Mouneshachari S.[1*]
Poornima G. J.[2]
Roopa Banakar[3]
Bharathi N.[4],
Swarnalatha K.[5]
Swetha B. S.[6]

Background based Authentication for Face Recognition Systems

Abstract
Face Recognition Systems are facing several challenges. One major challenge is fooling the system using face photos or images. The proposed paper has tried developing an efficient methodology to enable and support existing face recognition systems. The background of face in a given image is considered as a main source for authentication. The analysis and estimation of similarity among the background of the face before and after its capture is considered as one of the major parameter to authenticate the presence of face during its capture. The paper is applying image similarity techniques to estimate the percentage of the background in the provided face image to ascertain the presence of physical face during face recognition process.

Keywords: Face Recognition Systems, Background of Image, Image processing, Authentication, Histogram

INTRODUCTION

Face recognition systems have acquired their own importance in dealing with smarter ecosystems. Basically it has applications corresponding to human-computer interfaces, Identity estimations and in providing secured environments [1, 2]. An emergence in technologies related to Artificial Intelligence is offering and is in need of many applications using face recognition systems. Hence, the strengthening of face recognition systems is much essential on its security, authenticity, devices and technology. Various techniques and algorithms are designed based on deep learning methods. Multi-task Cascaded Convolutional Network (MTCNN) is one of the most widely used algorithm for face detections. Certain neural network structures are supporting in providing a better accuracy and speed [3]. Also, there are certain algorithms acting as standard techniques for face recognition namely Principal Component Analysis (PCA) [4], Facial Landmark Detection (FLD) [5], Gabor Wavelets (GW), Support Vector Machines (SVM) [6] and so on. Face alignments also plays a major role during face detection and recognition. FDDB[7] and WIDER FACE [8] are some of the benchmarks for face alignments.

Authentication of the physical face presence during face recognition is one of the challenging tasks for face recognition systems. There are several ways to fool the FRs now-a-days [10] [11]. Face morphing is one of the simplest methods to fool face recognition systems [9].

The proposed paper is trying to provide a unique solution to strengthen currently available face recognition systems. The proposed approach is considering the background details for CNN based feature extraction process to authenticate face physical presence.

1.Literature Survey

1.1Face detection and recognition

Face Detection Techniques: Before recognition of the faces in the given image, its detection plays a major role. Low Binary Pattern (LBP), Haar cascade, Single Shot Detector (SSD) and You Only Look Once (YOLO) models are some of the trending face detection techniques in the literature. The author has proved the accuracy of Haar cascade is upto 96.24% and for LBP classifier 94.74% [12]. The author [13] has experimented between Haar Cascades with YOLO v3 and declared that the Haar cascades functions faster with less accuracy rate of 45% whereas the later algorithm works slower with more
accuracy rate of upto 90%. Face Recognition is the later process to know the face label.

1.2Authentication systems

An overview of the main biometric identification technologies is provided in this survey, with an emphasis on their accuracy, difficulties, and developments.

Authors[18] provides a thorough examination of different fingerprint recognition methods with an emphasis on enhancing feature extraction and matching algorithms to increase system robustness and accuracy.
The study offers insightful information on real-world deployment challenges, like noise and distortion in fingerprint photos, and proposes cutting-edge solutions to address these problems, improving system dependability and recognition

[1]Department of CS&E, Jain Institute of Technology, Davangere
[2,3]Department of CS&E, Sri Krishna Institute of Technology, Bangalore
[4]Department of CS&E, Sri Siddhartha Institute of Technology, Tumkur
[5]Department of AI&DS, Maharaja Institute of Technology Thandavapura, Mysore
[6]Department of IS&E, Jain Institute of Technology, Davangere

rates. Authors [19] give a thorough rundown of fingerprint recognition methods, including minutiae-based and ridge-based approaches, and describe the development of feature extraction techniques and matching algorithms. The authors also cover problems like as picture quality, distortions, and the effect of aging on fingerprint features, as well as the difficulties in attaining high accuracy and resilience. There are many face recognition based applications [22]. These applications are suffering from spoofing issues. To improve the detection of spoofing attempts in biometric authentication, Author [20] suggests a sophisticated multi view biometric system that incorporates several camera views. By successfully differentiating between real and fake biometric characteristics, the study presents a revolutionary method that increases the precision and dependability of biometric systems, especially in face and fingerprint recognition. The susceptibility of face recognition and face anti-spoofing systems to adversarial assaults is examined by Zhou et al.,[21] who show how these attacks may simultaneously fool spoof detection systems and recognition models. In order to guarantee the security and dependability of facial biometric systems in practical applications, the study highlights the necessity for stronger defences against hostile perturbations.

1.3Structural Similarity Index (SSIM)

In image processing, structural similarity of pictures has been compared using image similarity metrics as MSE (Mean Squared Error) and SSIM (Structural Similarity Index). The authors [17] compare the altered time series images using these techniques. By assessing structural information, brightness and contrast, SSIM in particular has demonstrated efficacy in capturing perceptual quality, which makes it appropriate for time series exhibiting intricate, nonlinear patterns.

1.4Histogram based Similarity Index

Histogram indicates the intensity distribution among the components of any object. It has been employed in number of recent research activities [15][16]. The similarity measure between two images looks simple during its quotient estimation but not even acceptable whenever images are from different colour spaces. Hence author [14] has involved the best six colour spaces to convert the images into standard ones then processed for similarity measures.

2.METHODOLOGY

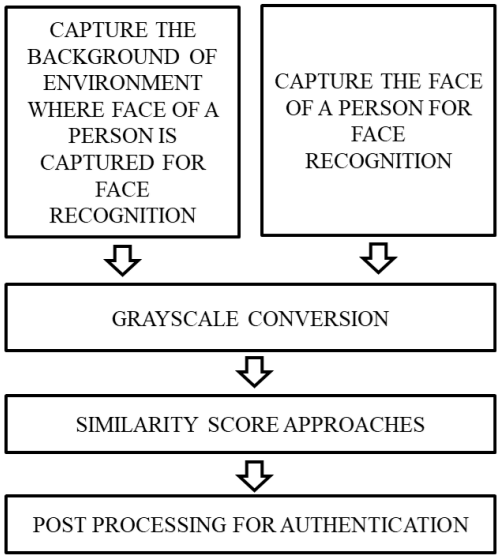

Figure 1. Methodology for background based authentication for face recognition systems using histogram technique.

Capture the background of environment where face of a person is captured for face recognition: The proposed methodology is authenticating physical presence of a person during face capture for face recognition is mainly depends on the background of environment where the face of a person is captured for face recognition.

Figure 2 is depicting the process of capturing the background for authentication before to capture face for face recognition through camera device. This process should be conducted before the face capture for face recognition.

Capture the face of a person for face recognition: Face of a person is a major component for face recognition process. The proposed methodology is insisting to capture the face of a person along with environment background. Figure 1 depicts the process of capturing face with background through camera device.

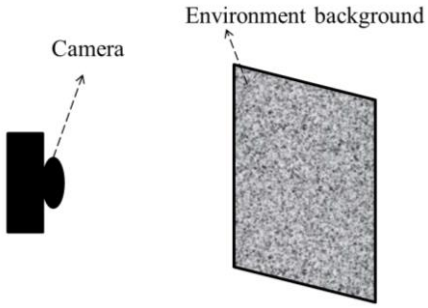

Figure 2. Process of environment background capture

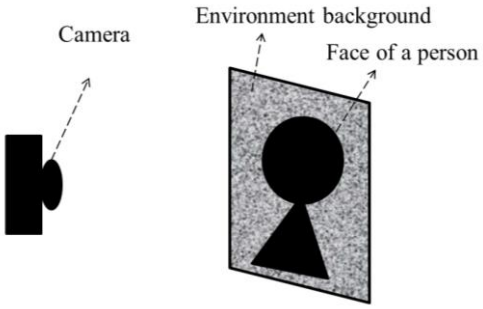

Figure 3. Process of face capture along with environment background

Similarity Score approaches: As mentioned in the literature Structural Similarity Index (SSIM) and Histogram based Similarity Index were involved to estimate similarity score between two given images that is face with background and another only background.

Authentication processing: The similarity index between two images indicates the presence of face during face recognition process. Threshold can be fixed based on the similarity model.

3.RESULTS AND DISCUSSIONS

The main title is centred, and in times new roman 14-point, boldface type. Only the first letter of the first word in the title needs to be capitalized except for the letters and words that are originally capitalized. Leave one blank lines after the title.

Figure 1 shows the images of faces along with backgrounds captured using mobile camera. Figure 2 shows only the backgrounds captured before the face capture.

Figure 4. Faces with background by name dee.jpg and jee.jpg

Figure 5. backgrounds without faces by name bk1.jpg and bk2.jpg

Table 1 Results of Histogram based similarity index

	dee.jpg	**jee.jpg**	**bk1.jpg**	**bk2.jpg**
dee.jpg	1.0	-0.20	0.006	-0.098
jee.jpg	-	1.0	-0.123	0.325
bk1.jpg	-	-	1.0	-0.025
bk2.jpg	-	-	-	1.0

Table 1 depict the results obtained through histogram based similarity index estimation between images. In the proposed experiment total four images are taken, two with faces and other two are only with corresponding backgrounds. Figure 6 depict the heatmap between two images of all combinations. As an experiment the similarity index with all other images were estimated and found an interesting results. Heatmap clearly shows the similarity exists between the face background and its actual background image. For example jee.jpg with bk2.jpg and dee.jpg with bk1.jpg. At the same time the indices are negative with other combination of images. The positive index indicates the existence of partial similarity between images. Also it proves that the face is present during its capture and avoids snoofing attacks. Other side, the negative indices indicate that no similarity between images says face absence during capture or image is simulated for fake authentication.

Figure 6. Heatmap or correlation matrix plot for Table 1

Table 2 Results of Structural Similarity Index (SSIM)

	dee.jpg	**jee.jpg**	**bk1.jpg**	**bk2.jpg**
dee.jpg	1.00	0.47	0.72	0.47
jee.jpg	-	1.00	0.58	0.42
bk1.jpg	-	-	1.00	0.62
bk2.jpg	-	-	-	1.00

Figure 7 shows the heatmap generated for the data mentioned in Table 2. Table 2 contains similarity indices obtained between images as shown in Figure 1 and Figure 2. These similarities are estimated using SSIM and Histogram based Similarity Index approaches. The heatmap shown in Figure 7 indicates a similarity between all image combinations, which is not accurate. Hence SSIM is not suitable for the proposed experiment.

4.CONCLUSION

This paper explored background-based authentication techniques for face recognition systems. In order to assess the efficacy of various picture similarity metrics, this study investigated background-based authentication strategies for face recognition systems. Because of its inability to precisely capture minute changes in background information, our tests showed that the Structural Similarity Index Measure (SSIM) is not a good fit for the suggested approach. The

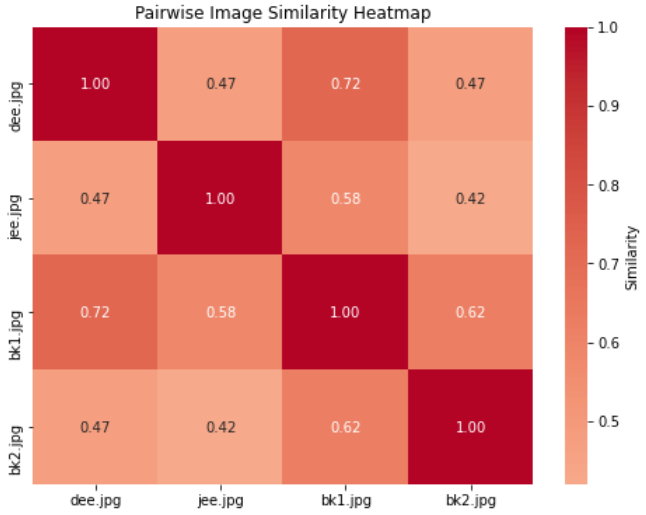

Figure 7. Heatmap or correlation matrix plot for Table 2

Histogram-based Similarity Index, on the other hand, produced noticeably superior outcomes. The Histogram-based Similarity Index approach demonstrated a higher capacity to differentiate between faces and background variations by examining the distribution of pixel intensities within the background region, producing more trustworthy authentication results. The difficulties presented by environmental changes, including changes in illumination or partial occlusions, which are frequently encountered in real-world circumstances, were more easily overcome by this method. These results lead us to the conclusion that a more promising approach to background-based authentication in face recognition systems is provided by the Histogram-based Similarity Index. Future research might improve this approach even further by adding more context-aware strategies to boost system resilience and performance under various circumstances.

REFERENCES

[1] Best-Rowden L, Jain A K. Longitudinal Study of Automatic Face Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 40(1), pp. 148-162.
[2] Zaaraoui H, Saaidi A, Alami R E, et al. A New Local Descriptor Based on Strings for Face Recognition. Journal of Electrical and Computer Engineering, 2020, 2020, pp. 1-10.
[3] J. Yan, Z. Lei, L. Wen, and S. Li, “The fastest deformable part model for object detection,” in IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 2497-2504.
[4] Mishra, Sidharth & Sarkar et. al.(2017). Principal Component Analysis. International Journal of Livestock Research. 1. 10.5455/ijlr.20170415115235.
[5] A. Sarsenov and K. Latuta, "Face Recognition Based on Facial Landmarks," *2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT)*, Moscow, Russia, 2017, pp. 1-5, doi: 10.1109/ICAICT.2017.8687015.
[6] Guodong Guo, S. Z. Li and Kapluk Chan, "Face recognition by support vector machines," *Proceedings Fourth IEEE International Conference on Automatic Face and Gesture Recognition (Cat. No. PR00580)*, Grenoble, France, 2000, pp. 196-201, doi: 10.1109/AFGR.2000.840634.
[7] Jain, Vidit, and Erik Learned-Miller. Fddb: A benchmark for face detection in unconstrained settings. Vol. 2. No. 6. UMass Amherst technical report, 2010.
[8] Yang, Shuo, et al. "Wider face: A face detection benchmark." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.
[9] Hörmann, Stefan, et al. "Face Morphing: Fooling a Face Recognition System Is Simple!." arXiv preprint arXiv:2205.13796 (2022).
[10] Cauli, Nino & Ortis, Alessandro & Battiato, Sebastiano. (2022). Fooling a Face Recognition System with a Marker-Free Label-Consistent Backdoor Attack. 10.1007/978-3-031-06430-2_15.
[11] Cheng-kun Jia, Min Long, Yong-chao Liu, Enhanced face morphing attack detection using error-level analysis and efficient selective kernel network,Computers & Security,Volume 137, 2024,103640, ISSN 0167-4048,
[12] Anirudha B Shetty, Bhoomika, Deeksha, Jeevan Rebeiro, Ramyashree, Facial recognition using Haar cascade and LBP classifiers, Global Transitions Proceedings, Volume 2, Issue 2, 2021, Pages 330-335, ISSN 2666-285X
[13] Obaida, Tameem Hameed, Nidaa Flaih Hassan, and Abeer Salim Jamil. "Comparative of Viola-Jones and YOLO v3 for Face Detection in Real time." vol 22 (2022): 63-72.
[14] Lee, S. M., Xin, J. H., & Westland, S. (2005). Evaluation of image similarity by histogram intersection. Color Research & Application, 30(4), 265–274. doi:10.1002/col.20122.
[15] Roy, Santanu, Kanika Bhalla, and Rachit Patel. "Mathematical analysis of histogram equalization techniques for medical image enhancement: a tutorial from the perspective of data loss." Multimedia Tools and Applications 83.5 (2024): 14363-14392.

[16] Sun, Shangquan, et al. "Restoring images in adverse weather conditions via histogram transformer." European Conference on Computer Vision. Springer, Cham, 2025.
[17] Liu, Yuhan, and Ke Tu. "TS3IM: Unveiling Structural Similarity in Time Series through Image Similarity Assessment Insights." arXiv preprint arXiv:2405.06234 (2024).
[18] Abdulameer, Firas S. "Developing and valuation for techniques fingerprint recognition system." Journal of the College of Basic Education 30.123 (2024): 29-45.
[19] Jain, Anil K., et al. "Fingerprint recognition." Introduction to Biometrics. Cham: Springer International Publishing, 2024. 75-117.
[20] Asmitha, P., et al. "Improved multiview biometric object detection for anti spoofing frauds." Multimedia Tools and Applications (2024): 1-17.
[21] Zhou, Fengfan, et al. "Adversarial Attacks on Both Face Recognition and Face Anti-spoofing Models." arXiv preprint arXiv:2405.16940 (2024).
[22] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). "Face recognition: A literature survey." ACM Computing Surveys (CSUR), 35(4), 399-458.

Authors

Dr. Mouneshachari S received the B.Eng. degree in Computer Science and Engineering from Kuvempu University, India, in 2000 and the M.Tech in Computer Science and Engineering from VTU, Belagavi, India and Ph.D. degree in Computer Science and Engineering from Jain University, Bengaluru, India in 2017. Currently, he is working as Professor at the Department of Computer Science and Engineering under VTU, Belagavi, India. His research interests include Cybersecurity, Internet of Things, EEG Analysis and Cloud computing. Also he has developed software solutions to societal and organization challenges. He is a reviewer for many reputed national and international journals and conferences.
Email: drmounesh.cs@gmail.com.

Poornima G J working as Assistant Professor, Department of CS&E, Sri Krishna Institute of Technology, Bengaluru. Her research interests include Computer Networks, Network Security, Deep Learning, Artificial Intelligence. Email: poornima.gj@gmail.com

Roopa Banakar working as Assistant Professor in Department of IS&E under VTU, Belagavi, India. Her research interest includes Artificial Intelligence, Machine Learning, Deep Learning, Computer Networks. Email: rp.banakar@gmail.com

Bharathi N Currently working as a Asst.Professor at Dept of CS&E at SSIT, Tumkur, India. Her research interests include Machine learning, NLP, IOT and Image processing
Email: bharathinghorpade@gmail.com

Dr. Swarnalatha K currently serving as the HoD of AI and DS at Maharaja Institute of Technology, Thandavapura, Mysore. Dr. Swarnalatha K has been recognized with several accolades, including Best Mentor, Best Paper Award, and certification as an International Educator. Email: swarnapradyu@gmail.com

Swetha B S currently working as Assistant Professor in Department of IS&E, Jain Institute of Technology, Davangere, India. Her research interests include Image processing, Internet of Things, Cybersecurity and Cloud computing.
Email: shwemouni@gmail.com