WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review on Face Fraud Detection in Online Exam

Vaishnavi Chincholkar, NeerajaBhide, Sakshi Powade, SonalSutar, Prof. Akash Dodke.

Department of Information Technology Engineering.Anantrao Pawar College Of Engineering And Research, Pune – 411009.

ABSTRACT

E-learning has developed tremendously over the last two decades, thanks to the advent of the Internet and technology. An important part of E-learning is the online assessment. Face recognition is commonly regarded as an alternate form of authentication that may be used to replace standard password approaches in a variety of access control applications. Despite major advancements, this method of authentication is still vulnerable to a number of flaws, including the use of printed pictures, 3D masks, and video replay assaults. Replay attacks, in which a pre-recorded video of the user is played and a printed photograph is placed in front of the camera, are the two most popular techniques to commit fraud while attending the examination in face recognition systems. As a result, a reliable face liveness detection approach is required for identifying spoof assaults and distinguishing between legitimate and illegitimate users utilizing machine learning techniques. We present a method that employs light reflection obtained from a camera while recording a video or taking an image of the examinee during an examination, based on the observation that different materials reflect light differentlyKeywords— Fraud Detection, Face Detection, Local Binary Patterns Histogram, Support Vector Machine, Alerts Notification.

Introduction

In computer-based communication, authentication is a problem. Face recognition is widely utilized in a variety of applications, including security and door control. This technique was built by employing face recognition to take student attendance.

Face recognition has piqued the interest of academics in a variety of domains, including security, image processing, and computer vision. Face recognition has also proven beneficial in the analysis of multimedia data. In video, face recognition is a difficult process that does not provide precision. It is simple for a human to distinguish if a person is male or female, but it is far more difficult for a machine or robot to do so. Gender identification using a person's voice is far easier than using facial images. This is a binary categorization that can be used in a variety of applications, including targeted advertising, surveillance, human-machine interaction, content-based indexing and searching, demographics, and biometrics.

The system acquires the grayscale image via image processing, making it simple to use. for the recognition of facial features To detect the face, the system employed Haar Classification. For face recognition, the system employs LBP features, or Local Binary Patterns.These characteristics are analyzed using LBP features, which aid in face recognition and attendance tracking.Face-recognition-based security systems are becoming increasingly prevalent. It has become one of the most used biometric methods in security systems as a result of advancements in computer vision and artificial intelligence. Face recognition-based security is already used to unlock smart phones and other devices. However, a spoofing attack can quickly compromise the system. Spoofing attacks are divided into three categories: 1) still image assaults, 2) video attacks, and 3) mask attacks.

Objectives

The objective of this project is to develop Automatic Facial Expression Recognition System which can take human facial images containing some expression as input and recognize and classify it into seven different expression class such as : I. Neutral II. Angry III. Disgust IV. Fear V. Happy VI. Sadness VII. Surprise.Several Projects have already been done in this fields and our goal will not only be to develop an Automatic Facial Expression Recognition System.

LiteratureSurvey

According to numerous research studies, there are four essential procedures that must be completed in order to undertake this project. i. Pre-processing ii. Face registration iii. Emotion classification iv. Extraction of facial features

Pre-processing: The term "pre-processing" refers to operations on images at the most basic level of abstraction.

Intensity photographs are used as input and output. The majority of the pre-processing processes that are used Registration of the face: Face

Registration is a computer technology that recognizes human faces in digital photographs and is used in a range of applications. The algorithm attempts to classify the given faces depicting one of the seven fundamental emotions in the third phase of categorization. Extraction of Facial Features: The process of locating certain regions, points, landmarks, or curves/contours in a given 2-D image or 3D range image is known as facial features extraction. a thermographic dataset They utilize this approach to construct their model since genuine and synthetic faces have different temperatures, therefore the radiation will be different. However, the model still has to be improved for greater accuracy. We employ a deep learning strategy in this research to rescue our model from mask and video attacks.

Reference Papers:

1. Improved CNN with Context and Texture Information for Face Liveness Detection.

Face recognition systems' security is becoming increasingly critical as the technology gets more widely used. Fake faces, such as those created from images or video clips of people, can be used to fool face recognition algorithms. As a result, a real face recognition system usually includes a face liveness detection module that can tell the difference between a fake and a real face. Face liveness detection has gotten a lot of interest, and a lot of research has been proposed.A real face has a 3D structure in the physical world, whereas a phony face from a photo or video is a 2D plane. A false face picture is simple to seem mirror reflection and has a degree of shape deformation when compared to a real face image. It's unavoidable to distort the color and lose some vital information during the second shoot.

- In this research, we offer a method for detecting face liveness that is both effective and robust. To effectively use low-level detailed information and high-level semantic information, this method combines an upgraded CNN with two bypass connections with a traditional texture-based framework. Context information is also used to aid in the liveness identification task. When compared to other available methods, this system is quite accurate.
- It is evident that ablating any aspect of the proposed method will reduce its performance. This implies that each component makes a clear contribution.

The HTER of the suggested approach in various configurations.However, determining which one contributes more is difficult because it depends on a variety of factors, including datasets, parameter settings, and so on. On the Replay dataset, for example, context information contributes more than texture information, whereas on the CASIA dataset, the opposite is true.

2. A two-stage strategy to detecting facial liveness that is both effective and efficient: Deep and based on motion based on learning

A strategy that combines two approaches This research proposes motion-based and deep learning-based approaches. We refer to two approaches as a two-stage strategy since they are cascaded with one another. We choose eye blink as a motion feature in a motion-based stage. Because it is simpler and more precise than other motion features like a moving lip, hand, or background, for example. A method for real-time eye blink detection was proposed by Soukupova et al. [8]. When the eye is blinked, the EAR (eye aspect ratio) decreases.

In paper, this approach of eye blink detection is applied. The DenseNet CNN architecture suggested by Gao Huanget al.[9] is a state-of-the-art approach. The proposed method makes use of this design. DenseNet has been trained on mask and video attacks as well as genuine face data, thus it will protect the system from these threats. In a nutshell, the first level will protect the system from picture attacks, while DenseNet will protect it from mask and video attacks.

- In order to select appropriate phases for liveness detection, each sort of spoofing attack should be thoroughly examined to determine its unique characteristics. The stages should be developed based on their properties. Analogy can be used to create a more robust and accurate facial liveness detection model.
- This work proposes a more accurate approach with two steps of face liveness recognition and real-time analysis. The key to success is to divide the liveness detecting workload across the two stages. If we can add more correct phases, the model's accuracy may improve as well.

3. Defending Face, Fingerprint, and Iris Recognition against Presentation Attacks

Biometric authentication is a method of automatically recognizing people based on their behavior, physical characteristics, and chemical characteristics. This technique has recently emerged as a vital mechanism for access control in many modern applications, where older approaches such as those based on knowledge (e.g., keywords) or tokens (e.g., smart cards) may be useless due to their ease of sharing, loss, theft, or manipulation. Biometrics are increasingly being utilized as the primary authentication factor for access control, as well as in conjunction with traditional authentication procedures as a "step-up authentication" component in two- or three-factor authentication systems.

- The beginning network for iris and fingerprints isn't even connected to the same object identification problem. The results demonstrated that deep learning can detect spoofing attacks almost accurately in some circumstances (AVTS iris benchmark). Only the last layer, which is tightly tied to the classification task done by the VGG network, has been altered in this simplified approach. However, two or all fully linked layers could be replaced to better utilize the output of the convolutional section of the network.

- The cross-dataset and cross-sensor experiments provide the second takeaway. The flexibility that defines convolu- tional networks appears to be the cause of these abysmal results. They can "decide" which found attributes of the input data to utilize in the categorization process because of the flexibility. However, if they are not trained on data that includes a representative sample of the conditions seen during testing, they will fail miserably, as most of the characteristics will no longer match the new data.

This is not a surprise outcome, because it simply necessitates solutions that incorporate prior knowledge of the modeled event. The current fascination with deep learning appears to have reignited an old debate: should we use models based on our understanding of the problem, which is neither complete nor accurate (referred to as "hand-crafted" solutions) or more flexible models that learn everything from the data (referred to as "data-driven" solutions)? It appears that a reasonable combination of both approaches will provide the highest level of reliability. We are convinced that the best of both worlds is the answer to this challenge.

4. A Survey of Biometric Antispoofing Methods in Face Recognition

'Fingerprints can't lie, but liars can make fingerprints," says the proverb. Unfortunately, this translation of an old Mark Twain quotation has been proven correct on numerous occasions. Not only for fingerprints, but also for a variety of other biometric characteristics like face, iris, voice, and even gait.

Every technology operates on its own schedule. The development of biometric technology has been steady and continuous from the initial pioneering efforts on automatic voice and facial recognition over 40 years ago. Researchers from a variety of fields, including as image processing, computer vision, and pattern recognition, have employed the most cutting-edge techniques in each of these areas to increase the security of the system.

Figures do not lie; but, liars do.biometric systems' performance Biometrics can now be used in a wide range of applications, including forensics, border and access control, surveillance, and online commerce, thanks to technical advancements.

• As discussed in this paper, a lot of research has been done on the vulnerabilities of biometric systems to direct attacks, and several ways to protect them from this threat have been offered. Furthermore, independent tests have revealed that several of these protective systems are capable of achieving extremely competitive results when tested in lab conditions. Despite all of these measures, commercial products, even those manufactured by the most advanced technology companies, continue to be vulnerable to hacker attacks. What is the best way to communicate this situation? A straightforward solution is not possible, as it is in most circumstances, because a lot of causes have contributed to the current situation.

• On the one hand, the biometric community has always followed the security via transparency approach, which was first established in the field of cryptography and subsequently generalized to all other security domains as "the enemy knows your system." This principle asserts that the fewer and simpler the secrets required to establish the security of a system, the easier it is to maintain that security. In other words, it's pointless to try to conceal or deny the vulnerabilities of biometric systems to spoofing because attackers will eventually expose them, with unforeseeable repercussions.

5. A novel non-linear modifier for robust face recognition using adaptive lighting normalization.

Face recognition has become a very essential area of research in the realm of computer vision and image understanding as biometric technology has advanced and evolved. Several researchers have contributed to this topic, and a high recognition rate for facial recognition has already been attained. However, as we can see, lighting with varied intensities of light from different angles might alter the face during biometric scans. Face recognition in real-time applications is difficult owing to fluctuating lighting conditions. The amount of light projected onto the face from a particular angle has an effect on the face's illumination.

It will be simple to recognize a face if the influence of illumination change is controlled. In recent decades, a number of strategies for lighting adjustment in face recognition have been introduced. Face photos lighted under various lighting circumstances can be processed as relighting (reproduce illumination) and un-lighting (normalize illumination) images, as shown. The proposed method is useful for face recognition lighting normalization.

• This work shows an adaptive approach to illumination normalization under different lighting circumstances to address the constraints of existing strategies with constant parameter values for illumination correction. The number of low frequency DCT coefficients utilized for illumination normalization is computed adaptively using the suggested approach. The amount of low frequency DCT coefficients generated improves face recognition accuracy while also reducing the temporal complexity of illumination normalization. DCT and IDCT both have a computational cost of O (NlogN), where N is the total number of pixels in the input image. In methods that work in the DCT domain, this amount of computation is always required. For instance, illumination normalization utilizing the proposed approach with BP classifier and PCA with k-NNC classifier, Discard LFDCT Coeff., DCT coefficient rescaling, and Simple Fuzzy filter (= 0.5) with AHE+Log. The number of low frequency DCT coefficients is generated adaptively in the proposed method based on illumination variations in the input image. To produce the illumination adjusted low frequency DCT coefficients, these computed coefficients are multiplied with non-linear polynomial coefficients with constant processing complexity (vector operation).

Discussion

• In this research, we offer a method for detecting face liveness that is both effective and robust. This technique combines an upgraded CNN with two bypass connections with a texture-based architecture.

• The stages should be designed based on their properties. Analogy can be used to create a more robust and accurate facial liveness detection model.

• It appears that the current obsession with deep learning has reignited an old debate: should we use models based on our understanding of the problem, which is neither complete nor accurate (referred to as "hand-crafted" solutions) or more flexible models that learn everything from the data (referred to as "data-driven" solutions)?

It appears that a reasonable combination of both approaches will provide the highest level of reliability. We are convinced that the best of both worlds is the answer to this challenge.

• To sum up, while a lot of effort has been done in the subject of spoofing detection and significant breakthroughs have been made, attacking tactics have also changed and become more sophisticated. As a result, there are still significant hurdles in the protection against direct attacks, which will ideally lead to a new generation of more secure biometric systems in the next years.

• In the future, the proposed approach will be tested to see if it can perform adaptively on the different channels of color face photos, making it more suitable for normalizing color image lighting.

Conclusion

The facial expression recognition system described in this paper presents a robust face recognition model based on the mapping of behavioral and physiological biometric variables. The physiological properties of the human face that are relevant to diverse expressions such as happiness, sorrow, fear, anger, surprise, and disgust are linked to geometrical structures that are reconstituted as the recognition system's basis matching template. As a property base, the behavioral aspect of this system relates the attitude behind various expressions. In genetic algorithmic genes, the property bases are divided into two categories: revealed and hidden. In the sphere of biometric security, the gene training set analyzes the expressional uniqueness of individual faces and provides a resilient expressional recognition model.

References

[1] “A Fast and Accurate System for Face Detection, Identification, and Verification” by Rajeev Ranjan, Ankan Bansal, Jingxiao Zheng, Hongyu Xu, Joshua Gleason, Boyu Lu, Anirudh Nanduri, Jun-Cheng Chen, Carlos D. Castillo, Rama Chellappa. , 2019 IEEE annual international conference

[2] Bimodal Face Recognition Based on Liveness Detection by WenlongGao ; Kai Jia ; Fang Xu ; Fengshan Zou ; Jilai Song. 2019 4th IEEE annual conference.

[3] Efficient two stage approach to detect face liveness Motion based and Deep learning based by Md. Mehedi Hasan ; Md. Salah Uddin Yusuf ; Tanbin Islam Rohan ; Shidhartho Roy 2019 4th IEEE coference

[4] Face Liveness Detection Based on the Improved CNN with Context and Texture Information by ChenqiangGao ;Xindou Li ; Fengshun Zhou ; Song Mu.

[5] Xu Zhang, Xiyuan Hu, Mingyang Ma, Chen Chen and Silong Peng Face Spoofing Detection based on3D Lighting Environment Analysis of Image Pair 2016 23rd International Conference on Pattern Recognition.

[6] JingjingLi ;Xinfeng Zhang ; Yongbing Zhang ; Haoqian Wang ; Fang Yang Face Liveness Detection Based On Multiple Feature Descriptors 2019 International Conference on Technologies and Applications of Artificial Intelligence.

[7] JongwooSeo, In-JeongChung , “Face Liveness Detection Using Thermal Face-CNN with External Knowledge ” , Symmetry 2019, 11(3), 360.

[8] Soukupová, Tereza and Jan Cech. “Real-Time Eye Blink Detection using Facial Landmarks.” (2016), 21st Computer Vision Winter Workshop, February 3–5, 2016

[9] Gao Huang ; Zhuang Liu ; Laurens van der Maaten ; Kilian Q. Weinberger , “Densely Connected Convolutional Networks ” , IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.[10] Haoliang Li, Wen Li, Hong Cao, Shiqi Wang, Feiyue Huang and Alex C. Kot, “Unsupervised Domain Adaptation for Face AntiSpoofing”, IEEE Transactions on Information Forensics and Security, Page(s): 1794 – 1809.

[11] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li and Li Fei-Fei, “ImageNet: A Large-Scale Hierarchical Image Database ”, IEEE Conference on Computer Vision and Pattern Recognition 2009

[12] Kim Y-H, Kim H, Kim S-W et al (2017) Illumination normalisation using convolutional neural network with application to face recognition. Electron Lett 53:399–401

[13] Lee KC, Ho J, Kriegman D (2005) Acquiring linear subspaces for face recognition under variable lighting. IEEE Trans Pattern Anal Mach Intell 27:684–698

[14] Lee P-H, Wu S-W, Hung Y-P (2012) Illumination compensation using oriented local histogram equalizationand its application to face recognition. IEEE Trans Image Process 21:4280–4289

[15] Mansoorizadeh M, Charkari NM (2010) Multimodal information fusion application to human emotion recognition from face and speech. Multimed Tools Appl 49:277–297