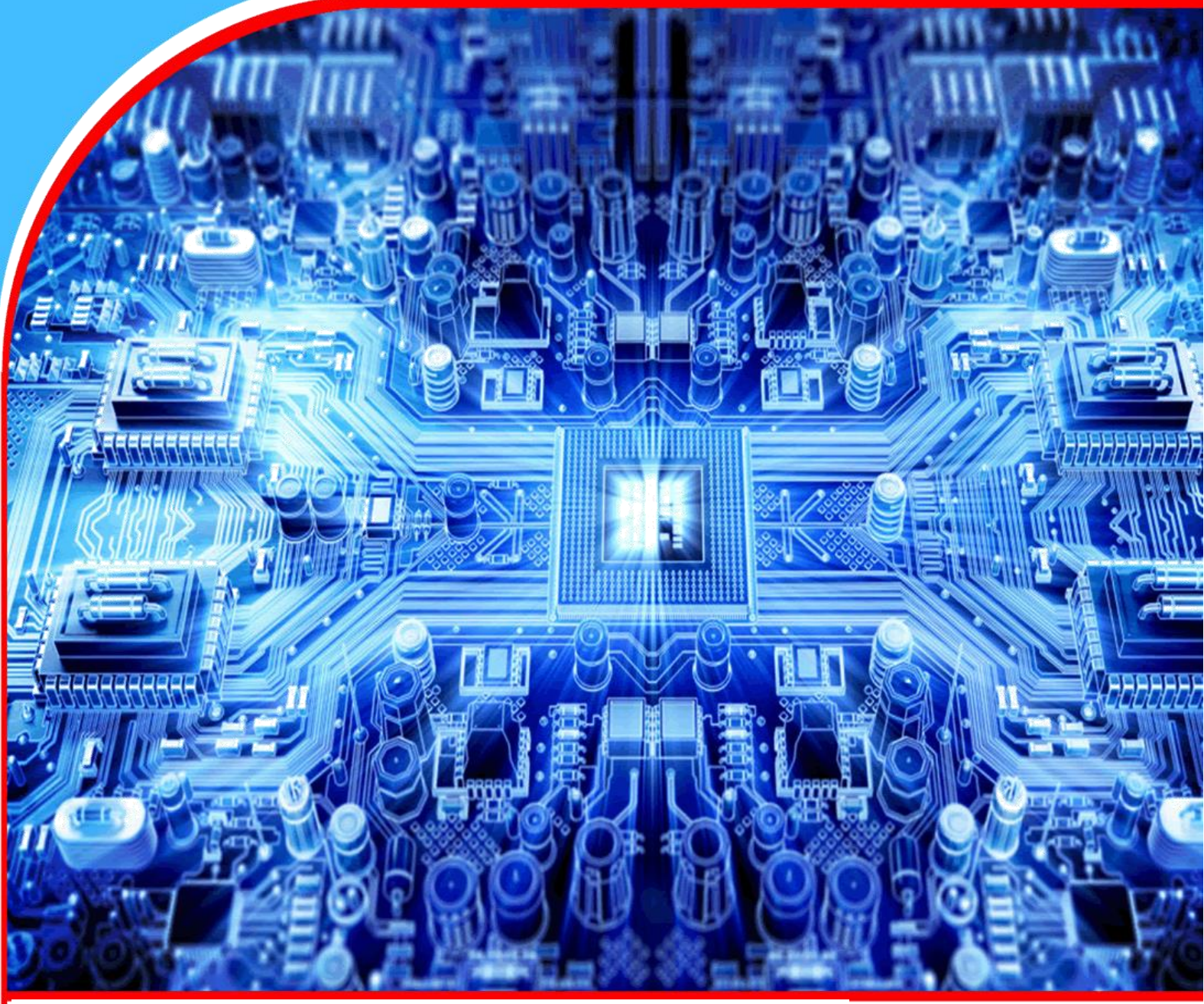
American Journal of
Computing and Engineering
(AJCE)



Biometric Presentation Attack Detection

Abdulrafiu Musa Imam

AJP

American Journal of Computing and Engineering
ISSN 2790-5586 (Online)
Vol.8, Issue 1, pp 32 – 56, 2025

www.ajpojournals.org

Biometric Presentation Attack Detection

Abdulrafiu Musa Imam
Nottingham Trent University

Abstract

Purpose: Biometric systems play a crucial role in authentication and identification processes but are vulnerable to various attacks that compromise their security and reliability. Detecting such attacks is critical to ensuring the integrity of these systems and maintaining user trust. This study focuses on detecting face presentation attacks using a cost-effective thermal sensor array. The primary goal is to combine an RGB camera, a thermal sensor array, and deep convolutional neural networks (CNNs) to differentiate between genuine face presentations and facial presentation attacks. The aim is to develop a novel biometric attack detection technique using the thermal sensor array, which is more affordable compared to other existing technologies.

Materials and Methods: The process involves the collection of 46,000 thermal images under various conditions and the application of CNN models for analysis. The thermal images are gathered under diverse lighting conditions, distances, and environments, and are then analyzed using deep learning models, specifically AlexNet and ResNet. The thermal sensor array is chosen for its cost-effectiveness.

Findings: The research findings demonstrate the effectiveness of the proposed approach in detecting attacks on biometric systems. Performance metrics such as an accuracy of 0.9671, an F1 score of 0.9893, a precision score of 0.9872, and a recall of 0.9914 highlight the robustness of the model in distinguishing between genuine and attacked presentations.

Implications to Theory, Practice and Policy:: This study contributes to the field of biometric attack detection by introducing a cost-effective approach using a thermal sensor array. It offers insights into detecting various types of attacks and highlights advancements made in the area of biometric system security. The findings have significant implications for enhancing the security and reliability of biometric systems in diverse applications.

Keywords: *Biometric Attack Detection, Face Presentation Attacks, Thermal Sensor Array, Deep Learning Models, Cost-Effective, Security, Reliability*

INTRODUCTION

Biometric attacks have become a significant challenge for both government and private institutions worldwide. Recent incidents highlight the vulnerabilities of these systems. According to media reports, the Chinese government's facial recognition-based ID authentication service was recently compromised, leading to the creation of fraudulent tax invoices worth over $76.2 million (500 million yuan) in less than two years. As reported by the *South China Morning Post*, the perpetrators generated high-resolution images of individuals mimicking natural movements such as nodding, blinking, and opening their mouths to deceive the system (Biometrics Research Group, 2021).

Similarly, researchers at the University of Adelaide in South Australia have uncovered new security risks associated with adversarial image attacks on object recognition systems, raising concerns about their implications for facial biometric security (Unite, 2021). These cases underscore the urgent need for advanced biometric attack detection systems capable of identifying and mitigating spoofing attempts. Various biometric detection methods are currently in use, including fingerprint scanning, facial and voice recognition, iris recognition, and even heart-rate sensors. Biometrics plays a crucial role in border control, e-passports, and financial sectors such as banking and insurance. The primary objective of biometric detection systems is to prevent unauthorized access to sensitive company or government databases.

This research focuses specifically on face presentation attack detection systems, aiming to enhance security against sophisticated spoofing techniques and ensure the integrity of facial recognition technology. This research aims to create a new technique for the detection of face presentation attacks at the sensor level. This will be accomplished by combining the standard RGB camera with another sensor, such as a thermal sensor array, to ascertain the liveness of the displayed object. This project is intended to primarily focus on the development of a spoof-resistant strategy for face presentation attacks, however, it is also intended to expand the project to improve the performance of the face recognition system using the low-resolution thermal image obtained from the thermal sensor array. The research involved taking different data of various attacks using the normal RGB Camera fused with a thermal sensor array. The following attacks will be considered:

i. 3D Face Mask Attacks
ii. Eye Blinking Attacks
iii. Video Replay Attacks
iv. Photo Display Attacks
v. Real Human Presentation Authentication

Despite advancements in biometric security, existing face presentation attack detection (PAD) systems remain vulnerable to increasingly sophisticated spoofing techniques. High-resolution image attacks, deepfake-based spoofs, and 3D mask attacks continue to bypass traditional detection methods. For instance, a recent large-scale fraud involving China's facial recognition-based ID authentication system demonstrated the ease with which biometric security can be compromised. Attackers successfully generated fraudulent tax invoices worth over $76.2 million (500 million yuan) by using high-resolution facial images that mimicked natural movements such as blinking and mouth opening (Biometrics Research Group, 2021). Similarly, research from the University of Adelaide in South Australia has highlighted the growing risk of adversarial image attacks on object recognition systems, raising concerns about the reliability of facial biometric

security (Unite, 2021). These incidents underscore the pressing need for more advanced and resilient biometric attack detection mechanisms.

Current biometric authentication systems primarily rely on single-modal detection met hods, such as RGB cameras, which are limited in their ability to differentiate between genuine human facial characteristics and spoofed images, masks, or video replays (Korshunov & Marcel, 2018). While some systems incorporate depth sensors or near-infrared cameras to enhance liveness detection, these approaches remain inadequate against increasingly sophisticated attack vectors (Patel et al., 2016). The primary limitation of existing methods is their inability to detect subtle yet critical physiological differences between real human faces and artificial imitations. Furthermore, most PAD techniques lack robust generalizability, reducing their effectiveness across diverse attack scenarios, as highlighted by recent studies on presentation attack detection failures (George et al., 2019).

This research seeks to address these limitations by developing an advanced face presentation attack detection system that integrates a standard RGB camera with a thermal sensor array. Unlike traditional PAD methods, which rely solely on visible spectrum data, this multi-sensor fusion approach leverages both RGB and thermal imaging to enhance security. Thermal sensor arrays provide additional liveness detection capabilities by capturing heat signatures that distinguish living human faces from non-living spoofs, a crucial improvement over existing PAD techniques (Raghavendra et al., 2015). This is particularly effective against printed photo attacks, deepfake-based spoofs, and video replay attacks, as these methods lack the natural heat emission of human skin, making them easier to detect using thermal imaging (Zhang et al., 2020). The dual-modal approach thus enhances biometric security by ensuring both structural and physiological authenticity in face recognition.

In addition to strengthening biometric security, this research aims to contribute to the broader field of face recognition by utilizing low-resolution thermal imaging to improve recognition accuracy under challenging lighting conditions. By fusing thermal and RGB data at the sensor level, this study will provide a more robust, generalizable, and resilient approach to biometric authentication. The findings will have significant implications for government agencies, border control systems, and financial institutions, where facial recognition plays a critical role in identity verification and fraud prevention (Sun et al., 2017). Through this innovative approach, the study seeks to bridge the existing gap in biometric security, offering a practical and effective solution to counter the growing threats posed by advanced biometric attacks.

Literature Review

The increasing frequency of attacks on biometric authentication systems has raised serious concerns about their reliability. To address these issues and restore public confidence, the National Institute of Standards and Technology (NIST) hosted the International Face Performance Conference (IFPC) in November 2022. This event brought together global experts to enhance transparency, trust, and understanding in face biometrics (Biometric Research Group, 2022). Biometric authentication remains widely used across various sectors, including financial services, government databases, and secure workstations, where it restricts unauthorized access through unique physiological and behavioral traits such as facial recognition, voice patterns, keyboard dynamics, and gait analysis (Wayman, 2001; Weaver, 2006).

Facial biometrics, which falls under both physiological and behavioral approaches, is central to this study. Behavioral techniques include signature recognition, voice authentication, keyboard dynamics, and gait tracking, whereas physiological methods involve fingerprint scanning, retina analysis, hand geometry, facial structure recognition, and DNA profiling. As facial biometrics continues to be implemented in border control, financial services, workstations, and online transactions, it has become a primary target for cybercriminals seeking to bypass authentication systems. Common attack methods include printed photographs, digital display attacks, video replays, and 3D mask fabrication (Raghavendra et al., 2015a). Given the rapid growth of the facial recognition market, which is now projected to reach $8.5 billion by 2025 (Markets and Markets, 2022), the urgency for more robust anti-spoofing measures has intensified.

Facial recognition spoofing has become increasingly accessible, with attackers leveraging images from mobile devices, social media, and open-source resources to generate highly deceptive face artifacts. Online tutorials detailing spoof creation have further exacerbated security risks (Mask, 2014). In response, researchers have developed various countermeasures. For instance, Galbally et al. (2014) proposed integrating liveness detection using image quality assessment metrics to differentiate genuine and fraudulent facial samples. Bakshi et al. (2020) utilized linear discriminant analysis (LDA) for facial anti-spoofing, evaluating detection accuracy with the Half Total Error Rate (HTER) and cross-dataset analysis.

Further studies have explored vulnerabilities in 3D mask-based spoofing attacks. Erdogmus and Marcel (2014) investigated the weaknesses of facial recognition systems against 3D mask spoofs using the Morpho and 3D Mask Attack Databases, offering insights into evolving attack methods. Pinto et al. (2015) introduced a video-based spoof detection algorithm, which analyzes noise patterns in restored footage to differentiate between real and fake access attempts. Similarly, Raja et al. (2015) developed an iris recognition-based presentation attack detection model by using modified Eulerian Video Magnification (EVM) to enhance subtle phase shifts in the eye region, effectively classifying normal and spoofed presentations.

With the rise of adversarial attacks and deepfake-based spoofs, deep learning models such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) have been increasingly employed in biometric security. CNN-based architectures are widely used for feature extraction and classification, offering significant improvements in facial liveness detection (Zhang et al., 2021). Additionally, GAN-based attack detection has emerged as a promising approach, where adversarial learning techniques generate synthetic attacks to enhance the robustness of biometric authentication models (Liu et al., 2022). Moreover, texture-based analysis methods—such as Local Binary Patterns (LBP) and deep texture descriptors—help distinguish real facial skin from artificial masks and digital spoofs by detecting subtle texture irregularities (Boulkenafet et al., 2016). These advancements significantly improve the ability of biometric systems to resist sophisticated attacks.

In addition to facial and video-based attack detection, researchers have explored audio-visual (AV) biometrics, which integrates voice authentication with facial recognition to improve accuracy under varying conditions. Wark et al. (1999), Sanderson and Paliwal (2004), Ben-Yacoub et al. (1999), Dieckmann et al. (1997), Chaudhari et al. (2003), and Brunelli and Falavigna (1995) have employed AV biometrics to analyze voice and lip movement synchronization for distinguishing legitimate users from impostors. This multimodal approach enhances security by mitigating vulnerabilities present in standalone face or voice recognition systems. Furthermore, biometric

security research has extended into finger vein presentation attack detection (PAD). Studies by Nguyen et al. (2013) and Raghavendra et al. (2015b) have explored unsupervised clustering methods such as K-means, Self-Organizing Maps (SOM), and K-medoids, along with neural networks, to enhance spoof detection in fingerprint-based authentication. Extensive research has been conducted on biometric attack detection, employing both software-based and hardware-based solutions. Software-based approaches include machine learning algorithms and challenge-response techniques, such as gaze collinearity detection. Meanwhile, hardware-based solutions involve light field cameras, multi-sensor cameras, and web cameras, all designed to counteract spoofing attempts like video replay, photo display, and audio-visual attacks.

Among emerging biometric security technologies, thermal imaging has demonstrated superior attack detection capabilities due to its ability to capture heat signatures that distinguish live human skin from non-living spoof artifacts. Unlike RGB-based facial recognition, which is vulnerable to printed images and deepfake attacks, thermal sensors detect infrared radiation emitted by the human body, making it nearly impossible for photo, video, or mask-based attacks to replicate (Zhang et al., 2020). The use of multi-sensor fusion combining RGB and thermal imaging significantly enhances biometric authentication accuracy, providing a robust defence against adversarial spoofing techniques. This research aims to leverage thermal sensor arrays for real-time face presentation attack detection, addressing critical vulnerabilities in current biometric security systems. By integrating deep learning-based texture analysis, GAN-based spoof detection, and multimodal fusion techniques, this study seeks to advance facial biometric authentication and improve its resilience against evolving cyber threats.

Table 2: Gaps in Biometric Attack Detection Technology

Technology	Technique/Methodology	Attacks Addressed	Advantage	Disadvantage
Multispectral Face Sensor (Zhang et al., 2011)	Captures both near-infrared and visible images, simplifying attack detection	Masks, video replay, photo display	Generalization	High sensor and computation costs; vulnerable to attacks (Ramachandra & Busch, 2017)
Light Field Camera (Raghavendra et al., 2015a)	Records direction and intensity of light	Photo display, phone attack	Generalization	High sensor and computation costs
Multispectral Face Sensor (Yi et al., 2014)	Analyzes color and texture of an image to detect attacks	Photo display	Generalization	High sensor and computation costs; vulnerable to attacks (Ramachandra & Busch, 2017)
Optical Flow (2014)	Detects eye blinks to identify attacks	Photo display	Effective for detecting photo-based attacks	Ineffective against masking and video replay attacks
Conditional Random Field (CRF)	Detects eye blinks to identify attacks	Photo display	Effective for detecting photo-based attacks	Ineffective against masking and video replay attacks
Web Camera (Institute of Electrical and Electronics Engineers, 2007)	Detects eye blinks to identify attacks	Photo display	Effective for detecting photo-based attacks	Ineffective against masking and video replay attacks
Challenge-Response with Gaze Collinearity	Uses gaze collinearity to detect spoofing	Photo display	Effective against photo display attacks	Ineffective against video-based attacks; high computational cost
Challenge-Response (Smith et al., 2015)	Uses different color displays to detect attacks	Video replay, photo display	Effective against photo display attacks	Ineffective against video-based attacks; high computational cost

Table 2 highlights the shortcomings of various biometric attack detection technologies and identifies areas requiring further research. To provide additional clarity, the literature surrounding some of these technologies is discussed below.

The challenge-response method using gaze collinearity was introduced to detect spoofing attempts through eye blinking (Ali et al., 2013). This approach involves directing the user's gaze toward groups of collinear dots on a screen, with attributes derived from gaze collinearity used to distinguish between genuine inputs and spoof attacks. However, biometric liveness detection based

on blinking has been shown to be susceptible to spoofing techniques (Ramachandra & Busch, 2017). Attackers can bypass this method by using masks with exposed eye areas to mimic blinking or by replaying video footage of a person's eyes, as illustrated in Figure 2.

Figure 3 Spoofing Attack Using Masks of Target Person with the Eyes Area Open for Blinking

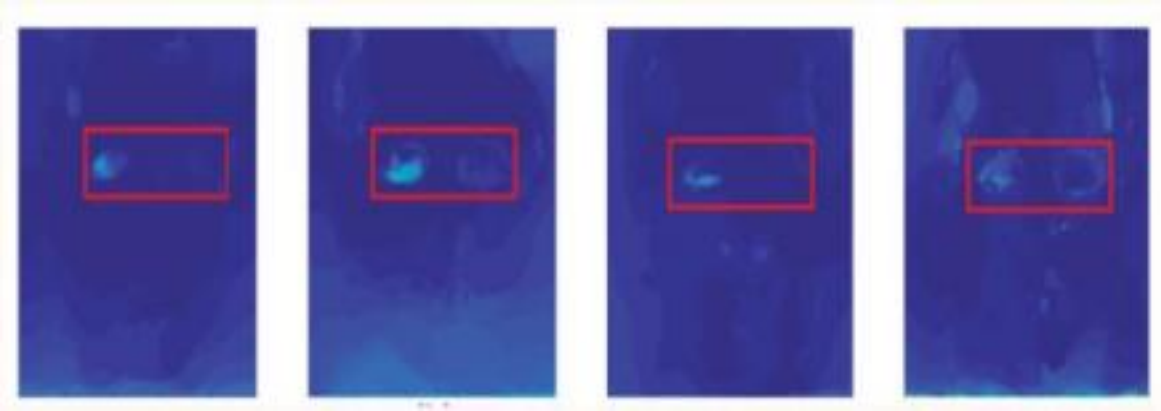


Figure 4 Spoofing Attack by Video replay to Demonstrate Eye Blinking

R. Ramachandra and C. Busch

Sensor characteristics. Cameras detect attacks based on the sensor type. This can be a light field sensor or rear-infrared or multispectral face sensor. Using a light field sensor camera (Raghavendra et al., 2015a) it records the direction and intensity of the light beam and generates numerous face pictures to reflect the depth fluctuation. The camera can detect photo or video spoofing and display an assault.

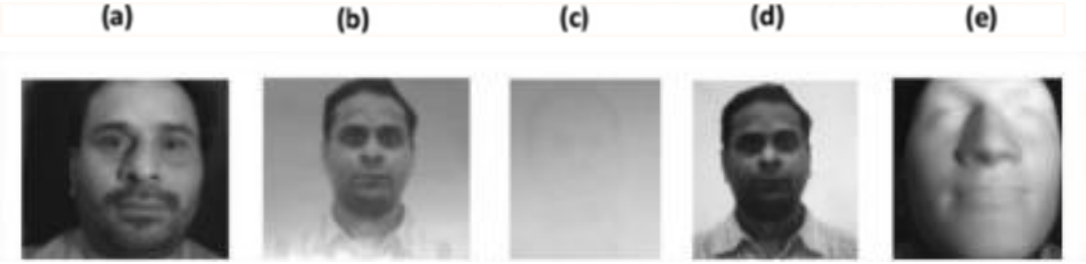


Figure 5 Images Detection Using Light Field Sensor/Rear-Infrared/Multispectral Face Sensor

R. Ramachandra and C. Busch

Figure 5 illustrates real face captures alongside attack rear-field analysis.

Among the various biometric presentation attack detection systems proposed by researchers, hardware-based approaches are considered the most reliable in mitigating attacks. However, these systems often come with high computational costs and expensive hardware. This challenge was also highlighted by Ramachandra and Busch (2017), who stated, "The adoption of hardware-based approaches may provide the necessary accuracy for detecting picture, display, and video replay attacks, but it will increase the cost and computational response time of facial recognition systems." This underscores the need for a more cost-effective and efficient hardware-based biometric presentation attack detection system.

This study proposes a novel method for sensor-based presentation attack detection. The approach involves integrating a standard RGB camera with an additional sensor, such as a thermal sensor array, to verify the presence of a live subject. While the primary objective is to develop spoof-resistant acquisition techniques for facial recognition, the project also aims to enhance the system's performance by utilizing low-resolution thermal images captured by the thermal sensor array.

A thermal sensor was chosen for this research due to its affordability and reliability. This study seeks to bridge the gap in hardware-based attack detection by providing a cost-effective yet dependable solution. The effectiveness of thermal sensors has already been demonstrated in various applications, including occupancy estimation and human segmentation (Naser et al., 2021), as well as user location tracking and home activity monitoring (Hevesi et al., 2014; Pontes et al., 2017).

Ethical and Social Impact of Artificial Intelligence in Image Recognition

The ethical and societal implications of artificial intelligence (AI) in image classification have recently gained significant attention, particularly in underrepresented and developing countries. Research conducted in the United States has shown that machine learning technologies, including image classification, can contribute to social divisions and reinforce class exclusion, disproportionately affecting minority populations (Hagerty & Rubinov, 2019).

Image classification, a core process in computer vision, involves assigning labels to images based on extracted information, linking visual content to specific class categories. In machine learning, image classification is often a form of supervised learning. Its applications extend beyond simple categorization and include face recognition, biometric attack detection, traffic regulation, and

market segmentation. These technologies are widely used in border control, banking, traffic management, and government institutions across diverse cultures and communities.

Despite the widespread adoption of image classification, machine learning, and AI technologies, ethical concerns remain a pressing issue. Ethics, in this context, refers to a set of guiding principles that emphasize values such as honesty, integrity, and fairness in the development and deployment of AI systems. Ethical considerations in AI and image classification focus on ensuring that machine learning models produce predictions that are trustworthy, comprehensible, accessible, unbiased, safe, and equitable for all users (Ajitesh Kumar, 2018).

The social implications of AI deployment relate to how these technologies affect individuals across various demographics, including factors such as ethnicity, geographical location, race, and socioeconomic status. While no universally accepted ethical framework exists for AI, Ajitesh Kumar (2018) proposed key ethical principles for image classification and machine learning:

- **Absence of Bias** – AI models should not intentionally include or exclude certain traits during training, deployment, or classification to favor specific groups while disadvantaging others. Image classification should be fair and free from preferential treatment.
- **Risk-Free AI (Safe AI)** – Models must be trained to minimize false-positive and false-negative results, which could have significant financial or human consequences. Proper governance and security measures should be implemented to regularly monitor training data and ensure the safety of life and property.
- **Explainability and Trustworthiness** – AI models should be transparent, with clearly defined functions, risks, and implications. This documentation serves to prevent legal liabilities, foster confidence among stakeholders, and ensure transparency in AI applications.
- **Trackability** – AI models should be monitored throughout their lifecycle to ensure accountability and compliance with ethical standards.
- Another widely recognized ethical framework for AI is Microsoft's "Principles of Responsible A**I"**, which serve as guidelines for ethical AI development and deployment (Adama David, 2022). These principles include:
- **Fairness** – AI technologies should be developed without bias based on race, gender, or other discriminatory factors to ensure equal opportunities for all individuals.
- **Dependability and Safety** – AI models must be reliable and designed to minimize errors and security risks.
- **Privacy and Security** – AI systems must protect user data and maintain confidentiality. Even after deployment, data privacy concerns should be continually addressed.
- **Inclusiveness** – AI should empower and serve all individuals, regardless of status, ability, gender identity, or ethnic background.
- **Transparency** – AI models should be explainable, allowing users to understand how predictions are made and ensuring informed decision-making.
- **Accountability** – AI developers and designers must adhere to governance frameworks and ethical standards to ensure their solutions comply with legal and regulatory requirements.

Methodology

The methodology of this study aims to propose an affordable and efficient solution for detecting face presentation attacks by integrating an RGB camera with a thermal sensor array. The primary goal of this research is to develop a reliable biometric attack detection system that can effectively differentiate between genuine face presentations and spoofing attempts. By utilizing thermal sensor technology, this approach offers a cost-effective alternative to more expensive existing methods. To achieve this, deep convolutional neural networks (CNNs) are employed to analyze thermal images and detect potential attacks.

The research begins by collecting a large dataset consisting of 46,000 thermal images captured under various environmental conditions such as lighting, distance, and background. The data is then pre-processed and cleaned to ensure its quality for further analysis. The study uses two well-established deep learning models, AlexNet and ResNet, to analyze the thermal images. These models are selected for their demonstrated effectiveness in image classification tasks. The dataset is used to train the models, and performance is evaluated using metrics like precision, recall, and F1 score.

In addition to developing and evaluating the model, a comparative analysis between AlexNet and ResNet is performed to assess which model better detects biometric presentation attacks in thermal images. The results of this evaluation are interpreted to understand the strengths and weaknesses of the proposed system. The methodology also includes an examination of the limitations encountered during the study and suggests avenues for future improvements.

The project design follows a structured, iterative process, as shown in a detailed flowchart. The process begins with configuring and preparing the hardware for data collection. Once the hardware is set up, the thermal images are collected, followed by pre-processing and cleaning of the data. The images are then subjected to feature extraction to prepare them for model training. Once the thermal images are properly prepared, an appropriate model is selected for training. The models are tested on both the training data and unseen data to evaluate their ability to detect face presentation attacks. Throughout the project, if any issues arise, such as poor image quality during pre-processing or overfitting during model training, the earlier steps are revisited for refinement until the objectives are successfully achieved.

Preparation for Data Collection

For data collection in this project, an Infrared thermal sensor will be connected to Melexis's EVB90640-41 board, which will be further connected to the computer system using a USB cable. Prior to establishing the connection, the necessary software needs to be installed and configured on the system to enable the capture of high-quality thermal images.

Figure 6 Data Collection Set-Up

The Figure 6 above, illustrates the necessary arrangement of hardware components for the data collection process in the system.

Thermal Sensor Array

A far infrared thermal sensor array (32x24 resolution) is designed to detect thermal radiation within the far infrared spectrum. It consists of a grid of thermal sensors arranged in a 32x24 resolution matrix, enabling the capture of detailed thermal images of the environment. This type of sensor is particularly useful in biometric attack detection because it can capture the thermal signatures of faces or other biometric traits and identify potential anomalies that suggest a fraudulent attempt, such as the use of masks or replayed images.

In the context of biometric attack detection, thermal sensor arrays provide significant advantages. First, their non-contact nature allows the system to gather thermal data without requiring physical contact, promoting a hygienic and user-friendly experience. Second, thermal imaging offers the ability to detect spoofing attempts more effectively than traditional visual (RGB) cameras, as it reveals discrepancies in temperature patterns that are often hidden to the naked eye. Finally, these arrays are cost-effective compared to more advanced biometric technologies like 3D facial recognition or iris scanning, making them a viable option for affordable biometric security solutions.

Despite these advantages, there are a few limitations to be mindful of. The primary challenge is the limited identification capabilities of thermal imaging, as it mainly captures temperature patterns rather than fine details of facial features. Additionally, the sensitivity to environmental factors such as ambient temperature, lighting conditions, and occlusions like glasses or scarves can affect the accuracy of thermal readings. Furthermore, since the use of thermal sensors in biometric attack detection is still an emerging field, there is a lack of standardized protocols and benchmarks for performance evaluation.

To mitigate these limitations, this project focuses on enhancing the thermal capture environment and employing deep learning techniques, specifically Convolutional Neural Networks (CNNs), to improve the accuracy of attack detection. Through these advancements, the project aims to contribute to the growing field of biometric attack detection by making it more effective, reliable, and standardized.

Software Configuration for Data Collection

The MLX90640 to MLX90641 thermal sensor array is designed to capture thermal radiation emitted by objects within its field of view, generating thermal images that are critical for biometric attack detection. This project focused on configuring the sensor board with specific parameters to obtain high-quality thermal images. The key configuration settings included a frame rate of 4 Hz, an emissivity of 0.99, a resolution of 2, a chess pattern, an IIR filter depth of 4, a threshold of 2.5, a TGC factor of 4, and an interpolation factor of 2. These settings directly influence the attributes and quality of the thermal images produced.

At a frame rate of 4 Hz, the sensor array captured an average of 240 images per minute. The emissivity setting (0.99) accounts for thermal radiation emitted by non-perfect blackbody objects, such as human skin, enhancing the sensor's ability to accurately capture heat signatures. Each pixel in the image corresponds to a 2x2 grid of sensor elements, influencing the level of detail captured in the thermal images.

The chess pattern configuration helps reduce non-uniformity across the sensor array, improving the consistency of the thermal data. The IIR filter depth (4) and TGC factor (4) settings are used to mitigate noise and compensate for temperature variations across the field of view, ensuring more accurate thermal measurements. The threshold setting (2.5) filters out low-level thermal radiation, enhancing the signal-to-noise ratio and ensuring that only relevant data is captured.

Interpolation (set to 2) is employed to fill in missing data elements in the thermal image, which may arise due to variations in the field of view or other factors. This process helps maintain the integrity of the image by ensuring that missing data points are appropriately estimated.

The thermal images generated represent both the sensor array itself and any objects within its field of view, factoring in noise, temperature variations, and other elements that may impact image quality. MATLAB was used for subsequent image processing and analysis, employing various image classification techniques to identify and detect biometric presentation attacks.

Data Pre-Processing

The thermal sensor array does not directly store images in traditional formats like JPEG or PNG. Instead, it captures thermal data from each individual sensor in the array, where each sensor detects the temperature at a specific location within the scene. This results in a grid of temperature values corresponding to the array's resolution, which are typically represented as a matrix or array. To visualize and analyze the thermal data, specialized software or algorithms are used to convert these temperature values into thermal images.

These thermal images can be represented in different formats, such as color palettes or grayscale, where each distinct color or shade of gray corresponds to a specific temperature range, allowing for more intuitive interpretation and analysis. According to Manjunatha and Srinivas (2020), a combination of pre-processing techniques like median filtering, contrast stretching, and histogram equalization enhances the accuracy and robustness of biometric systems used for face recognition. Building on these insights, this project implemented various pre-processing techniques to improve the quality and reliability of thermal images used for biometric attack detection.

The primary goal of the pre-processing phase is to enhance the accuracy and reliability of biometric feature identification, improving the overall performance of the system and its ability to detect and prevent attacks. The following pre-processing steps were executed:

1. Data Import and Extraction: The data is imported into the MATLAB environment, where the relevant information is extracted by skipping the header rows.
2. Data Structuring: The extracted frame is divided using delimiters and stored as a string array containing temperature values.
3. Matrix Transformation: A transposed matrix is generated from the extracted frame to adjust the dimensions of the array from 32x24 to 24x32.
4. Time Value Extraction: The time value from the first row and column is retrieved.
5. Temperature Conversion: The temperature values are extracted from the relevant rows and columns and are converted from string format to double format for easier manipulation.
6. Image Orientation Adjustment: The matrix is reoriented by rotating it 90 degrees clockwise to match the required dimensions and orientation.
7. Minimum Temperature Identification: The minimum temperature value in the thermal image is determined.
8. Extreme Value Replacement: Any temperature values exceeding 33 degrees Celsius are replaced with the minimum temperature value to eliminate anomalies and extreme readings.
9. Multithresholding: Multithresholding is applied to differentiate between background and foreground elements within the image. A threshold value is calculated, and the image is binarized to create a clearer distinction between relevant features.
10. Image Presentation: The final pre-processed thermal image is displayed as a heatmap using the 'jet' colormap, with the axes labels removed for cleaner visualization.
11. Image Storage: The processed thermal image is then stored as a PNG file for further analysis and evaluation.

Experimental Results and Discussions

In this section, the experimental results obtained from the study on biometric attack detection using a thermal sensor array are presented and analyzed. The aim is to offer a summary of the findings, assess the performance of the biometric attack detection system, and compare the outcomes achieved with the AlexNet and ResNet models.

Presentation and Analysis of Results

A total of 46,000 thermal images were collected under various lighting conditions and distances using the thermal sensor array. These images were labeled according to the type of biometric attack being investigated. The categories included:

- Human_Attacks
- Picture_Attached_with_Hot_Objects
- Picture_Attacks
- Real_Human_Face
- Video_Replay_Attacks

Data were gathered from both **male and female adults** and **children**, ensuring a diverse dataset for human authentication. The images were analyzed using the **AlexNet** and **ResNet** models. Due

to computational limitations, the best 5000 images were selected for analysis. The results are presented and analyzed below.

Confusion Matrices

The confusion matrices for the **ResNet** and **AlexNet** models are as follows:

ResNet Confusion Matrix:

CopyEdit

695 0 0 1 4
0 696 1 0 3
7 10 666 0 17
21 0 0 675 4
7 0 0 0 693

AlexNet Confusion Matrix:

CopyEdit

674 1 17 3 5
4 665 19 0 12
0 0 700 0 0
0 1 1 695 3
6 0 2 0 692

Accuracy Results

The accuracy of the two models is summarized in the table below:

Model	**Accuracy**
AlexNet	0.9798
ResNet-50	0.9691

From the table, it is evident that **AlexNet** achieved a higher accuracy of **0.9798**, while **ResNet-50** achieved **0.9691**. Both models performed well in classifying different attack types, but **AlexNet** slightly outperformed **ResNet-50** in terms of accuracy.

While accuracy is a key metric, other evaluation metrics such as **precision**, **recall**, and **F1 score** must also be considered when determining the better model for biometric attack detection.

Analysis and Interpretation of Label Results

The following table presents the **True Positives (TP)**, **True Negatives (TN)**, **False Negatives (FN)**, and **False Positives (FP)** for each model's confusion matrix:

Labels Investigated	Human_Attacks	Picture_Attached_with_Hot_Objects	Picture_Attacks	Real_Human_Face	Video_Replay_Attacks
Models					
AlexNet	TP = 674	TP = 665	TP = 700	TP = 695	TP = 692
	FP = 6	FP = 2	FP = 39	FP = 3	FP = 20
	FN = 26	FN = 35	FN = 0	FN = 5	FN = 8
	TN = 2790	TN = 2798	TN = 2761	TN = 2797	TN = 2780
ResNet-50	TP = 695	TP = 696	TP = 666	TP = 675	TP = 693
	FP = 35	FP = 10	FP = 1	FP = 1	FP = 28
	FN = 5	FN = 4	FN = 34	FN = 25	FN = 7
	TN = 2765	TN = 2790	TN = 2799	TN = 2799	TN = 2772

Analysis of Performance Metrics:

- True Positives (TP): These represent the correct identification of biometric attacks.
- AlexNet achieved higher TP values for Picture_Attacks and Real_Human_Face, demonstrating effective detection in these categories.
- ResNet-50 excelled in detecting Human_Attacks, Picture_Attached_with_Hot_Objects, and Video_Replay_Attacks with higher TP values, indicating it correctly identified more attack instances in these categories.
- True Negatives (TN): These represent the correct identification of authentic biometric instances.
- ResNet-50 performed better in most categories, showing higher TN values for Human_Attacks, Picture_Attached_with_Hot_Objects, and Video_Replay_Attacks, indicating more accurate identification of legitimate biometric data.
- AlexNet achieved higher TN values for Picture_Attacks and Real_Human_Face, demonstrating superior performance in these categories.
- False Negatives (FN): These are legitimate instances misclassified as attacks.
- ResNet-50 had low FN values for Human_Attacks, Picture_Attached_with_Hot_Objects, and Video_Replay_Attacks, showing a lower misclassification rate.
- AlexNet had extremely low FN for Picture_Attacks and Real_Human_Face, indicating minimal misclassification for these attack types.
- False Positives (FP): These are attacks incorrectly classified as legitimate instances.
- AlexNet demonstrated a lower FP for Human_Attacks, Picture_Attached_with_Hot_Objects, and Video_Replay_Attacks, suggesting fewer false positives in these categories.

- ResNet-50 performed well in minimizing FP for Picture_Attacks and Real_Human_Face, showing a good rate of identifying true attacks as attacks.

Both models demonstrated strong discriminative capabilities in identifying biometric attacks and distinguishing between authentic and attack instances. While **ResNet-50** outperformed **AlexNet** in detecting certain attack types, **AlexNet** excelled in others.

In conclusion, both models showed significant potential for biometric attack detection, with **AlexNet** slightly outperforming **ResNet-50** in terms of accuracy and specific categories. However, further analysis and testing are necessary to identify the best-suited model for practical biometric systems based on the task's requirements.

Analysis and Interpretation of Results

The performance of the **AlexNet** and **ResNet-50** models in biometric attack detection is further examined using **precision**, **recall**, and **F1 score** metrics, as presented in **Table 10** below:

Models	**Accuracy**	**Precision**	**Recall**	**F1 Score**
AlexNet	0.9798	0.9854	0.9629	0.9740
ResNet-50	0.9691	0.9872	0.9914	0.9893

Evaluation of the Models

From Table 10, the following key points can be observed:

- AlexNet has an accuracy of 0.9798, meaning it correctly classifies approximately 97.98% of the dataset's samples.
- The precision of 0.9854 indicates that when AlexNet classifies a sample as an attack, it is correct approximately 98.54% of the time.
- The recall of 0.9629 shows that the model correctly identifies 96.29% of the actual attack samples.
- The F1 score of 0.9740 represents a good balance between precision and recall.
- ResNet-50, on the other hand, has an accuracy of 0.9691, meaning it correctly classifies approximately 96.91% of the dataset's samples.
- The precision of 0.9872 shows that ResNet-50 is accurate 98.72% of the time when predicting an attack.
- The recall of 0.9914 indicates that it correctly identifies 99.14% of the actual attack samples.
- The F1 score of 0.9893 indicates an even better balance between precision and recall.

Critical Analysis of the Model Results

- Accuracy: AlexNet marginally outperforms ResNet-50 with an accuracy of 97.98%, compared to 96.91% for ResNet-50. However, accuracy alone may not fully reflect the effectiveness of a model for biometric attack detection.
- Precision: ResNet-50 exhibits a slightly higher precision of 0.9872, compared to 0.9854 for AlexNet. This suggests that ResNet-50 makes fewer false positive classifications, thereby classifying more attacks accurately without misclassifying legitimate samples.

- Recall: ResNet-50 also performs better in recall, with a value of 0.9914, compared to 0.9629 for AlexNet. This means ResNet-50 is able to identify a higher percentage of the actual attacks, ensuring fewer missed detections.
- F1 Score: The F1 score, which combines both precision and recall, is 0.9893 for ResNet-50, which is slightly higher than AlexNet's F1 score of 0.9740. This indicates that ResNet-50 achieves a better balance between precision and recall.

From the critical analysis of the results, it is clear that ResNet-50 performs better than AlexNet in terms of precision, recall, and F1 score. The higher recall of ResNet-50 ensures a lower rate of false negatives (missed attacks), while its higher precision reduces the rate of false positives (misclassifying legitimate data as an attack). The F1 score further supports this, showing a superior balance between precision and recall for ResNet-50.

However, AlexNet still demonstrates impressive performance, particularly in terms of accuracy. While ResNet-50 may perform better in identifying attacks with fewer errors, AlexNet has a slight edge in overall classification accuracy.

It is also important to note that other factors such as computational resources, training time, and application-specific requirements should be considered when deciding on the most appropriate model. For instance, ResNet-50's superior precision and recall may make it the more suitable choice for applications where minimizing false positives and false negatives is critical.

Subject	**Actual Labels**	**Adult / Child**	**Trained Model**					
-		-	**Predicted Label by ResNet**			**Predicted Label by AlexNet**		
-	-	-	**Predicted Real Face Label (RF)**	**Predicted Non-Real Face Label (Attack) (VR, PA, FM)**	**SCORE**	**Predicted Real Face Label (RF)**	**Predicted Non-Real Face Label (Attack)**	**SCORE**
-	-	-						
A	VR/A	M	-	PA	0	-	VR/A	1
A	RF	M	RF	-	1	RF	-	1
A	PA	M	-	PA	1	-	PA	1
A	FM	M	-	FM	1	-	FM	1
A2	VR/A	M	-	PA	0	-	VR/A	1
A2	RF	M	RF	-	1	RF	-	1
A2	PA	M	-	PA	1	-	PA	1
A2	FM	M	-	FM	1	-	FM	1
B	VR/A	F	-	VR/A	1	-	VR/A	1
B	RF	F	RF	-	1	RF	-	1
B	PA	F	-	PAHO	0	-	PA	1
B	FM	F	-	FM	1	-	PA	0
B2	VR/A	F	-	PA	0	-	VR/A	1

B2	RF	F	RF	-	1	RF	-	1
B2	PA	F	-	PA	1	-	FM	0
B2	FM	F	-	FM	1	-	FM	1
C	VR/A	C	-	VR/A	1	-	VR/A	1
C	RF	C	RF	-	1	RF	-	1
C	PA	C	-	PA	1	-	PA	1
C	FM	C	-	FM	1	-	FM	1
C2	VR/A	C	-	VR/A	1	-	VR/A	1
C2	RF	C	RF	-	1	RF	-	1
C2	PA	C	-	PA	1	-	PA	1
C2	FM	C	-	FM	1	-	FM	1
D	VR/A	C	-	VR/A	1	-	VR/A	1
D	RF	C	RF	-	1	RF	-	1
D	PA	C	-	PA	1	-	PA	1

D	FM	C	-	FM	1	-	FM	1
D2	VR/A	C	-	VR/A	1	-	VR/A	1
D2	RF	C	RF	-	1	RF	-	1
D2	PA	C	-	PA	1	-	PA	1
D2	FM	C	-	FM	1	-	FM	1
E	VR/A	T	-	VR/A	1	-	VR/A	1
E	RF	T	RF	-	1	RF	-	1
E	PA	T	-	PA	1	-	PA	1
E	FM	T	-	FM	1	-	FM	1
E2	VR/A	T	-	VR/A	1	-	VR/A	1
E2	RF	T	RF	-	1	RF	-	1
E2	PA	T	-	PA	1	-	PA	1
E2	FM	T	-	FM	1	-	FM	1

	Actual Label	ResNet-50 Predicted				AlexNet Predicted			
		Correctly Predicted	Wrongly Predicted	Wrongly Predicted As		Predicted Correctly	Wrongly Predicted	Wrongly Predicted As	
Human	Real Face	9 or 90%	1 or 10%			10 or 100%	0 Or 0%		
Non-Human Face	Replay Video	7 or 70%	3 or 30%			10 or 100%	0 or 0%		
	Picture Attack	9 or 90%	1 or 10%			9 or 90%	1 or 10%		
	Facemask	1O or 100%	0 or 0%			9 or 90%	1 or 10%	PA	

Keys	
A, A2, B, B2, C, C2, D, D2, E, E2	Subject presented
VR	Video Replay
PA	Picture Attacks
FM/A	Face Mask Attacks
RF	Real Face
C	Children
T	Toddler
1	Correct Prediction
0	Wrong Predictions

Conclusion

Both AlexNet and ResNet-50 demonstrate strong performance in biometric attack detection using a thermal sensor array. AlexNet performs slightly better in terms of accuracy, while ResNet-50 excels in precision, recall, and F1 score. ResNet-50's higher precision and recall suggest it has a better ability to correctly identify attacks while minimizing false positives and false negatives. Based on these performance metrics, ResNet-50 is likely the more suitable model for biometric attack detection. However, depending on specific system requirements, AlexNet could still be a viable option, especially if a marginal improvement in accuracy is preferred. Further considerations regarding resource usage and training time are also essential when making a final decision on the optimal model for deployment in a real-world biometric system.

REFERENCES

Adama, D. (2022). Principles of Responsible AI.

Alessandro Mascellino. (2021). Adversarial image attacks could spawn new biometric presentation attacks. Biom. Res. Group.

Ali, A., Deravi, F., & Hoque, S. (2013). Directional sensitivity of gaze-collinearity features in liveness detection. In 2013 Fourth International Conference on Emerging Security Technologies (pp. 8–11). IEEE. https://doi.org/10.1109/EST.2013.7

Ben-Yacoub, S., Abdeljaoued, Y., & Mayoraz, E. (1999). Fusion of face and speech data for person identity verification. IEEE Transactions on Neural Networks, 10(5), 1065–1074. https://doi.org/10.1109/72.788647

Biometrics Research Group. (2021). China's facial recognition fraud scandal highlights security risks. South China Morning Post.

Brunelli, R., & Falavigna, D. (1995). Person identification using multiple cues. IEEE Transactions on Pattern Analysis and Machine Intelligence, 17(10), 955–966. https://doi.org/10.1109/34.464560

Chaudhari, U. V., Ramaswamy, G. N., Potamianos, G., & Neti, C. (2003). Information fusion and decision cascading for audio-visual speaker recognition based on time-varying stream reliability prediction. In 2003 International Conference on Multimedia and Expo (pp. III–9). IEEE. https://doi.org/10.1109/ICME.2003.1221235

Chrzan, B.C. Martin. (2014). Liveness detection for face recognition (Master's thesis). Masaryk University, Faculty of Informatics.

Cooper, I., & Yon, J. (2019). Ethical issues in biometrics. *Science Insights*, 30, 63–69. https://doi.org/10.15354/si.19.re095

Dieckmann, U., Plankensteiner, P., Schamburger, R., Fröba, B., & Meller, S. (1997). SESAM: A biometric person identification system using sensor fusion. In J. Bigün, G. Chollet, & G. Borgefors (Eds.), Audio- and Video-Based Biometric Person Authentication (pp. 301–310). Springer Berlin Heidelberg. https://doi.org/10.1007/BFb0016009

George, A., Marcel, S., & Evans, N. (2019). Biometric Presentation Attack Detection: Beyond Handcrafted Features. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 1(3), 170–181.

Hevesi, P., Wille, S., Pirkl, G., Wehn, N., & Lukowicz, P. (2014). Monitoring household activities and user location with a cheap, unobtrusive thermal sensor array. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 141–145). ACM. https://doi.org/10.1145/2632048.2636084

Institute of Electrical and Electronics Engineers (Ed.). (2007). 2007 IEEE 11th International Conference on Computer Vision: ICCV 2007; Rio de Janeiro, Brazil, 14 - 21 October 2007. IEEE Service Center.

Korshunov, P., & Marcel, S. (2018). DeepFakes: Realism and Vulnerability of Face Recognition to Image Manipulations. *IEEE Transactions on Information Forensics and Security*, 13(11), 2842–2855.

Naser, A., Lotfi, A., & Zhong, J. (2021). Adaptive thermal sensor array placement for human segmentation and occupancy estimation. IEEE Sensors Journal, 21(3), 1993–2002. https://doi.org/10.1109/JSEN.2020.3020401

Nguyen, D. T., Park, Y. H., Shin, K. Y., Kwon, S. Y., Lee, H. C., & Park, K. R. (2013). Fake finger-vein image detection based on Fourier and wavelet transforms. *Digital Signal Processing*, 23(6), 1401–1413. https://doi.org/10.1016/j.dsp.2013.04.001

Patel, K., Han, H., Jain, A. K., & Rathgeb, C. (2016). Cross-Spectral Face Recognition: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 38(5), 1041–1055.

Pontes, B., Cunha, M., Pinho, R., & Fuks, H. (2017). Human-sensing: Low-resolution thermal array sensor data classification of location-based postures. In N. Streitz & P. Markopoulos (Eds.), Distributed, Ambient and Pervasive Interactions (pp. 444–457). Springer International Publishing. https://doi.org/10.1007/978-3-319-58697-7_33

Raghavendra, R., Raja, K. B., & Busch, C. (2015a). Presentation attack detection for face recognition using light field camera. *IEEE Transactions on Image Processing*, 24(3), 1060–1075. https://doi.org/10.1109/TIP.2015.2395951

Raghavendra, R., Raja, K. B., Yang, B., & Busch, C. (2015). Presentation Attack Detection for Face Recognition using Multi-Spectral Imaging. *IEEE Transactions on Information Forensics and Security*, 10(3), 556–569.

Raghavendra, R., Surbiryala, J., & Busch, C. (2015b). An efficient finger vein indexing scheme based on unsupervised clustering. In IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015) (pp. 1–8). IEEE. https://doi.org/10.1109/ISBA.2015.7126343

Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys*, 50(8), 8:1–8:37. https://doi.org/10.1145/3038924

Sanderson, C., & Paliwal, K. K. (2004). Identity verification using speech and face information. *Digital Signal Processing*, 14(6), 449–480. https://doi.org/10.1016/j.dsp.2004.05.001

Smith, D. F., Wiliem, A., & Lovell, B. C. (2015). Face recognition on consumer devices: Reflections on replay attacks. IEEE Transactions on Information Forensics and Security, 10(5), 736–745. https://doi.org/10.1109/TIFS.2015.2398819

Sun, Y., Wang, X., & Tang, X. (2017). Beyond Part Models: Person Retrieval with Refined Part Pooling (and A Strong Convolutional Baseline). IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017, 4809–4818.

Unite, A. (2021). Adversarial Attacks on Object Recognition Systems Raise Security Concerns for Biometrics. University of Adelaide Research Blog.

Wark, T., Sridharan, S., & Chandran, V. (1999). Robust speaker verification via fusion of speech and lip modalities. In 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing (Vol. 6, pp. 3061–3064). IEEE. https://doi.org/10.1109/ICASSP.1999.757487

Yi, D., Lei, Z., Zhang, Z., & Li, S. Z. (2014). Face anti-spoofing: Multi-spectral approach. In S. Marcel, M. S. Nixon, & S. Z. Li (Eds.), Handbook of Biometric Anti-Spoofing (pp. 83–102). Springer London. https://doi.org/10.1007/978-1-4471-6524-8_5

Zhang, J., Liu, Y., Zhang, X., & Tao, D. (2020). Face Anti-Spoofing: From 2D and 3D Masks to Deep Learning. *International Journal of Computer Vision*, 128(1), 2223–2246.

Zhang, Z., Yi, D., Lei, Z., & Li, S. Z. (2011). Face liveness detection by learning multispectral reflectance distributions. In Face and Gesture 2011 (pp. 436–441). IEEE.