The Door Face Panels

Image Analysis and Facial Recognition Technology Security

Jean Carla Romin
February 15, 2025

Introduction

An integrated camera system built into doors significantly contributes to the security of clients' homes. These camera features prioritize the safety of homeowners and their loved ones by providing real-time surveillance and comprehensive image analysis. Through AI-enhanced systems, intruders and potential threats can be immediately identified, offering a proactive approach to security. The camera system is integrated with the door's smart lock features, enabling users to remotely view the live camera feed, control access permissions, and receive real-time alerts via their mobile apps. This integration enhances convenience alongside, ensuring that homeowners can respond in due time to any imminent threats, even when they are away from home.

This report focuses on identifying security risks and potential vulnerabilities of IoT devices, specifically concerning the configurations, software, and other components of cameras and surveillance devices. We will examine the weaknesses of image analysis algorithms, such as susceptibility to false positives and negatives, limited performance in low-light conditions, and challenges in classification accuracy. Additionally, we will explore techniques and features that can enhance the reliability of Facial Recognition Technology (FRT). Improvements include the use of thermal imaging for identifying live humans avoiding spoofing, high-resolution cameras for better performance in low-visibility environments, regular firmware and software updates to defend against emerging threats, and multi-factor authentication to increase security and prevent unauthorized access to the system. By addressing these vulnerabilities and leveraging these technologies, we can create more robust and secure camera systems that provide homeowners with peace of mind and a higher level of protection.

Furthermore, the report will focus on the importance of data encryption and following best security practices, such as **OWASP** and **NIST** standards to safeguard the footage and personal information collected by these devices. As IoT devices become increasingly interconnected, the space for threat actors to exploit has also expanded. Thus, ensuring the integrity and confidentiality of personal data is a must to deliver a high-quality product for the clients' homes. We will discuss the importance of regular software updates and patches in protection from emerging threats and maintaining the long-term security of these systems. Ultimately, by combining advanced image analysis technology with best security practices, we can reassure clients that their families’ safety and privacy are prioritized with our smart home devices.

Camera Technologies

The two camera technologies that we will be discussing are Image Analysis and Classification and Facial Recognition Technology (FRT).

Image Analysis and Classification

Image Analysis and Classification is a branch of artificial intelligence (AI) that involves processing and categorizing images based on their features. This technology utilizes machine learning and deep learning models to analyze visual data, recognize patterns, and classify images into predefined categories. By mimicking human visual perception, these systems can detect objects, colors, textures, and other key elements within an image. Neural networks, particularly convolutional neural networks (CNNs) , are commonly used in image classification, as they can extract intricate patterns and features from image data.

Image analysis and classification algorithms are primarily developed by researchers, technology companies, open-source communities, and government agencies. Researchers in universities and research institutions conduct studies to further develop image recognition and classification models. Furthermore, technology companies such as Google, Microsoft, and Meta develop AI-based image processing algorithms for applications like facial recognition, medical imaging, and autonomous vehicles. Additionally, open-source communities contribute to widely used frameworks such as Google's TensorFlow, and Meta's PyTorch, allowing developers worldwide to access and improve image classification tools. Government and defense agencies also play a role in developing image analysis algorithms for security, surveillance, and defense applications.

The development of image classification algorithms follows a process to ensure accuracy, fairness, and ethical considerations. It begins with data collection and preprocessing, where large data sets of labeled images are gathered from sources. These images undergo preprocessing steps such as resizing, normalization, and augmentation to enhance model performance. The next stage involves model development, where neural networks, particularly **Convolutional Neural Networks (CNNs)**, are trained on labeled data.

Here’s the step-by-step process of training a model to utilizing it for classification:

1. **Collecting and Preparing Data:** The computer needs a lot of example images to learn from. If we are training it to recognize cats and dogs, we give it thousands of labeled pictures of each.
2. **Training the Model:** The computer looks at all these images and tries to figure out what makes a cat a cat and a dog a dog. It notices patterns like shapes, colors, and textures.
3. **Testing the Model:** After training, we show the computer new images it hasn’t seen before to see if it can correctly classify them.
4. **Improving the Model:** If the computer makes mistakes, we adjust its settings and give it more training to make it better over time.
5. **Using the Model:** Once the computer is good at recognizing images, we can use it for real-world tasks like scanning medical images for diseases, identifying people in security cameras, or organizing photo albums on a smartphone.

Once models are trained, they undergo evaluation and validation to ensure reliability. This step involves testing the models on unseen data using performance metrics such as false match rate (FMR), false non-match rate (FNMR), precision, and confusion matrices. Cross-validation techniques help assess the model's generalizability to different data sets. Ethical and bias considerations are also crucial in image classification. Developers follow established guidelines to minimize biases in data sets and ensure fairness across different demographics. Regulatory frameworks such as the General Data Protection Regulation (GDPR) and AI ethics principles provide guidance on responsible AI development.

After validation, the models are deployed in various applications, including medical diagnostics, security systems, and autonomous vehicles. Continuous monitoring and retraining are essential to maintaining high performance as new data becomes available. Additionally, industry standards help ensure that AI-based image classification systems are accurate and reliable. Organizations such as the International Organization for Standardization (ISO) define frameworks for AI concepts, including ISO/IEC 22989 and ISO/IEC 23053. By following these processes and standards, developers can create ethical, effective, and high-performing image analysis and classification systems.

Facial Recognition Technology

Facial Recognition Technology or FRT is a form of biometric authentication that operates within a subgroup of Vision AI which identifies humans by analyzing their facial features in photos or videos. Such systems use deep learning, a type of artificial intelligence that processes information and data through multiple layers, in order to simulate processes similar to a human's neural network. In other words, it wants to generate a result by thinking like a “human.” The system is trained with a large pool of data with thousands or millions of examples to help recognize patterns. When identifying a face, the system looks at details like the distance between key facial features, skin texture, or even heat patterns, and compares these to known faces to accurately predict the identity of the individual.

In our daily lives, we use it to open our mobile devices, log-in to online banking apps, or tag friends in photos. In a broader aspect, facial recognition technology is widely used in various of fields and industries including, but not limited to:

- Retail
- Healthcare
- Finance
- Security
- Government Agencies
- Transportation

FRT is primarily used in situations where identifying individuals quickly and accurately is crucial, such as, verifying customer identities, monitoring security, or preventing fraud. As technology advances, facial recognition systems are expected to become more accurate and capable of operating in diverse conditions. Innovations such as 3D facial recognition, emotion detection, and improved AI algorithms will further expand its applications. However, addressing ethical, legal, and privacy concerns will be critical to ensuring its responsible and equitable use in society.

Facial recognition technology uses AI to identify people by comparing their facial features to a database. The process works like this:

1. Captures or receives an image of a person's face.
2. Analyzes the individual's key facial features.

3. A unique digital map of those facial features is created, called a facial signature.
4. Compares the facial signature to images stored in a database.
5. Checks for a match or any resemblance to any of the images in the database.

Facial recognition technology is closely monitored to make sure it is used fairly and does not violate privacy or human rights. Governments, companies, and researchers set rules and guidelines to prevent misuse, such as mass surveillance or discrimination. Because facial recognition can collect sensitive personal data, strict laws and ethical standards are in place to control its use.

Many countries worldwide have laws to regulate the usage and storage of facial recognition technology. In Europe, the **General Data Protection Regulation (GDPR)** requires companies to explicitly ask for consent before collecting biometrics such as facial data. The state of Illinois, USA, passed the **Biometric Information Privacy Act (BIPA)** to protect people by requiring companies to inform users before using facial recognition technology. In 2019, San Francisco became the first U.S. city to ban facial recognition technology in city agencies, such as law enforcement under the **Acquisition of Surveillance Technology Ordinance**. The **Cyberspace Administration of China (CAC)** has rules requiring companies to be clear when they use facial recognition. These guidelines stress that companies should be open about how they use the technology, make sure their systems do not discriminate, and take responsibility if their technology harms people.

Regulatory Compliance

The deployment and usage of facial recognition technologies is subject to various privacy regulations aimed at protecting personal data and privacy.

California Consumer Privacy Act (CCPA)

In 2018, the California Consumer Privacy Act or CCPA was a law established to protect the personal data of California residents from organizations and businesses. This law states that businesses must follow data collection, processing, and storage standards such that consumers have the following rights,

- **The right to know:** Consumers have the right to know what personal data is being collected, how the data is used and who it is being shared with.

- **The right to delete:** Consumers can request to have their personal data deleted without any consequences. Businesses cannot deny this request unless there are legal reasons to do so.
- **The right to opt-out:** Consumers can request or opt-out of the sale or sharing of personal data.
- **The right to non-discrimination:** Businesses cannot deny consumers services or treat them differently if consumers have chosen to practice their CCPA rights.

California Privacy Rights Act (CPRA)

The California Privacy Rights Act or CPRA was an extension to the existing CCPA rights. The following rights were added in 2023,

- **The right to correct:** Consumers have the right to correct any wrong information that businesses have recorded about them.
- **The right to limit:** Consumers have the right to choose what is done to data that is categorized as *sensitive data*, which includes biometric data.

Canadian Regulations

Personal Information Protection Act (PIPA)

The **Personal Information Protection Act,** or **PIPA,** is privacy legislation enacted in **Alberta, British Columbia,** and **Quebec**, regulating how private-sector organizations collect, use, and disclose personal information. PIPA aims to protect individuals' privacy rights while requiring organizations to use personal data for legitimate purposes. Under PIPA, facial data is considered as *personal information*, therefore subject to the PIPA's general rules for collection, use, disclosure, and protection. These rules include,

- An organization must obtain **consent** to collect, indirectly collect, use, and disclose personal information.
- Organizations can only collect and use biometric data for specific, **disclosed purposes**.
- Organizations must implement strong **security measures** to protect facial recognition data from unauthorized access, breaches, or leaks.
- Organizations should **retain** biometric data only until necessary, then **delete** once no longer required.

- PIPA also states that individuals have the **right to request** to view what data has been collected and for their data to be deleted.

Personal Information Protection and Electronic Documents Act (PIPEDA)

The **Personal Information Protection and Electronic Documents Act (PIPEDA)** has classified facial recognition data as *sensitive personal information* that requires an additional layer of security and protection. PIPEDA is a federal law that is applied to private-sector organizations in all Canadian provinces and territories. However, some provinces have their own privacy legislation which may take precedence over PIPEDA. PIPEDA provides a thorough guide for organizations and how they should manage biometric data in their commercial processes. That is, PIPEDA governs how private-sector organizations in Canada collect, process, and disclose personal information. Relevant PIPEDA security and privacy principles that would be applicable to facial recognition technology included,

- Organizations must obtain **explicit consent** before collecting or using facial data.
- Private-sector organizations must **inform users** about how facial recognition data is processed and stored.
- Organizations are required to provide the **purpose** of collecting facial data. **Transparency** is a significant principle to PIPEDA, and disclosing important information that would affect people is crucial.
- **Limited use of data**, the biometric data acquired cannot be processed and used to extract additional information. For example, biometrics can reveal secondary information relating to people's health, ethnicity, or biological relationships.
- **Destroy raw biometric data**, after the information needed was extracted from raw biometric data to create a template, the raw data used should be properly deleted.
- Organizations are required to **ensure the accuracy and quality** of the technology used for biometric authentication.
- In the event of a data breach, the organization must have a **robust breach plan** to protect the privacy and security of their users' data.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation or the GDPR classifies biometric data as special categories of personal data and prohibits its processing unless organizations closely follow the GDPR's regulations and standards regarding its collection and storage. Biometric data is defined as "*personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprint data.*"

Additionally, GDPR standards apply to Canadian organizations as well. That is, Canadian organizations must comply with the GDPR if they:

- have an established presence in the EU.
- offer goods and services to individuals in the EU.
- monitor the behaviour of individuals in the EU.

Art. 5 GDPR: *Principles relating to processing of personal data*

Key principles for processing facial recognition data, ensuring it is used **lawfully, fairly,** and **transparently**. Organizations must collect **only necessary data**, use it for a **specific purpose**, and **delete it** when no longer needed. Facial recognition systems must be accurate to prevent misidentifications and must be securely protected against breaches. Companies are responsible for proving compliance and can face fines if they fail to follow these rules. These regulations help protect individuals' privacy and rights while ensuring ethical use of facial recognition technology.

Art. 9 GDPR: *Processing of special categories of personal data*

Due to being categorized as special categories of personal data, processing of biometric data such as facial recognition, iris recognition, and fingerprint data is prohibited. For facial recognition to be lawful, organizations must have a valid reason for processing biometric data, the processing of biometric data is prohibited unless,

- **Explicit consent** from the individual was given.
- It was done in the **public interest**, governments can use it for national security or law enforcement, but only under strict conditions.
- **Vital interest,** it can be used if extremely necessary. For example to save someone's life, such as identifying unconscious patients in a hospital.

Art. 13 GDPR: *Information to be provided where personal data are collected from the data subject*

Organizations and entities that use facial recognition must inform people how and why their facial data is being collected. This refers to the GDPR's Right to be Informed article, emphasizing the need for transparency with the handling and processing of personal data. Information that organizations must inform individuals about include,

- Who is collecting the data.
- The purpose of data collection and where it will be used.
- The retention period of the data.
- Recipients of the data and whether that data will be shared with third parties.

Art. 25 GDPR: *Data protection by design and by default*

Organizations must design their facial recognition systems to prioritize the protection of personal data and privacy. Companies can take actions such as,

- **Minimizing data collection**, that is, only collecting data that is necessary.
- **Transferring and storing data with encryption** to secure any personally identifiable data.
- Ensuring that the data collected and stored is **properly deleted** after the set timeline. GDPR's Right to be Forgotten states that individuals have the right to request a copy of any facial recognition data collected about them, and ask for their data to be deleted if there is no legal reason to keep it.

Art. 32 GDPR: *Security of processing*

Organizations are required to implement appropriate technical and organizational measures to protect data against risks such as unauthorized access, loss, or damage. For facial recognition technology, Article 32 has significant implications because it involves the collection and processing of highly sensitive biometric data. Regarding facial recognition technology, organizations should consider but not limited to,

1. **Data security measures are maintained when dealing with biometric data.** Those measures include, ensure that facial recognition data is encrypted during storage and transmission and implement access controls to limit data access to authorized personnel only. This protects data from unauthorized access and breaches.
2. **The risk assessment and management of technology and systems.** Before deploying any facial recognition systems, companies must conduct a *Data*

Protection Impact Assessment (DPIA) to identify and mitigate risks, ensuring that privacy concerns and security vulnerabilities are addressed.

3. **Part of the CIA triad, confidentiality and integrity of the data must be delivered.** Facial recognition systems must ensure that data is both accurate and secure, preventing tampering and ensuring the system operates without errors that could compromise security.
4. **Regular security testing and evaluation of FRT and image analysis systems** is detrimental to the security of data. Penetration testing and vulnerability assessments are required to evaluate the security of facial recognition systems and ensure they are resilient against potential threats.

Illinois Biometric Information Privacy Act (BIPA)

Illinois passed the **Biometric Information Privacy Act or BIPA** in 2008 to ensure the protection of individuals' biometric data. This act prohibits organizations to collect an individual's biometric data unless specific requirements are met. BIPA aims to establish standards for the collection of biometric data with the consumer's best interest in mind. Additionally, BIPA directly addresses the issue of companies selling and profiting off of consumer data, by presenting a set of regulations that tackles these issues. Some key points that a company must follow under BIPA include,

- **Explicit consent** from the individual was given. Information the company must share includes the purpose of the collection, and the duration for which the data will be stored.
- The company must publicly disclose the **data retention period** and the **data destruction date**.
- Under BIPA, organizations **cannot sell, trade, or profit** from an individual’s biometric data in any way.
- The company must use reasonable **security measures** to protect biometric data, including encryption and restricted access protocols.

Case: Patel v. Facebook Lawsuit

Electronic Privacy Information Center or EPIC filed a case against Facebook for violating the Biometric Information Privacy Act (BIPA). Facebook was under fire for collecting and storing users' facial data without their explicit consent. This was identified to be from the tag suggestion feature of the social media platform. The feature used facial recognition to identify individuals in images and suggest tags without users knowledge of the technology being used. Facebook did not follow the standards established by BIPA such as, **collecting data without prior consent, not**

disclosing the data retention period and deletion date. Therefore, the court ruled that Facebook's actions caused harm to users by violating their privacy rights, leading to a $650 million settlement from Facebook. This case emphasizes the importance of following compliance standards with laws like BIPA, GDPR, and Canada's PIPEDA.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

ISO/IEC 27001:2022: *Information security management systems*

The best-known standard for information security management systems (ISMS) worldwide. This standard provides organizations guidance for establishing, implementing, maintaining and improving an ISMS. Furthermore, by following the standard, organizations have set measures to manage risks related to the security of data. Regarding facial recognition technology and biometric data processing, ISO/IEC 27001:2022 includes standards such as,

- **Risk Assessment and Management:** Organizations must identify and assess risks related to biometric data storage, processing, and transmission. Addresses measures for access control, cryptography, physical security and incident management.
- **End-to-end encryption:** Implement encryption techniques to protect biometric templates of individuals.
- **Update security measures:** Regularly review and update security measures to counter emerging threats. Preparation for a cyber attack is as important as the response itself.

ISO/IEC 24745:2022: *Biometric information protection*

ISO/IEC 24745:2022 is an international security standard that defines best practices for the protection of **biometric information**, including facial recognition data. It provides guidelines on secure storage, processing, and transmission of biometric templates, ensuring that personal biometric data remains confidential, maintains integrity, and protects against unauthorized access.

- The standard emphasizes **end-to-end encryption** and **secure transmission protocols** to prevent attackers from intercepting facial recognition data.
- Promotes **template protection techniques**, that is, only storing encrypted facial recognition templates and not raw biometric images.

- **Regulated access controls** to prevent unauthorized access to biometric data. Limit biometric data access to authorized personnel and devices only.
- The standard enforces **privacy-preserving storage methods,** using on-device facial recognition instead of transmitting biometric data to cloud servers, reducing exposure to breaches.
- Home security devices handling facial recognition must **comply with regional privacy regulations.** ISO/IEC 24745:2022 aligns with laws like BIPA (Illinois), GDPR (Europe), and PIPEDA (Canada) by ensuring biometric data is collected with consent, securely stored, and deleted when no longer needed.

ISO/IEC 30136:2018: *Performance testing of biometric template protection schemes*

ISO/IEC 30136:2018 defines **evaluation methods** for biometric accuracy, reliability, and security. Recommends secure biometric data practices that would reduce the likelihood of threat actors accessing biometric data. Provides guidelines for **evaluating false acceptance rates (FAR)** and **false rejection rates (FRR)** in FRT to improve the accuracy of facial recognition systems in real-world environments. In the case of DFP, the standard ensures that smart home security devices correctly identify authorized individuals while preventing unauthorized access with accuracy.

ISO/IEC 19794-5:2011: *Biometric data interchange formats*

ISO/IEC 19794-5:2011 is a standard that defines the **image format, quality requirements, and data structure** for facial recognition systems. It ensures that facial images are captured, stored, and transmitted in a standardized way, enabling smooth communication between different facial recognition devices and software. Taken directly from the website, this standard addresses the following,

- Specifies a **record format for storing, recording, and transmitting** information from one or more facial images or a short video stream of facial images.
- Specifies **scene constraints** of the facial images.
- Specifies **photographic properties** of the facial images.
- Specifies **digital image attributes** of the facial images, and provides best practices for the photography of faces.

Security Vulnerabilities

FRT Accuracy

Facial recognition systems can be very accurate under ideal conditions, especially when matching clear reference images, such as passport photos or mugshots. However, in real-world situations, the accuracy drops significantly. Factors like movement, poor lighting, shadows, or people not facing the camera can cause error rates to rise. Aging also affects accuracy, as changes in a person's face over time can make it harder to match photos taken years apart. The accuracy of facial recognition also varies greatly depending on the environment. In controlled settings like airport gates, top algorithms can achieve higher accuracy, but in more challenging settings like sports venues, accuracy significantly drops. There's also a large gap between different vendors and their models, with some algorithms being much more accurate than others. This means that, while some facial recognition systems perform well, most struggle to achieve consistent results, showing that the technology is not yet reliable across the board.

The accuracy of a facial recognition system or image classification model is crucial to the security of the device and network. An authentication system that uses facial recognition technology and image analysis to identify and give clearance to individuals is more likely to fail and misidentify said individuals, potentially putting the security of assets and/or personal safety at risk. When the accuracy of a facial recognition system or an image classification system is low, then it can produce false positives and false negatives. A false positive occurs when an unknown individual is misidentified as someone known, while a false negative occurs when a known individual is misidentified as someone unknown.

Case: False Positives Results in Wrongful Jailing

A lawsuit was filed against a department store chain, Macy's, as well as Sunglass Hut by a 61-year-old man, Harvey Eugene Murphy Jr. was wrongfully accused and arrested after a facial recognition system identified him as the culprit for a past armed robbery incident (Bhuiyan 2024). Sunglass Hut and Macy's allegedly used facial recognition technology to identify Murphy as a suspect in a 2022 armed robbery in Houston, Texas. Murphy denied those claims as he was residing in California at the time. The misidentification led to a wrongful arrest and several psychological and physical impacts on Murphy. Upon further investigation, the technology falsely identified Murphy based on low-quality camera footage, leading to a wrongful arrest. The errors highly likely occurred due to poor-quality images. Additionally, facial recognition was used without his consent, raising privacy concerns. Murphy's case emphasizes the importance of the accuracy of facial recognition technology, as wrongful identifications can lead to severe consequences for the individuals involved.

Improvements and Recommendations

To improve the accuracy of the system, here are some recommendations to consider:

- **High-Resolution cameras:** Image quality significantly impacts the performance of a facial recognition or image classification system.
- **Optimized Camera Placement:** Position cameras at strategic locations to get the best possible angle and line of sight for facial recognition, such as near entrances where faces are most likely to be well-lit and centered in the frame.
- **Variety of Images:** When training image classification models, the model's accuracy can improve if it was trained with a larger amount of images and a wider variety of images. For example, including both high-quality and low-quality images, different angles of a person's face, augmented images of the individual (horizontal/vertical flipping, cropping, scaling of pictures), and images of individuals expressing different emotions.
- **Real-time Recognition:** For a security camera system, it’s important that the recognition process is fast and accurate. Optimizing the system to quickly compare live footage to the stored image data of the known individuals ensures that the user does not experience long delays when trying to access the home.

Implementing these measures to the Door Face Panels will surely bring it closer to its goal of safety and security using advanced technology.

Firmware Security

Firmware is embedded software that enables hardware devices to function, it acts as the bridge between physical components and the operating system. Firmware security ensures that this essential software remains protected from vulnerabilities, unauthorized modifications, and cyber threats. Regarding FRT, firmware acts as the foundational software embedded within security devices, such as smart cameras and access control systems. As the software controls how they operate and process facial recognition data. Ensuring the security of firmware is crucial, as vulnerabilities can expose these systems to cyber threats, leading to unauthorized access and data breaches. Despite advancements in FRT, insecure firmware can undermine the reliability and integrity of the technology, making devices susceptible to tampering, and unauthorized surveillance.

Case: Faulty Doorbell Camera

Consumer Reports, an independent organisation that conducts consumer-focused product testing, released a report that reveals the security flaws of a doorbell camera model with various brand names and was widely sold on major retailers. These security flaws allowed unauthorized access to the live video feed of the doorbell camera, posing a risk to the homeowners' privacy and security. The doorbell cameras shared the same mobile application, **Aiwit**, and the same manufacturer, **Ekan** (Hollister 2024).

The main issue with these devices is that they lacked encrypted video connections, leaving the video feeds exposed to potential interception by hackers. With this camera, threat actors can easily discover a user's public-facing IP address and Wi-Fi networks (Higginbotham & Wroclawski 2024). Additionally, weak firmware security enabled attackers to exploit system weaknesses, allowing them to access and view camera footage, capture screenshots, and reset account ownership without the homeowner's knowledge. Without the necessary encryption and lack of strong firmware security measures, unauthorized individuals could easily access and view the camera footage, capture screenshots, and reset account ownership, without the homeowner's knowledge.

Improvements and Recommendations

To enhance firmware security and ensure the reliability of facial recognition technology, the following best practices should be implemented:

- **Regular Firmware Updates:** Organizations should provide timely security patches to address known vulnerabilities, and users should enable automatic updates to stay protected. This is a preventive measure that is a proactive approach to securing systems. Outdated software is more susceptible to malicious actors probing and exploitation of system vulnerabilities.
- **Data Encryption:** Encrypt data both at rest and in transit to prevent unauthorized access. Generating encryption keys for firmware protects the data for potential interception and unauthorized access.
- **Secure Boot Process:** Ensure that devices only run firmware from trusted sources by implementing cryptographic signature verification before booting. Only allow execution if the signature is from a verified valid source, reducing the risk of unauthorized access.

- **Tamper Detection:** Implement tamper-resistant hardware and software mechanisms to detect and respond to unauthorized modifications. This includes tools and algorithms that monitor suspicious actions from unknown sources.
- **Regular Penetration Testing:** Conduct regular security assessments to identify and mitigate potential firmware vulnerabilities before they can be exploited. Identifying the vulnerabilities before they have been exploited is a preventive measure for data breaches and unauthorized access attempts.

API Security

Application Programming Interfaces (APIs) are essential components of modern technology, enabling communication between software applications. In FRT, APIs facilitate data exchanges between devices, cloud services, and databases, allowing for real-time authentication and processing of biometric data. However, insecure APIs can introduce critical vulnerabilities, exposing sensitive personal data to unauthorized access from threat actors.

Improvements and Recommendations

To enhance API security in facial recognition systems, the following best practices should be implemented:

- **Regular Security Audits:** Conduct penetration testing and risk assessments to identify and address API vulnerabilities before they can be exploited. A proactive way to prevent cyber attacks is by identifying any flaws and addressing these issues before threat actors get to them.
- **Role-Based Access Control:** Role-based access control (RBAC) to restrict access to sensitive API endpoints. Only give individuals the necessary access they require to get the job done, implementing the least privilege principle.
- **Data Encryption:** Use Transport Layer Security or TLS 1.3 encryption to secure API communications and prevent interception from malicious actors. TLS can be used to verify the identity of the server, preventing man-in-the-middle (MITM) attacks that try to impersonate a trusted server.
- **Limit Requests:** Limit the number of API requests per user within a specific time period to prevent abuse and brute-force attacks. Reduces the risk of overloading the system with a denial-of-service attack (DoS) that would impact system operations.
- **Input Validation and Sanitization:** Protect against injection attacks by validating and sanitizing API inputs. Review entry points in the system, ensure that accepted inputs are strictly defined, and remove any suspicious and

unnecessary characters (sanitize). Input can only be accepted once completely sanitized and validated.

- **Monitor Security Logs:** Continuously monitor API activity for suspicious behavior and implement real-time alerts for potential security breaches. SIEM tools should be used to detect and identify any potential threats to catch them early on.

Network Protocol Security

Network protocols are fundamental to communication between devices and systems, ensuring the seamless transmission of data. In IoT devices that use facial recognition technology, secure network protocols are essential for protecting sensitive biometric data during transmission between cameras, servers, and authentication systems. Weak or compromised network protocols can expose these communications to interception, and malicious activities performed by threat actors, putting privacy and security at risk.

Improvements and Recommendations

To enhance network protocol security in facial recognition systems, the following best practices should be implemented:

- **Use Secure Transport Layer Protocols:** Implement TLS 1.3 to encrypt data in transit and reduce the likelihood of interception. TLS 1.3 is the latest version and recommended security protocol for online communication.
- **Implement Network Segmentation:** Isolate facial recognition systems from general network traffic to limit exposure to potential attacks. That is, creating a dedicated network segment for the FRT system. Isolate the system by configuring firewalls to have strict access control lists (ACLs) and implement the least privilege principle to restrict unauthorized access attempts.
- **Enable Secure DNS and Firewall Protections:** Utilize DNS security and firewall rules to detect and block malicious activities. Blocking known and potentially malicious domains reduces the risk of DNS-based attacks that could cause network operation interruptions.
- **Regularly Update Protocols:** Ensure that network protocols and firmware are regularly updated to patch known vulnerabilities. Updates are necessary to protect data from new and emerging cyber threats. Turning on automatic updates would be ideal, to avoid missing any important updates and patches.
- **Monitor Network Traffic for Anomalies:** Deploy intrusion detection systems (IDS) and continuous monitoring to detect suspicious activity in real-time.

Monitoring network and server logs can help in potentially finding malicious activities and actors within the network.

Data storage and encryption

Biometric data has a significant amount of regulations and expectations in terms of its storage, usage, and retention. Given the sensitive data collected, threat actors and hackers are more likely to aim for databases storing biometric data to perform fraudulent activities. If such databases are compromised, it could lead to identity theft or unauthorized access to private accounts like online banking accounts. Data breaches involving facial recognition systems are a growing concern, as biometric data is permanent and cannot be reset like a password. Once facial data is exposed, it is compromised forever, posing a long-term risk to affected individuals. Unlike traditional passwords, once biometric data is leaked, it cannot be changed, making its protection crucial. Therefore, it is essential for organizations to implement robust encryption methods both during data transmission and storage to protect against unauthorized access. Strong encryption standards, such as **Advanced Encryption Standard (AES)** and **Transport Layer Security (TLS)**, should be used to ensure that data is encrypted even if a threat actor manages to gain access to the data. Applying encryption in multiple layers creates a secure and robust data protection plan.

Layer	Function	Encryption
Application	Secures biometric **data at rest** and in use.	**AES-256**
Transport	Secures biometric **data in transit** between devices and servers.	**TLS 1.3**

1. **AES-256:** This encryption standard is widely used for securing sensitive data, which would be ideal for encrypting biometric data. AES-256 is a symmetric encryption algorithm, it offers faster encryption and decryption of data as it only uses one key. Additionally, it is highly effective in securing data as it offers a strong 256-bit key size making it difficult to crack through brute-force attacks.

2. **TLS 1.3:** TLS 1.3 is the latest version and recommended security protocol for online communication between the IoT device, network, and servers. Highly

reducing the risk of interception from unknown entities, ensuring data integrity. TLS 1.3 is also significantly faster than the previous versions, offering lower latency and increased speed. The previous version, TLS 1.2 also had outdated cryptography features which resulted in vulnerabilities, all of these features have been removed in the implementation of TLS 1.3, offering a more secure and robust method for transmission of data.

Adversarial Attacks

Man-in-the-Middle (MITM) Attacks

A Man-in-the-Middle attack is a cyber threat where an attacker intercepts and manipulates communications between two parties without their knowledge. IoT devices are vulnerable to these attacks, given that attackers can worm their way into a network if it's not properly secured. For smart home devices, specifically FRT, MITM attacks can be used to eavesdrop on authentication data, intercept and alter access requests, or inject malicious commands to gain unauthorized entry. These attacks typically exploit weaknesses in unencrypted transmissions, insecure APIs, or outdated network protocols, allowing hackers to capture and replay biometric data, disable security measures, or remotely unlock doors. Because many smart home devices rely on network-based authentication, a compromised communication channel can put the entire security system at risk. Without end-to-end encryption, or proper authentication safeguards, MITM attacks can expose sensitive biometric data and compromise the safety of homeowners.

Response to Attack

1. **Containment:** Immediately remote authentication mechanisms. Force all active users to logout (via DFP app) and require re-authentication to prevent persisting access from the threat actors. Send real-time security alerts to homeowners via a trusted communication channel. Configure firewalls to block suspicious IP addresses and ensure no unnecessary network ports are open, to contain the situation and prevent any more interception.
2. **Analysis:** Inspect network traffic before and during the attack timeframe to analyze and identify unauthorized data or packet injection attempts using network monitoring tools (Wireshark, Zeek, etc.). Alongside network logs, examine device logs and look for suspicious login attempts, failed authentications, and unknown device connections.
3. **Recovery:** Restore the system to a backup version before the attack to eliminate any potential backdoors or modifications introduced by the attacker.

Require affected users to reset their biometric data and use a more secure multi-factor authentication (MFA) system that includes secondary verification methods.

4. **System Updates:** Once the attack has been mitigated and defended against, update any system vulnerabilities that were identified during the analysis of the attack. Additionally, take actions towards prevention techniques such as,

Improvements and Recommendations

- **Implement End-to-end encryption:** End-to-end encryption or E2EE is a way to prevent malicious actors from accessing personal data. E2EE encrypts data in use, at rest, and in transit, making it difficult for unauthorized entities to intercept and modify sensitive information. The personal data remains encrypted until it reaches its specified destination.
- **Intrusion Detection and Prevention Systems:** Intrusion detection and prevention systems or IDPS monitors networks for signs of potential breaches and suspicious activities, notifying security teams and initiating automated mitigation techniques.

Deepfake Spoofing

A deepfake is the combination of "deep learning" and "fake". That is, deepfake spoofing is a type of adversarial attack where threat actors use AI to digitally alter videos or images to impersonate a person's physical appearance and likeness. These deepfakes are so well-made that they can be used to bypass FRT authentication, which typically rely on comparing a person’s live facial features to pre-recorded data. Deepfakes can replicate facial movements, expressions, and even unique identifying features, which makes it possible for attackers to impersonate an individual without the need to physically be present. Since many systems use single-factor authentication, such as facial recognition, they are highly vulnerable to spoofing techniques. Attackers can use a deepfake video of the homeowner’s face to bypass the system, potentially gaining unauthorized access to the home. The reliance on visual cues, such as the face, without further verification steps, increases the risk of exploitation.

Case: Deepfake Bypasses Biometric Authentication

A financial institution in Indonesia reported a deepfake fraud incident, where a generated deepfake managed to bypass the biometric authentication of their mobile banking app. In this case, the fraud protection team of Group-IB led the investigation and discovered more than 1,100 deepfake fraud attempts that ultimately led to estimated losses of up to $138.5 million (Huang 2024). The fraudsters extracted customer information from social media, malware, and the dark web and manipulated photos and face-swapping technologies. This method allowed the threat actors to mimic real-time facial expressions bypassing the liveness detection security mechanism. Furthermore, the threat actors exploited vulnerabilities in the fraud detection systems through app cloning, allowing them to access more customer accounts.

Response to Attack

With the rise of AI use, deepfake spoofing might become a common attack on facial recognition systems. Being prepared to respond to such attacks is crucial, since systems are constantly at risk. Once a deepfake spoofing attack has been identified by the facial recognition system here are steps to respond to the attack:

1. **Containment:** Lock smart home system features and require manual override. Disable any home security feature that has remote access to block any unauthorized actions. That is, using a physical key to access the home instead of facial or biometric authentication. Furthermore, alert homeowners and notify security teams about the threat.
2. **Analysis:** Once necessary steps to contain the attack and prevent data loss is performed, study the deepfake video, network and firewall logs. Reviewing security logs to find unauthorized access attempts and unknown device connections, can help track where the attack came from.
3. **Recovery:** Restore the system to a backup version before the attack to eliminate any potential backdoors or modifications introduced by the attacker. Require affected users to reset their biometric data and use a more secure multi-factor authentication (MFA) system that includes secondary verification methods. Lastly, ensure that any stored biometric templates are encrypted using AES-256 and that access to them is strictly limited.
4. **System Update:** Identify any changes or system updates needed to patch the vulnerabilities exploited by the threat actors to prevent the same attack in the future.

Improvements and Recommendations

This incident highlights the risks in relying on **single-method biometric security**. To prevent potential exploitation, financial institutions and businesses are urged to adopt multi-layered security and advanced anti-fraud systems. Actions organizations can consider are:

- **Implement Multi-Factor Authentication**: Similar to how it's used in online applications, MFA can also be applied to home security. Alongside FRT, homeowners can add an extra layer of security by using a combination of a puzzle, pin code on the lock, or another biometric parameter like fingerprint or iris identification.
- **Infrared cameras or Thermal cameras:** Another mitigation technique for deepfakes is placing infrared cameras or heat detection cameras. Only the live-feed of humans that project heat is identified as a valid figure.
- **Liveness detection:** A technique that uses an algorithm to determine if a subject is a live human by analyzing facial movements such as, blinking, smiling, and head movement. Other features an algorithm can detect are eye reflections, most AI generated images and videos would fail to replicate this.
- **Educate Users on Biometric Security:** Inform users to limit public exposure of their facial images online to reduce the risk of biometric data being scraped for deepfake attacks.
- **Regular Testing FRT Model:** Regularly test the facial recognition model against new deepfake techniques and update detection mechanisms accordingly.

Recommendations

This section is a collection of recommendations to mitigate image analysis and facial recognition technology security vulnerabilities.

Scope	Recommendations
Authentication Mechanisms	● **Multi-Layered Security:** Combine FRT authentication with a second form authentication such as: ○ Pin or Password ○ Fingerprint ○ Authenticator App
Data Training Techniques	● **Variety of Images:** When training image classification models, the model's accuracy can improve if it was trained with a larger amount of images and a wider variety of images. For example, including both high-quality and low-quality images, different angles of a person's face, augmented images of the individual (horizontal/vertical flipping, cropping, scaling of pictures), and images of individuals expressing different emotions. ● **Liveness detection:** A technique that uses an algorithm to determine if a subject is a live human by analyzing facial movements such as, blinking, smiling, and head movement. Other features an algorithm can detect are eye reflections, most AI generated images and videos would fail to replicate this. ● **Regular Testing FRT Model:** Regularly test the facial recognition model against new deepfake techniques and update detection mechanisms accordingly.
	● **High-Resolution cameras:** Image quality significantly impacts the performance of a facial recognition or image classification system. ● **Optimized Camera Placement:** Position cameras at strategic locations to get the best possible angle

Camera Hardware	and line of sight for facial recognition, such as near entrances where faces are most likely to be well-lit and centered in the frame. ● **Infrared cameras or Thermal cameras:** Another mitigation technique for deepfakes is placing infrared cameras or heat detection cameras. Only the live-feed of humans that project heat is identified as a valid figure.
Data Encryption	● **Implement End-to-end encryption:** End-to-end encryption or E2EE is a way to prevent malicious actors from accessing personal data. E2EE encrypts data in use, at rest, and in transit, making it difficult for unauthorized entities to intercept and modify sensitive information. The personal data remains encrypted until it reaches its specified destination. ● **AES-256** for data at rest and in use. ● **TLS 1.3** for data in transit.

System Security Protocols	● **Regularly Update Protocols:** Ensure that security protocols are regularly updated to patch identified vulnerabilities. Updates are necessary to protect data from new and emerging cyber threats. Turning on automatic updates would be ideal, to avoid missing any important updates and patches. ● **Risk Assessment and Penetration Testing:** Organizations must identify and assess risks related to biometric data storage, processing, and transmission. Penetration testing and vulnerability assessments are required to evaluate the security of facial recognition systems and ensure they are resilient against potential threats. ● **Intrusion Detection and Prevention Systems:** Intrusion detection and prevention systems or IDPS monitors networks for signs of potential breaches and suspicious activities, notifying security teams and initiating automated mitigation techniques. ● **Implement Network Segmentation:** Isolate facial recognition systems from general network traffic to limit exposure to potential attacks. That is, creating a dedicated network segment for the FRT system. Isolate the system by configuring firewalls to have strict access control lists (ACLs) and implement the least privilege principle to restrict unauthorized access attempts. ● **Input Validation and Sanitization:** Protect against injection attacks by validating and sanitizing API inputs. Review entry points in the system, ensure that accepted inputs are strictly defined, and remove any suspicious and unnecessary characters (sanitize). Input can only be accepted once completely sanitized and validated.
Preventive Measures	● **Educate Users on Biometric Security:** Inform users to limit public exposure of their facial images online to reduce the risk of biometric data being scraped for deepfake attacks.

More Experimental Features

The DFP records a live feed of its surroundings, capturing images of both known and unknown individuals detected by the system. These captured images are stored and made accessible via the security system's mobile app, allowing the homeowner to review and identify whether the subject is a known individual or not. This process also allows for further training of the system's image classification model, improving its accuracy over time. Unfortunately, this raises concerns about consent since images of individuals possibly just passing the street, or parcel delivery personnel would be captured without their knowledge and consent. This unintentional collection of data could lead to privacy issues, particularly if individuals' images are stored and used without proper consent protocols in place.

References and Sources

A guide to data security. (2025, January 16). Retrieved February 16, 2025, from Ico.org.uk website: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/#5

Bhuiyan, J. (2024, January 23). Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit

Biometric recognition and authentication systems. (2019). Retrieved from Ncsc.gov.uk website: https://www.ncsc.gov.uk/collection/biometrics

Cloudflare. (2018). Why use TLS 1.3? | SSL and TLS vulnerabilities. Retrieved from Cloudflare.com website: https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/

Edwards, M. (2017, July 11). ISMS Online. Retrieved from ISMS.online website: https://www.isms.online/iso-27001/

Foran, P. (2024, March 16). Do you have a video doorbell? Some models can be hacked. Retrieved February 10, 2025, from CTVNews website: https://www.ctvnews.ca/toronto/article/do-you-have-a-video-doorbell-some-models-can-be-hacked/

Higginbotham, S., & Wroclawski, D. (2024, February 29). These Video Doorbells Have Terrible Security. Amazon Sells Them Anyway. Retrieved February 10, 2025, from Consumer Reports website: https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/

Hollister, S. (2024, February 29). This "Amazon's Choice" video doorbell could let just about anyone spy on you. Retrieved February 10, 2025, from The Verge website: https://www.theverge.com/2024/2/29/24086218/eken-aiwit-tuck-video-doorbell-amazon-temu

How do we keep biometric data secure? (2024, February 22). Retrieved February 10, 2025, from Information Commissioner's Office website: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/

Huang, Y. (2024, December 4). Deepfake Fraud: How AI is Bypassing Biometric Security in Financial Institutions. Retrieved February 10, 2025, from Group-IB website: https://www.group-ib.com/blog/deepfake-fraud/

ICO. (2023, May 19). What is special category data? Retrieved from ico.org.uk website: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/

National Institute of Standards and Technology. (2020, February 6). Facial Recognition Technology (FRT). Retrieved from NIST website: https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0

News, C. (2024, December 6). At-home cameras face hacking and safety concerns. Retrieved from Cbsnews.com website: https://www.cbsnews.com/video/at-home-cameras-face-hacking-safety-concerns/

Patel v. Facebook. (n.d.). Retrieved from EPIC - Electronic Privacy Information Center website: https://epic.org/documents/patel-v-facebook/

Winder, D. (2024, December 4). Now AI Can Bypass Biometric Banking Security, Experts Warn. *Forbes*. Retrieved from https://www.forbes.com/sites/daveywinder/2024/12/04/ai-bypasses-biometric-security-in-1385-million-financial-fraud-risk/