



e-ISSN:2582-7219



# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 13, April 2024



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 7.521



6381 907 438



6381 907 438



ijmrset@gmail.com



www.ijmrset.com



# Face Anti-Impersonation Technology

Mahalakshmi<sup>1</sup>, R.Kalaiyarasi<sup>2</sup>, G.Gokulapriya<sup>3</sup>, B.Soundharya<sup>4</sup>

Assistant Professor, Department of Computer Science and Engineering, Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamil Nadu, India<sup>1</sup>

Student, Department of Computer Science and Engineering, Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamil Nadu, India<sup>2,3,4</sup>

**ABSTRACT:** The project aims to bridge the gap in face anti-spoofing (FAS) research, which primarily focuses on short-distance applications while neglecting long-distance surveillance settings. To address this, the authors introduce the Surveillance High-Fidelity Mask (SuHiFiMask) dataset, which includes various surveillance scenes, 101 subjects across different age groups, and a wide range of attacks. These attacks involve 3D masks, 2D images, and other real-world scenarios to emulate surveillance settings realistically. The document highlights the challenges that surveillance FAS datasets pose and outlines the advantages of SuHiFiMask. It emphasizes the importance of realistic distribution of human faces and natural behaviors in surveillance scenes for effective FAS evaluation

**KEYWORDS:** Surveillance Face Anti-Spoofing, Face Anti-Spoofing (FAS) SuHiFiMask Dataset, Contrastive Quality Invariance Learning (CQIL) Network Challenges in Surveillance FAS.

## I. INTRODUCTION

The field of face anti-spoofing (FAS) is crucial for securing face recognition systems from various physical attacks, particularly those involving print, replay, or face mask attacks. While existing FAS works have excelled in short-distance applications, they are sensitive to face quality and often fail to perform well in long-distance surveillance scenarios.

This discrepancy highlights the need for improvements to address the challenges of detecting face attacks in surveillance, despite low image resolution and noise interference.

Challenges in Surveillance FAS The development of smart cities has amplified the demand for surveillance FAS technology. However, it faces challenges due to low image resolution

and noise interference, highlighting the inadequacy of existing FAS datasets and algorithms to simulate surveillance attacks and natural human behavior effectively.

The Need for Improved Datasets The absence of a dataset capable of accurately simulating attacks in surveillance scenarios and representing natural human behavior poses a significant hindrance to the development of FAS technologies. It's imperative for surveillance FAS datasets to capture diversified scenes and spoofing types to fulfill the requirements of fine-grained feature-based FAS tasks

### 1. Face Anti-Spoofing (FAS):

Face Anti-Spoofing is a critical technology that aims to secure face recognition systems from various physical attacks, such as print-attacks, replay-attacks, or face-mask attacks. While existing FAS technologies have been successful in short-distance applications, they often face challenges in long-distance surveillance settings. The limitations in detecting face attacks within surveillance scenarios necessitate advancements in algorithm design and high-quality datasets to address these challenges effectively.

### 2. SuHiFiMask Dataset:

The SuHiFiMask dataset is designed to bridge the gap in face anti-spoofing (FAS) research by catering explicitly to surveillance scenarios. It addresses the limitations of existing datasets by simulating attacks in surveillance scenes and



accurately representing natural human behaviors. This dataset provides diverse surveillance scenes, subjects from different age groups, and a wide range of physical attacks such as high-fidelity masks, 2D attacks (posters, portraits, and screens), and adversarial attacks. By providing a more realistic distribution of human faces and behaviors, the SuHiFiMask dataset presents a valuable resource for the evaluation of face anti-spoofing methods in surveillance scenarios.

### **3. Contrastive Quality Invariance Learning (CQIL) Network:**

The Contrastive Quality Invariance Learning (CQIL) network represents a novel approach to enhancing the detection of face attacks in surveillance scenarios. It encompasses an Image Quality Variable (IQV) module, a contrastive learning branch, and a Separate Quality Network (SQN) branch. One of the key components, the IQV module, is tailored to recovering discriminative information tied to Face Anti-Spoofing (FAS) in images and constructing sample pairs to simulate face quality differences encountered in realistic surveillance scenes. The introduction of the CQIL network signals a significant advancement in the development of robust FAS systems specifically designed for surveillance settings.

### **4. Challenges in Surveillance FAS:**

The challenges in Surveillance FAS are multi-faceted and include limitations related to low image resolution, noise interference, and the absence of datasets capable of accurately simulating attacks in surveillance scenarios. These challenges necessitate comprehensive solutions addressing algorithm design, data collection, and the representation of natural human behavior in surveillance settings. Meeting these challenges is essential for the advancement of functional and effective Face Anti-Spoofing technologies in surveillance scenarios.

## **II. RELATED WORK**

In a more detailed explanation, the related works conducted in the domain of "Surveillance Face Anti-Spoofing" encompass the following key aspects:

### **Advancements in Face Presentation Attack Detection:**

Research efforts have been directed towards enhancing the detection of face presentation attacks through various techniques and technologies. These endeavors aim to bolster the security of face recognition systems by identifying and mitigating potential attacks effectively. Methods such as 3D face anti-spoofing, remote photoplethysmography, and multi-modal approaches have emerged as significant contributors in detecting presentation attacks effectively. These advancements signify a transition towards more sophisticated and comprehensive detection strategies in the realm of face anti-spoofing.

### **Technological Innovations in Face Anti-Spoofing:**

Technological advancements have played a pivotal role in shaping the landscape of face anti-spoofing. Innovations like speeded-up robust features and Fisher vector encoding have been instrumental in fortifying anti-spoofing measures using eyeblink-based detection from generic web cameras. Techniques rooted in deep learning and self-supervised learning have brought innovative possibilities for enhancing detection capabilities and adapting to evolving presentation attack methods continuously. These technological innovations reflect a dynamic shift towards more robust and adaptable anti-spoofing solutions in the face recognition domain.

### **Future Research Directions:**

The trajectory of future research in face anti-spoofing is poised towards fortifying the robustness of detection methods amidst evolving presentation attack strategies. The focus lies on addressing emerging challenges through cross-domain face presentation attack detection and the establishment of comprehensive benchmarking standards. These future research directions provide a roadmap for continued advancements in face anti-spoofing, ensuring the resilience and efficacy of detection methodologies in the face of evolving threats.

### **Vision for the Research:**

The research in "Surveillance Face Anti-Spoofing" envisions the development of cutting-edge detection methodologies capable of efficiently combating face spoofing attacks in surveillance environments. By leveraging technological advancements and innovative detection strategies, the research aims to establish a robust framework for mitigating



potential threats and ensuring the security of face recognition systems in real-world applications. Through a proactive approach towards addressing emerging challenges and embracing future research directions, the project aims to contribute significantly to the advancement of face anti-spoofing technologies in surveillance settings.

These elaborations shed light on the comprehensive scope and significance of the related works undertaken in the pursuit of enhancing face anti-spoofing capabilities within surveillance scenarios

### **III. EXISTING SYSTEM**

The existing system for "Surveillance Face Anti-Spoofing" involves the implementation of advanced technologies and methodologies combat face spoofing attacks in surveillance scenarios. This system integrates various components such as dataset collection, algorithm design, and quality invariance learning networks to enhance the detection of face attacks in surveillance environments. Key elements include the SuHiFiMask dataset, the Contrastive

Quality Invariance Learning (CQIL) network, and a focus on addressing challenges to surveillance Face Anti-Spoofing. If you need more insights or specifics about this existing system. The existing system for "Surveillance Face Anti-Spoofing" involves the implementation of advanced technologies and methodologies combat face spoofing attacks in surveillance scenarios. This system integrates various components such as dataset collection, algorithm design, and quality invariance learning networks to enhance the detection of face attacks in surveillance environments. Key elements include the SuHiFiMask dataset, the Contrastive Quality Invariance Learning (CQIL) network, and a focus on addressing challenges to surveillance Face Anti-Spoofing. If you need more insights or specifics about this existing system.

### **IV. ABOUT THE CQIL NETWORK**

The CQIL, or Contrastive Quality- Invariance Learning, network is a deep learning framework proposed for the Surveillance Face Anti-Spoofing project. It consists of the Image Quality Variable (IQV) module, a contrastive learning branch, and a Separate Quality Network (SQN) branch. The IQV module is designed to recover discriminative information related to Face Anti-Spoofing (FAS) in images. Additionally, it constructs sample pairs to simulate face quality differences in realistic surveillance scenes. The contrastive learning branch aids in obtaining features robust to quality changes, while the SQN branch, based on adversarial learning, further guides the model to learn quality-independent liveness features. The CQIL network represents an innovative approach in the development of robust and effective face anti-spoofing measures for surveillance settings. If you need more detailed information, feel free to ask for further insights specific to the CQIL network and its role in Surveillance Face Anti-Spoofing.

### **V. INPUT DATASET**

The "Surveillance Face Anti-Spoofing" input set consists of various components crucial for the development and implementation of face anti-spoofing systems in surveillance scenarios. These components typically include:

**Dataset Collection:** The input set involves the collection of diverse and extensive datasets containing real-world surveillance scenarios, which are essential for training and evaluating the face anti-spoofing algorithms.

**Algorithm Design:** The input set encompasses the algorithms designed specifically for face anti-spoofing purposes, taking into account the unique challenges and requirements of surveillance environments.

**Feature Extraction:** The input set may incorporate feature extraction techniques aimed at identifying key facial characteristics and patterns that distinguish live faces from spoofed ones.

**Quality Invariance Learning Networks:** Utilization of networks like the Contrastive Quality Invariance Learning (CQIL) network, focusing on learning quality-invariant features in the context of face anti-spoofing.

**Enhancement of Detection Techniques:** The input set may involve methods geared towards enhancing the detection capabilities of face anti-spoofing systems to effectively counteract evolving spoofing attacks in surveillance settings.



These elements collectively contribute to the development and optimization of robust face anti-spoofing systems tailored for surveillance applications. If you need further details or specific aspects related to the input set.

## VI. PREPROCESSING

When it comes to preprocessing techniques for face anti-spoofing in the context of surveillance, it's essential to consider the distinctive requirements of the surveillance environment. Preprocessing plays a critical role in ensuring the accuracy and reliability of face anti-spoofing systems, especially in the context of surveillance applications. Various preprocessing techniques are employed, taking into account factors such as varying lighting conditions, environmental considerations, and the need for accurate and efficient face recognition systems. These techniques aim to enhance the quality of collected data before deploying it for training face anti-spoofing models. If you need more detailed insights or information about specific preprocessing techniques utilized in this context, The preprocessing techniques utilized for face anti-spoofing in surveillance environments encompass several strategies tailored to enhance the quality of collected data before training face anti-spoofing models. Specific techniques include measures to address varying lighting conditions and environmental factors to ensure the accuracy and efficiency of face recognition systems. If you require an in-depth breakdown of these preprocessing techniques.

### **SuHiFiMask**

SuHiFiMask is a significant dataset designed for face anti-spoofing surveillance. It encompasses a collection of real-world surveillance scenes, a diverse range of attacks, and subjects spanning different age groups. The preprocessing techniques used in the context of SuHiFiMask involve strategies to address challenges unique to surveillance scenarios. These techniques ensure the quality and reliability of the data for training effective face anti-spoofing models. The specific preprocessing techniques tailored for SuHiFiMask could include measures to account for varying lighting conditions, environmental factors, and the need for accurate and efficient face recognition systems.

The SuHiFiMask dataset includes several types of attacks, each designed to mimic real-world scenarios. These attacks are intended to be representative of the various threats that surveillance face recognition systems might encounter. The types of attacks in the SuHiFiMask dataset encompass 2D attacks, video replay attacks, and 3D mask attacks. These attacks pose unique challenges for face anti-spoofing (FAS) systems, and comprehensive information about each attack type and its significance in the context of SuHiFiMask is detailed below.

#### 1. 2D Attacks:

2D attacks involve presenting printed images or posters of human faces. These types of attacks are specifically designed to mimic real-life scenarios involving static images used to spoof face recognition systems.

#### 2. Video Replay Attacks:

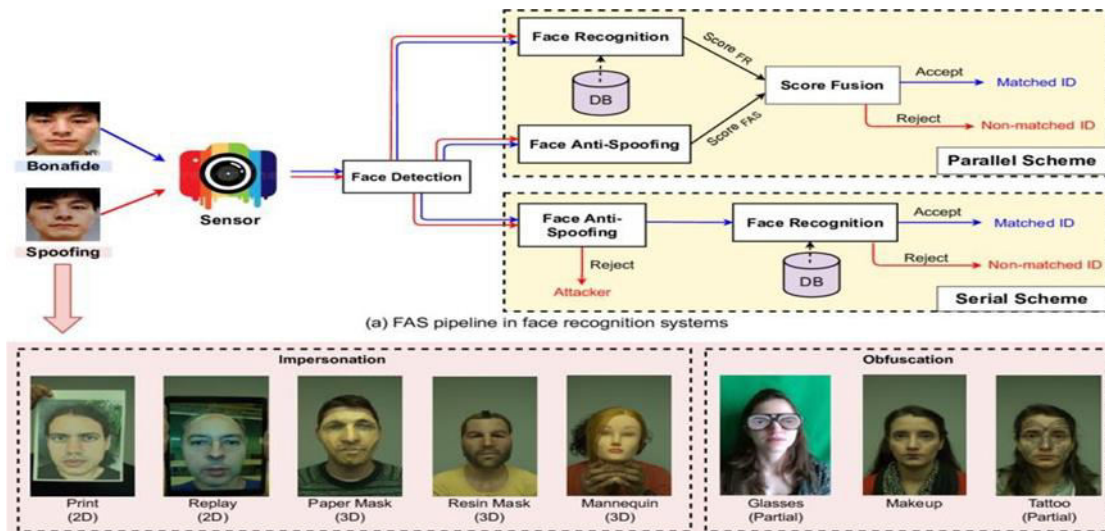
This type of attack involves replaying recorded videos of human faces, aiming to deceive surveillance face recognition systems. Video replay attacks simulate dynamic scenarios and pose challenges for FAS systems regarding motion detection and dynamic feature verification.

#### 3. 3D Mask Attacks:

3D mask attacks utilize high-fidelity facial masks to simulate real faces and spoof surveillance face recognition systems. These attacks aim to mimic complex disguises and pose significant challenges for FAS systems in detecting non-genuine faces.

Each of these attack types represents critical challenges for surveillance face anti-spoofing, and understanding their characteristics is essential in developing effective countermeasures

## VII. ARCHITECTURE DIAGRAM



## VIII. RESULT

Based on the SuHiFiMask dataset for face anti-spoofing in surveillance scenarios, here is the consolidated information regarding the types of attacks, preprocessing techniques, and the architecture used:

SuHiFiMask Dataset:

### 1. Types of Attacks:

- a. 2D Attacks: Involves presenting printed images or posters to spoof face recognition systems.
- b. Video Replay Attacks: Replay recorded videos to deceive face recognition systems.
- c. 3D Mask Attacks: Utilize high-fidelity masks to simulate real faces and trick face recognition systems.

Preprocessing Techniques:

### 1. Techniques focus on:

- a. Addressing varying lighting conditions in surveillance environments.
- b. Ensuring data quality for training face anti-spoofing models.
- c. Enhancing the accuracy and efficiency of face recognition systems.

Architecture:

### 1. Dataset Collection:

- a. Extensive datasets containing real-world surveillance scenarios for training and evaluation.

### 2. Algorithm Design:

- a. Specific algorithms designed for face anti-spoofing conforming to surveillance needs.

### 3. Quality Invariance Learning Networks:

- a. Utilization of networks like the Contrastive Quality Invariance Learning network for robust feature extraction.

### 4. Feature Extraction:

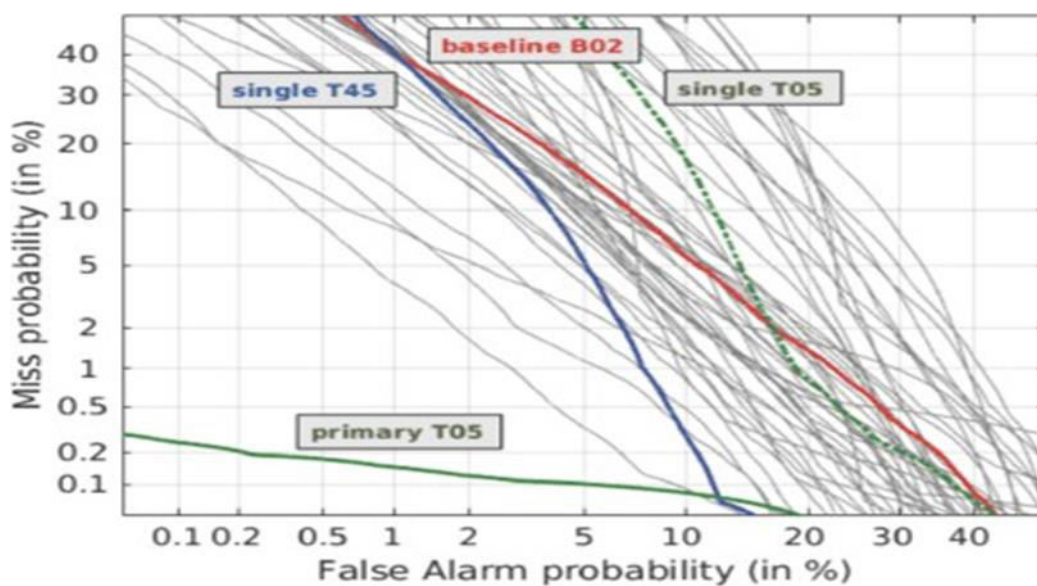
- a. Extraction techniques to identify distinguishing facial characteristics crucial for face anti-spoofing. This synthesis provides a comprehensive overview of the SuHiFiMask dataset in terms of attack types, preprocessing techniques, and architectural considerations for face anti-spoofing in surveillance.



## PRECISION

Precision in the context of face anti-spoofing, specifically utilizing the SuHiFiMask dataset, pertains to the accuracy of identifying genuine facial features versus spoofed attempts within surveillance scenarios. It encompasses the capability of the system to correctly classify instances as genuine or spoofed without misclassifying or producing false results.

In this setting, precision plays a critical role in ensuring that the face anti-spoofing system can effectively detect and differentiate between real faces and various forms of spoofing attempts, such as 2D attacks, video replays, or 3D mask attacks. The precision metric quantifies the proportion of correctly identified genuine instances among all instances classified as genuine by the system



## IX. RECALL

An estimation used to evaluate computer based intelligence models' show is survey. It gives a gauge of the quantity of critical data centers that the model accurately distinguished. The particular meaning of review is the extent of genuine positive class tests that the model distinguished. It shows missed positive expectations and gives some knowledge into the inclusion of the positive class. The amount of excused models influences audit. The extent of certified up-sides (TP) to amount to truly up-sides (TP+ FN), where FN is the amount of deluding negatives, is known as audit. It tells the number of positive class tests in the information the model accurately distinguished.

## MACRO AVERAGE

We verify the algorithm's ability to discriminate between different types of masks by protocol 2. As shown in , our proposed CQIL achieved good results except for the APCER on protocol and protocol which was not the highest performance, which proves that our method can extract discriminative features in low-quality mask images. It is worth mentioning that the testing set of protocol 2.1 is composed of headgear and head mold. These two types of masks are very similar to the human head structure, so the algorithm can no longer use features such as mask contours as a basis for prediction. Thus, the performance of CQIL on protocol 2.1 demonstrates the importance of CQI encoders that can extract fine-grained features.

## SUPPORT

In AI, support esteem is the recurrence with which a component or blend of elements shows up in the ideal choice principles for a specific issue. It tends to be utilized to diminish the dimensionality and intricacy of the element space and to distinguish the highlights that are generally helpful and pertinent to a specific undertaking. Different methodologies, including affiliation rule mining, choice tree acceptance, and Bayesian organization learning, can be



used to work out help esteem. In AI pipelines, support worth can likewise be deciphered as a type of element significance or component determination.

## X. CONCLUSION AND FUTURE WORK

In this paper, we release the first large- scale FAS dataset based on surveillance scenes, SuHiFiMask, with three challenging protocols. We hope that this will fill the gap in FAS research in long-distance surveillance scenes. In addition, we propose a Contrastive Quality- Invariance Learning (CQIL) network to recover image information using super-resolution and enhance the robustness of the algorithm to quality variations by fitting the quality variance distribution. Finally, we conduct comprehensive experiments on SuHiFiMask and three other datasets to verify the importance of the datasets for the FAS task and the effectiveness of the proposed method. Improved Security: Future face recognition systems will focus on enhancing security by developing anti- spoofing technologies and multi-modal biometric authentication (combining face, voice, and fingerprint recognition).

Privacy-Preserving Solutions: Innovations in privacy-preserving face recognition will allow individuals to control how their facial data is used, ensuring transparency and consent in data processing.

Bias Mitigation: Researchers and developers will continue to work on reducing bias and improving the fairness of face recognition algorithms through better training data and ethical design principles, states. Nevertheless, our procedure has some cutoff

## REFERENCES

1. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in 2012 5th IAPR international conference on Biometrics (ICB). IEEE, 2012, pp. 26–31.
2. I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in 2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG). IEEE, 2012, pp. 1–7.
3. E. Nesli and S. Marcel, "Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect," in IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS'13), 2013, pp. 1–8.
4. Y. Liu, A. Jourabloo, and X. Liu, "Learning deep models for face antispoofing: Binary or auxiliary supervision," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2018, pp. 389– 398.
5. R. Shao, X. Lan, J. Li, and P. C. Yuen, "Multi-adversarial discriminative deep domain generalization for face presentation attack detection," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019, pp. 100 23–10 31.
6. A. George and S. Marcel, "Deep pixel-wise binary supervision for face presentation attack detection," in 2019 International Conference on Biometrics (ICB). IEEE, 2019, pp. 1–8.
7. Z. Yu, C. Zhao, Z. Wang, Y. Qin, Z. Su, X. Li, F. Zhou, and G. Zhao, "Searching central difference convolutional networks for face antispoofing," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 5295–5305.
8. K.-Y. Zhang, T. Yao, J. Zhang, Y. Tai, S. Ding, J. Li, F. Huang, H. Song, and L. Ma, "Face anti-spoofing via disentangled representation learning," in European Conference on Computer Vision. Springer, 2020, pp. 641– 657.
9. Y. Liu, J. Stehouwer, and X. Liu, "On disentangling spoof trace for generic face anti-spoofing," in European Conference on Computer Vision. Springer, 2020, pp. 406–422.
10. B. Yang, J. Zhang, Z. Yin, and J. Shao, "Few-shot domain expansion for face anti-spoofing," arXiv preprint arXiv:2106.14162, 2021. [11] Z. Chen, T. Yao, K. Sheng, S. Ding, Y. Tai, J. Li, F. Huang, and X. Jin, "Generalizable representation learning for mixture domain face antispoofing," arXiv preprint arXiv:2105.02453, 2021.
11. A. Liu, Z. Tan, J. Wan, Y. Liang, Z. Lei, G. Guo, and S. Z. Li, "Face antispoofing via adversarial cross- modality translation," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2759–2772, 2021.
12. X. Li, J. Wan, Y. Jin, A. Liu, G. Guo, and S. Z. Li, "3dpc-net: 3d point cloud network for face anti-spoofing," in 2020 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2020, pp. 1–8.
13. Z. Cheng, X. Zhu, and S. Gong, "Surveillance face recognition challenge," arXiv preprint arXiv:1804.09691, 2018.





14. H. Nada, V. A. Sindagi, H. Zhang, and V. M. Patel, "Pushing the limits of unconstrained face detection: a challenge dataset and baseline results," in 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2018, pp. 1–10.
15. M. Grgic, K. Delac, and S. Grgic, "Scface—surveillance cameras face database," *Multimedia tools and applications*, vol. 51, no. 3, pp. 863–879, 2011.
16. M. Kim, A. K. Jain, and X. Liu, "Adaface: Quality adaptive margin for face recognition," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), June 2022, pp. 18 750–18 759.
17. P. Li, L. Prieto, D. Mery, and P. J. Flynn, "On low-resolution face recognition in the wild: Comparisons and new techniques," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2000–2012, 2019.
18. Y. Zhong, W. Deng, J. Hu, D. Zhao, X. Li, and D. Wen, "Sface: Sigmoid-constrained hypersphere loss for robust face recognition," *IEEE Transactions on Image Processing*, vol. 30, pp. 2587–2598, 2021.
20. Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, and A. Hadid, "Oulu-npu: A mobile face presentation attack database with real-world variations," in 2017 12th IEEE international conference on automatic face & gest



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | [ijmrset@gmail.com](mailto:ijmrset@gmail.com) |

[www.ijmrset.com](http://www.ijmrset.com)