NVEO
Natural Volatiles &
Essential Oils

Adapted Facial Recognition And Spoofing Detection For Management Decision Making System: A Visually Impaired People Perspective

Pooja Singh[1] , N.Jeebaratnam[2] , Harish G Ugraiah[3] , Mrs. Galiveeti Poornima[4] , Mr. Ajay.P[5]

[1]Department of Physics, Faculty of Science, Shree Guru Gobind Singh Tricentenary University, Gurugram, Haryana- 122505.

[2]Department of Electronics and communication Engineering, Centurion University of technology and management ,Paralakhemundi, odisha-761211

[3]Professor and Principal, Arihant Institute Of Commerce and Management, Bangalore, Karnataka- 560062

[4]Assistant Professor, Department of Computer Science and Engineering, Presidency University, Bangalore, Karnataka-560064

[5]Research Scholar, Department of Electronics and Communication Engineering, Anna University, Chennai, India

Abstract:

Biometrics is the measuring and analysis of biological data such as fingerprints, retinas, irises, DNA, face patterns, voice patterns, and hand measurements for the goal of identifying a person. It is becoming more prevalent in both corporate and public security systems to use biometric verification for authentication. As a result of the permanent, ubiquitous, and easy-to-access physical and behavioural traits of individuals, biometrics are able to provide trustworthy identity management systems. Around 0.7 of the world's population has some kind of visual disability, according to the World Health Organization's estimations. Of them, 39 million are blind. Many blind individuals throughout the world are unable to identify the persons standing in front of them, and there are others who struggle to recall someone's name. This method makes it simple to identify the subject. Visually challenged individuals may identify strangers with the use of computer vision and picture analysis. Face recognition and spoofing detection are used in this system to identify people who are standing outside your house. In addition, users will be able to add previously unknown individuals and keep track of everyone who comes to their house using this system.

Keywords: Facial pattern, Face-recognition, spoofing detection, visually-impaired, Bio Metrics, Voice pattern.

1. INTRODUCTION

Many aspects of daily life are becoming easier thanks to facial recognition technologies. There is no longer a need for a password or fingerprint to authenticate an individual's identification. Using these new technology, people can get into buildings without a key or go past airport security with ease. Facial recognition, like any other privacy technology, is being targeted by criminals via spoofing. The implications of a successful spoofing assault might be rather serious. Unauthorized entry may be gained into even the most secure of structures, whether it's a house or a business. Bad actors don't even have to pick a lock to go in and out of a building. Depending on the severity, this may lead to anything from theft of private information to the destruction of essential infrastructure. Learn about the most prevalent techniques of faking face recognition here. What's more, what you can do to stop them from happening in the first place. Passwords have been used for user authentication for a long time. Since passwords are becoming more difficult to remember, the need for a more convenient and safe method of user authentication grows. This fact serves as inspiration for the development of biometric security solutions that do not rely on passwords. Each biometric has its own set of benefits and drawbacks. For example, fingerprint recognition is the most widely used commercial biometric, although it demands a lot of user cooperation. Furthermore, iris recognition is quite accurate, but it is heavily dependent on the quality and involvement of the participants, as well as on the camera.

In terms of both accessibility and dependability, face-recognition is a boon. It may be used to identify uncooperative persons at a distance of up to a few hundred feet. In spite of significant research, there are still variances in facial recognition owing to different elements in real-world circumstances, such as lighting, position, emotion, occlusion, and age. The popularity of 3D face recognition grew as a result of the technology's ability to circumvent position and lighting issues.

As a result of face analysis, visually impaired persons can do a wide range of everyday duties with increased ease and security, allowing them to be more self-reliant and secure. There have been significant advancements in facial recognition over the last several years and it's nearing perfection. People with impairments have benefited from developments in face recognition. To provide one recent example, it has developed a face recognition-enabled intelligent walking stick for the blind. A face recognition system, GPS, and Bluetooth are all included in the cane. Anyone who has a photograph of an acquaintance or a friend saved on the SD card stick will cause the stick to vibrate and offer Bluetooth headset advice on how to contact them. Anyone who is within 10 metres of the device will be able to use it. As with any GPS navigator, the user will be able to get directions to anywhere they want to go owing to the GPS. But today's biometric systems can handle additional issues, such as spoofing, in addition to the work of recognition. Techniques that allow an attacker, generally maliciously, to pass through a communication other than via the manipulation of data entities are known as "backdoors." It is the goal of this project to design, construct, and test a mobile app that incorporates a face-recognition and anti-spoofing system. For the blind and visually impaired, we aim to provide them a method to better their lives and raise their sense of safety and well-being in their own homes or when they interact with others. Validation of the design was done with actual users and a genuine scenario that mimicked what a video portero or a visually challenged person could experience while using their mobile device to shoot photographs. Below, we'll explore some of the contributions: First, a face normalisation approach is presented for the face identification algorithm that is resilient to rotations and misalignments. It has been shown that a robust normalisation technique may considerably improve the success rate of a face identification programme.

2. Literature Review

As the need for security applications grows, so does the importance of human recognition. Biometrics offer secure and efficient identity management systems via the use of permanent, universal, and easy-to-access physical and behavioural features of the individuals. As a result, biometrics is a hot issue right now.

Various approaches have been taken to address the issue of face recognition for visually impaired persons. An overview of the effort that has gone into developing the architecture shown here is provided in the table below. However, in [2], a face recognition system for the visually handicapped is provided on mobile devices, but the emphasis of meetings is on what parts of the visual field are caught by the mobile. An LBP-based face recognition system was created in [3]. Using additional descriptors, such as the Local Ternary Pattern [5] or the Histogram of Gradients [6], they arrived to this conclusion. However, it found that its performance was marginally better than that of the LP and its computational costs were lower. [7] has designed a cane with a face recognition technology embedded into it. Detection spoofing is not carried out in any of these ways, putting the system vulnerable to such assaults. People with vision difficulties, in particular, should be aware of this aspect, according to us. Furthermore, none of the options above are geared for video porters.

The Receiver Operating Characteristic (ROC) curve, which depicts the probability of genuine acceptance vs the likelihood of erroneous acceptance, is often used to demonstrate the verification performance of recognition systems. ROC curves aren't the sole method used in this paper. Detection Error Trade-Off (DET) curves are also used in certain circumstances to indicate verification results. The y-axis of the DET curve represents the false rejection rate, rather than the genuine acceptance rate, which is the key distinction. The term Equal Error Rates (EER) is also used in this research to highlight verification results. True Acceptance Rate (FAR) and False Rejection Rate (FRR) are identical at EER.

The first face is recognised and separated from the backdrop in face-recognition systems.

In order to normalise the face, a number of landmarks are marked. Finally, either verification or identification mode is used to authenticate the user. Amidst all the literature, there are notable contributions such as Eigenface [4], Fisherface, and Local Binary Patterns (LBP). However, the introduction of new face databases such as The Facial Recognition Technology, The Facial Recognition Vendor Test, and the Face Recognition Grand Challenge (FRGC) [7] challenges the standard techniques by providing new datasets (2D, 3D, video etc.). So as a result, these databases have a significant impact on the development of better face recognition techniques. The use of 3D shape cues (either in the form of a 3D curvature description or a 2.5D depth feature) for face identification has been shown in recent surveys [3] to be superior than traditional intensity image-based approaches. 3D shape information, for example, is unaffected by lighting changes. It provides additional information about 2D textures, and stiff surface registrations can easily handle perspective fluctuations [1–4]. There is, however, an imbalance between the efficiency and precision of the 2D data and the high-quality 3D data that most of the literature studies claim findings on (e.g. 3D faces in FRGC, which are collected by a digital laser scanner with depth resolution of 0.1 mm within the normal sensing range). High-resolution RGB picture capture typically takes less than 0.05 seconds, whereas face depth map scanning typically takes around 9 seconds [11]. (and hence with high user cooperation, which is conflicting with the non-cooperative property of face recognition). While all intensity information may be recorded by 8 bits, the depth of an object of 10 cm requires 10 bits for accurate assessment. Accordingly, comparing 2D and 3D face recognition using such data is not completely fair and hinders the adoption of 3D and multi-modal face recognition in actual settings due to this imbalance.

There are a number of advantages to the Kinect sensor, including the fact that it provides both 2D and 3D information concurrently at interactive rates, allowing face-recognition systems to be used in real-time and online environments. As much as we know about Kinect's overall sensor quality, it's still a long way off from the laser scanning quality that's often used in 3D face recognition studies.

3. Spoofing in Face Recognition

An effort to impersonate another individual and get access to an identification system is known as spoofing. spoofing is a genuine danger to face recognition systems because to the ease with which facial data may be gathered in a contactless way. Photograph, video, and mask assaults are all examples of spoofing attacks. The identification of 3D mask assaults looks to be more difficult than the detection of 2D attacks, such as image and video attacks, because of their 3D face form properties. In this section, spoofing attacks and countermeasures in face recognition are broken down into two categories: 2D and 3D.

Due of their simplicity and cheap cost, pictures and videos are frequently used to spoof face-recognition systems. Photo and video assaults against facial recognition systems have been shown. Researchers found that laptops from companies like Lenovo, Toshiba and Asus may be readily fooled by using the Windows XP or Vista operating systems. These laptops employ facial recognition to verify the identity of their users. Security and Vulnerability Research Team of University of Hanoi revealed how to easily spoof the systems "Lenovo's Veriface III," "Asus' SmartLogon V1.0.0005", and "Toshiba's Face Recognition 2.0.2.32" using phoney facial photographs of the user during Black Hat 2009 conference. On the NIST's National Vulnerability Database (NVD) in the United States, it is also stated that this vulnerability has been added. There must be countermeasures in place to improve the security and robustness of face biometric systems, as this basic example shows. A picture spoofing example is shown in Figure 1.

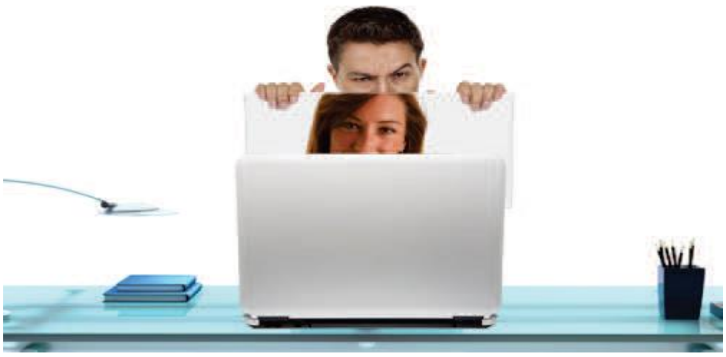

Figure.1: An example photograph attack for spoofing purposes.

In recent years, the topic of spoofing has gained a lot of attention, yet research on face anti-spoofing technologies are still quite few. Consequently, anti-spoofing is a hot research area. The goal is to build non-intrusive countermeasures that can be incorporated into current facial recognition systems without the need for additional equipment or human intervention.

Photograph spoofing may be detected using a variety of methods. If a picture is not limited to a single image, the present algorithms focus on liveness identification and motion analysis. It is possible to apply several countermeasures to individual photos, depending on texture analysis. For pictures, the depth map is flat, whereas it changes depending on whether or not the subject is moving. Many countermeasures based on motion analysis have been discussed in the literature. In [9], the authors derive a reference field from the actual optical flow field data under the premise that the test zone is a 2D plane. For this purpose, the degree of difference between the two fields is employed to discriminate between a 3D face and a 2D image. To identify assaults, [8] uses a collection of face locations that are automatically found and analysed using geometric invariants. Rather of relying on a picture of a person, they employ 3D depth information of a human head to identify the presence of a real person. Following a basic optical flow analysis, a heuristic classifier is used to analyse the trajectory of a chosen region of the face in the series of photos [7]. Other studies [15] combine these ratings with liveness features as eye-blinks or lip movements. [11] and [5] are two examples of countermeasures based on liveness detection. For this reason, the analysis of many photographs throughout time is required to determine the presence of liveliness.

On the other hand, texture analysis-based countermeasures may also be applied to individual photos. The frequency spectrum of a live face may be used to identify spoofing, for example [2]. Photo high frequency components are expected to be lower than live facial pictures in [12]. As mentioned in [13], this strategy works well when the picture photos are poor in resolution and small in size. Images are analysed in [8] to look for printing artefacts, which are then reported. Micro-texture details and texture and local shape features of genuine faces and face prints are investigated in the works of Määtta et al. [6,9], and very good results are given for the detection of face print assaults using the publicly accessible NUAA database [3].

4. System Architecture

Our culture is becoming more dependent on biometric identification. Biometrics is a word that relates to measurements pertaining to human traits. Biological and behavioural unique identifiers such as faces, voices, fingerprints, signatures, gait, among others, may be utilised as a form of identification and access control in this situation. The usage of biometric traits and procedures has been around for a long time. Humans and certain animal species may identify each other based on their appearance or voice, and this is also the case in the animal kingdom.

Biometrics are now used in a wide range of applications, including forensics, border and access control, surveillance, and on-line commerce, because researchers from a variety of fields, including image processing, computer vision, and pattern recognition, have applied various techniques to improve the performance of biometric systems.

Face recognition and fingerprint scanning are two of the most often utilised biometric security methods. There is a need to create a fail safe system that lets to "keep the prize" away from attackers since facial recognition systems are the most often targeted [10].

According to the International Biometric Group (IBG) [3], the face is the second most widely used biometric in the world, just after the fingerprint. Because of the biometric passport (e-passport), which allows people to enter countries by simply comparing their face to the passport's picture, as well as the increasing presence of biometric applications for personal computers and mobile phones to the extent of opening/accessing your personal bank account using face identification, it is used worldwide. Since biometric technologies are being used to construct national identification schemes in poorer nations, too, For every Indian citizen, the India Unique Identification Authority (IUIA) is producing and issuing a unique ID based on face recognition and fingerprint scanning. There are several reasons why researchers have focused on faking the face, which is one of the biometrics.

Figure shows that each of these biometric systems is subject to a variety of assaults.

Presenting a phoney biometric attribute of a user and then presenting it as the genuine user is the main emphasis of this study, which is known as the Presentation Attack (PA) at the sensor. When it comes to hacking assaults, biometric samples may be changed during processing or various parts of the process can be overridden such as a comparator or even a database for example can be manipulated. In this study, the primary goal is to establish whether or not the person presenting the attribute is a valid customer. In certain domains, the phrase "liveness detection" is used as a synonym for spoof detection; however, in most cases, the term "liveness detection" refers to the detection of vitality indicators, such as a user's heartbeat or blinking eyelids. A subgroup of PAD approaches, this phrase is referred to in this article. This form of assault, sometimes known as an artefact, is dependent on the device's resolution or the type of support utilised to deliver the bogus copy. When it comes to the result, external variables such as lighting or background circumstances might have a significant impact.

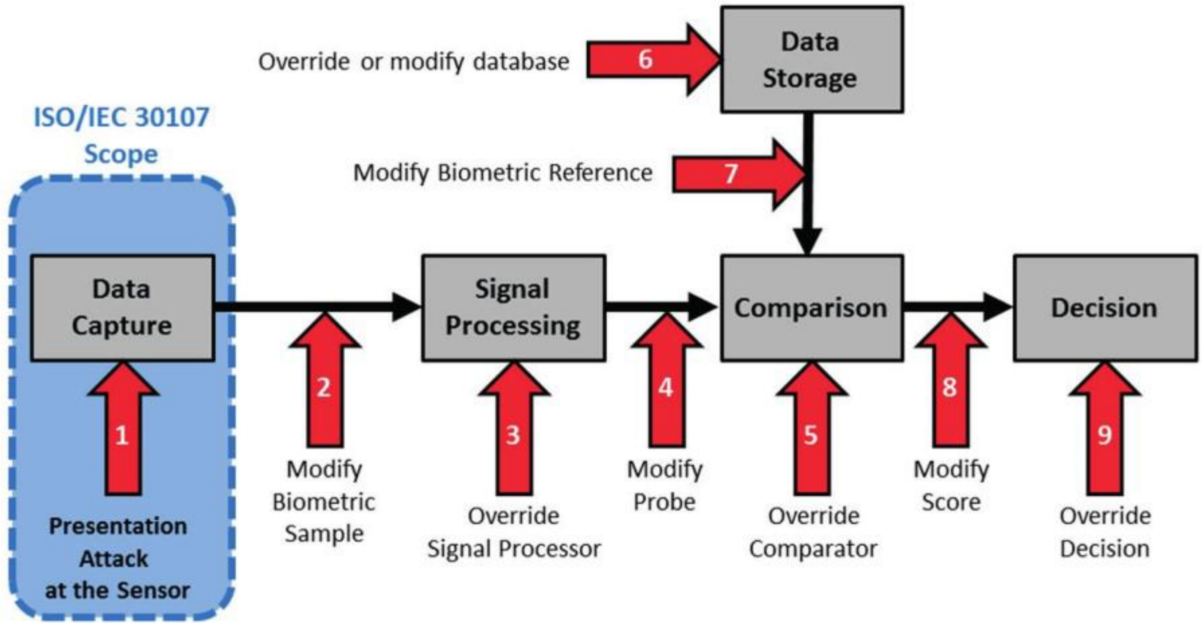

Figure.2: Different points of attacks in a biometric system.

Additionally, each scan generates a massive amount of data that should ideally be analysed in real time. These strategies rely on extracting characteristics that can identify presentation attacks, although these features are generally basic and processed before being related to each other.

In certain circumstances, correlation between various methods might lead to an improvement in the overall result [6], but this is particularly difficult to perform since it is impossible to know whether methods can be improved or not. Deep Learning's newly discovered capability has made this process much easier in the modern day (DL). In order to generate a good conclusion, such algorithms may extract multiple separate traits that are judged relevant by the algorithm itself, but the programmer can have some effect. Some aspects may be omitted from the network in order to get the best possible results. Many people believe that these Machine Learning (ML) technologies are effective because they accelerate the whole process, can be taught to learn from errors, and are capable of uncovering unexpected connections that aid in completing a job more quickly and efficiently.

5. Face Recognition Systems

Introduces [9], the 3D face recognition system used as a starting point for this investigation. The TABULA RASA project has likewise chosen it as its foundation system [11]. As an input, it employs a 3D model of the face. Each sample in the database has already had three landmark points labelled at the tip of the nose and the outer corners of the eyes. Using two sets of landmarks (landmarks of the generic model and the subject's face), a linear transformation is first calculated using the least squares method. By using least squares, we imply that the total sum of squares of the mistakes produced in the answers of all equations is reduced to a minimum. By decreasing the squared distance between the generic model's point sets and the subject's face, we get the best LSS fit. Thus, a generic model is applied to the face of the subject using a transformation that incorporates rotation, translational scaling and isotropic scaling. Iterative Closest Point (ICP) approach [13] is used to further refine the alignment. As a final step, 140 previously chosen points on the generic model are linked with the nearest vertices on the face under examination, and TPS warping [16] is performed to the generic model, resulting in warping parameters (WP) of size 140 x 3. [16] The classifier is given WPs that denote departures from the common structure. As a final step, the recognition rates of two different face models are calculated by taking the median of their respective feature-vector-cosine distances (WP). A example model built using this technology, known as WP, is shown in Figure 3 (below).

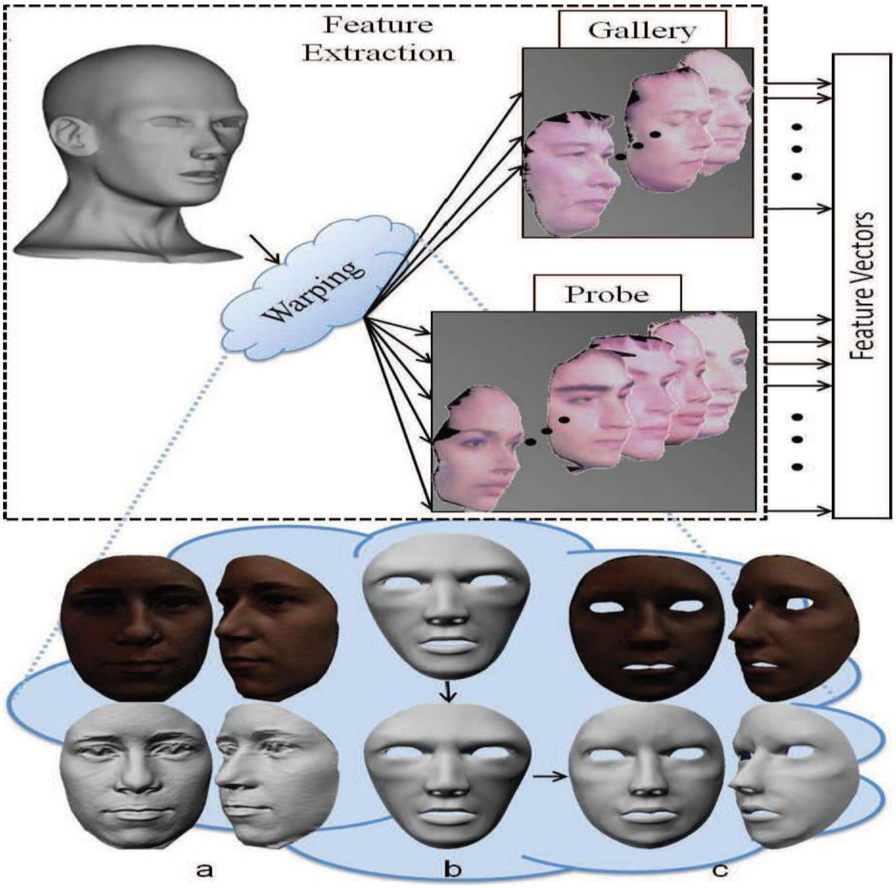

Figure 3: An example of how to extract features from a model is shown

Faces with and without texture of the topic (a) For example, (b) a generic model before and (c) after alignment, as well as after warping.

Local Binary Patterns (LBP) [4] are used as a starting point for 2D face recognition. Because of its discriminative power, computational simplicity, and ability to withstand monotonic gray-scale fluctuations produced by, for example, lighting differences, LBP has become a popular tool for the description of human facial features. To some part, the LBP approach's robustness is due to the use of histograms as features. For facial recognition in 2D.

6. Results and Analysis

Two sorts of experiments are carried out in order to determine the efficiency of the suggested method. In the first experiment, the suggested technique is compared to the approaches described in [14]. Experiment 2 is designed to demonstrate the impact of DoG filtering on the suggested method. Figure 4 compares the classification accuracies (percent) determined by applying three classification approaches to five kinds of input characteristics specified in [1].

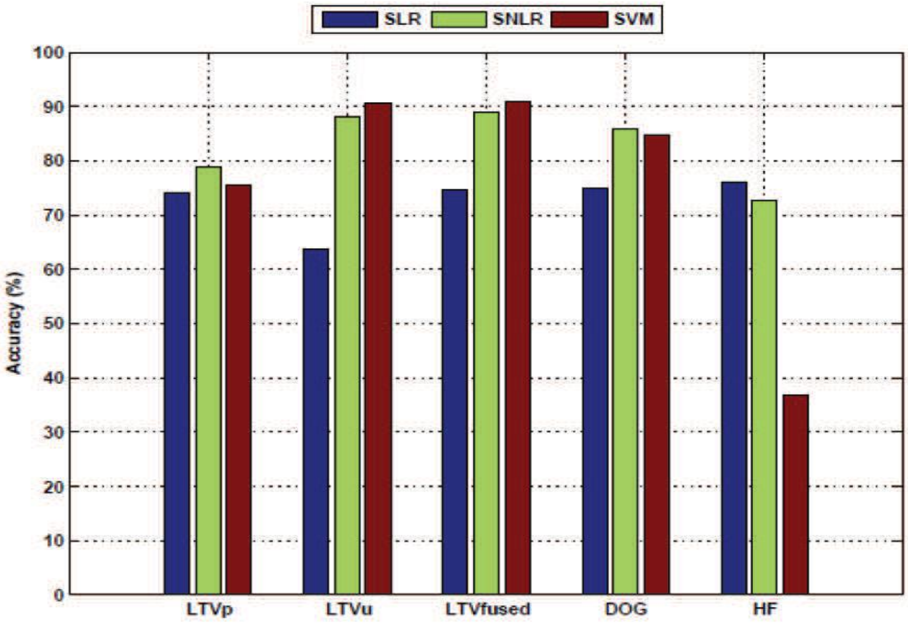

Figure.4: Comparison of detection rates using SLR, SNLR, SVM as classifiers
and LTVp, LTVu, LTVfused, DoG and HF as input features.

Using the database presented in [13], this paper does an accurate comparison to the other approaches in [13]. As a result of this study, the following classifiers were used: SLR, SNLR, and SVM; illuminance component of image estimated with Logarithmic Total Variation (LTVu), reflectance component of image estimated with Logarithmic Total Variation (LTVp), DoG filtered image, and high frequency component of image (HF). For the best results, pictures are fused (LTVfused) such that the illuminance and reflectance components are combined (Figure.4). Figure.4 shows that the suggested method is at least as good as most of the other methods displayed in this figure, if not better than most of them.

Figure 4 reveals that, at the outset, the proposed method outperforms the SLR classifier when applied to all input feature categories. Furthermore, it is obvious that SLR, SNLR and SVM classifiers perform worse than our findings (88.03 percent) when DoG, HF and LTVp are utilised as input features for the SLR classifiers. According to Figure 4, the best results are achieved when input characteristics like LTVu and LTVfused are combined with classifiers like SNLR and SVM. This approach's outcome (88.03 percent) is, nonetheless, competitive with these ones. In fact, our method offers certain benefits over the best-performing strategies in this figure. When using LTVu and LTVfused features, the picture must be divided into illuminance and reflectance components; but in the suggested way, the procedure is applied directly to an image. The categorization mechanism in our approach is also quite straightforward. As a result, the suggested technique provides a detection accuracy of 88.03% with the benefits of reduced computing complexity and tolerance to light and rotation variations, making it a viable alternative to more traditional methods.

According to [7], the countermeasure approach described in this work is based on texture and contrast analysis. Following our investigation of the NUAA database, a number of research have been published on the identification of picture spoofing utilising the database. Määtta et al. have reported the most accurate face-print detections to date [7, 8]. In each of these tests, spoofing detection rates are almost flawless when utilising the NUAA database.

In the aforementioned test, a re-captured facial picture identification rate of roughly 88% is obtained when the lighting conditions change. An first pre-processing phase called DoG filter isolates places from which a significant amount of spoofing data may be acquired for Test 1. Here, we'll see how DoG filtering affects the suggested technique. Both with and without DoG filtering, the outcomes of the strategy. There's no doubt about the impact of DoG filtering on the content. When DoG filtering is implemented as a pre-processing step, there is a considerable improvement over the scenario when DoG filtering is not applied. In order to recognise recorded pictures, DoG filtering produces a frequency spectrum with useful data that may be used to eliminate misleading information and noise from captured photos.

Basic mode is a biometric system without spoofing or countermeasures, which is the initial mode DB-r is used to assess the baseline performance. In order to assess performance, all-vs-all verification is used. DB-r access is checked against all other DB-r identities. False Rejection Rate (FRR) and True Acceptance Rate (UAR) are two metrics used to evaluate the performance of a system, which is defined as the percentage of users who are refused while authenticating against their own template and approved when authenticating against another template (False Acceptance Rate - FAR). Mask assaults are used in the second method of assessment of face-recognition systems (baseline under attacks in Figure.5). It's possible to utilise either the DB-r or the DB-m. A decrease in performance is predicted when spoofing attacks are used.

When faked, the system accepts a certain number of assaults per second. According to FRR, a high percentage of real-access attempts are mistakenly labelled as assaults by the system. Only the test set is utilised for the assessments of 2D and 3D face recognition systems here. In the suggested countermeasures, a train set is employed to train classifiers. Figure.5 depicts the 3D and 2D baseline systems' behaviour in the presence and absence of assaults. Each of the findings is provided in terms of detection error trade-off (DET) profiles, which show how a system behaves when the decision threshold is altered, idling, or how the false rejection rate changes with the false acceptance rate, respectively.

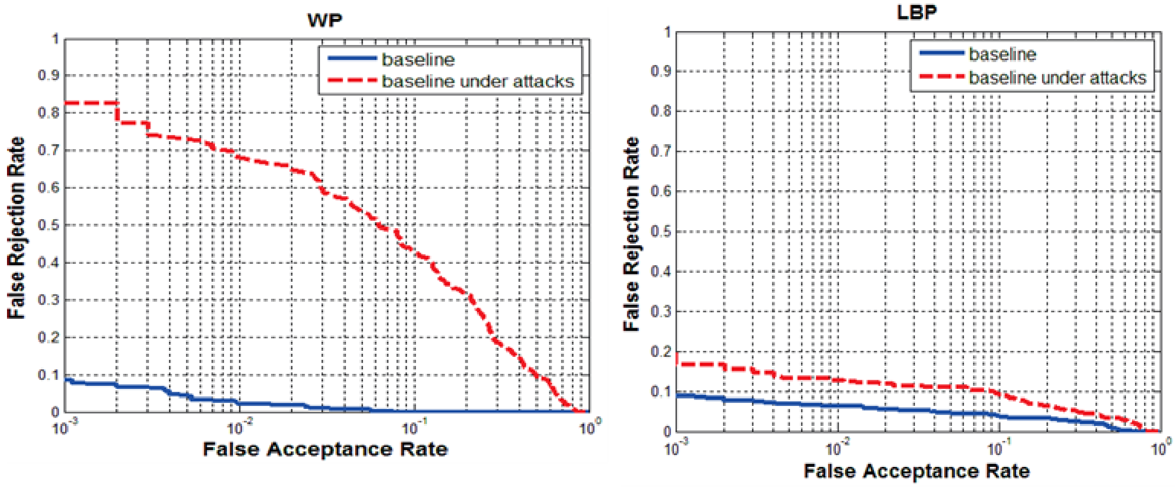

Figure.5: The DET Curves of the 3D and 2D face baseline biometric system

with/without mask attacks, respectively.

Both 2D and 3D face recognition systems may be fooled by mask assaults; however, mask attacks have a higher chance of succeeding with 3D face recognition vs 2D face recognition systems (area between red and blue curves is much more for 3D compared to 2D face recognition system).

The Equal Error Rate (EER) in the baseline mode rises from 1.8 percent to 25.1 percent for 3D face recognition and from 4.7 percent to 9.9 percent for 2D face recognition systems when attacked. Real face and mask assault 3D form qualities are more comparable than texture characteristics. If you're trying to discover mask assaults, texture analysis may be more useful than 3D shape analysis. According to [74], the ability to withstand mask spoofing is both approach and modality dependent. Spoofing mask assaults on facial recognition systems need the use of countermeasures in order to minimise their effect.

7. Conclusion

Recaptured image detection is presented in this study based on the examination of the various contrast and texture characteristics of captured and recaptured pictures. When compared to the findings provided in [13], which used the identical NUAA database in their trials, the suggested technique provides pretty excellent results. The benefits of this method are its simplicity and lack of user involvement. There have been a number of research on how to prevent photo assaults from being detected. Compared to 2D spoofing methods like image and video, 3D mask assaults on facial recognition systems are a novel topic. Until now, no one has studied the effect of 3D mask assaults on current identification systems.

References

1. A. Fernández, J. L. Carús, R. Usamentiaga and R. Casado, "Face Recognition and Spoofing Detection System Adapted To Visually-Impaired People," in IEEE Latin America Transactions, vol. 14, no. 2, pp. 913-921, Feb. 2016, doi: 10.1109/TLA.2016.7437240.
2. Maiden Baum, S., Harass, S., Abound, S., Buchs, G., Chebat, DR, Levy-Tzedek, S., & Amedi, A. (2014). The "EyeCane", a new electronic travel aid for the blind: Technology & swift learning behavior. Restorative Neurology and Neuroscience, 32 (6), 813-824.

3. C. Kramer, KM, Hedin, DS, & Rolkosky, DJ (2010, August). Smartphone based face recognition tool for the blind. In Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE (pp. 4538-4541). IEEE.
4. Ahonen, T., Hadid, A., & Pietikainen, M. (2006). With Face description Local binary patterns: Application to face recognition. pattern Analysis and Machine Intelligence, IEEE Transactions on, 28 (12), 2037-2041.
5. Tan, X., & Triggs, B. (2010). Local Enhanced feature sets for texture face recognition under difficult lighting conditions. Image Processing, IEEE Transactions on, 19 (6), 1635-1650.
6. Dalal, N., & Triggs, B. (2005, June). Histograms of oriented gradients for human detection. In Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on (Vol. 1, pp. 886-893). IEEE.
7. Chingovska, I., Anjos, A., & Marcel, S. (2012, September). on the Local effectiveness of binary patterns in face anti-spoofing. in Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the (pp. 1-7). IEEE.
8. Benlamoudi, A., Samai, D., Ouafi, A. Taleb-Ahmed, A., Bekhouche, S. E., & Hadid, A. Face Detection Spoofing Using Images From Single Active Shape Models With Stasm And LBP.
9. A. Fernandez, JL Carus, R. Usamentiaga, E. Alvarez, R. Casado, "Unobtrusive Health Monitoring System Using Video-Based Physiological Information and Activity Measurements ", In IEEE International Conference on Computer, Information, and Telecommunication Systems, CITS 2015, IEEE, vol. 1, no. 1 pp. 100- 104, Gijon (Spain), 2015.
10. J. Määttä, A. Hadid and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1-7, doi: 10.1109/IJCB.2011.6117510.
11. N. Daniel and A. Anitha, "A Study on Recent Trends in Face Spoofing Detection Techniques," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 583-586, doi: 10.1109/ICICT43934.2018.9034361.
12. Y. B. Reeba and R. Shanmugalakshmi, "Spoofing face recognition," 2015 International Conference on Advanced Computing and Communication Systems, 2015, pp. 1-5, doi: 10.1109/ICACCS.2015.7324132.
13. A. F. Ebihara, K. Sakurai and H. Imaoka, "Efficient Face Spoofing Detection With Flash," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 4, pp. 535-549, Oct. 2021, doi: 10.1109/TBIOM.2021.3076816.
14. A. F. Ebihara, K. Sakurai and H. Imaoka, "Specular- and diffuse-reflection-based face liveness detection for mobile devices", Proc. IEEE Int. Joint Conf. Biometr. (IJCB), pp. 1-11, 2020.
15. S.-Q. Liu, P. C. Yuen, X. Li and G. Zhao, "Recent progress on face presentation attack detection of 3D mask attacks" in Handbook of Biometric Anti-Spoofing, Cham, Switzerland:Springer, pp. 229-246, 2019, [online] Available: http://link.springer.com/10.1007/978-3-319-92627-8_11.