; Schulte, B.A.; Dubno, J.R. Age-related hearing loss: A loss of voltage, not hair cells. *Semin. Hear.* **2006**, *27*, 228–236. [CrossRef]
51. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [CrossRef]