Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.249
Peer Reviewed Journal
https://doi.org/10.69758/GIMRJ2407IIIIV12P0003

e-ISSN No. 2394-8426
Special Issue on Scientific Research
Issue–II(II), Volume–XII

ADVANCED SECURITY SYSTEM USING IMAGE PROCESSING

Sutanuka Bhowmik
Department of Electronics and Communications Engineering
Year 3
Future Institute of Engineering and Management
Sonarpur, Kolkata, India, PIN 700150
Email-sutanuka.bhowmik04@gmail.com

Dr. Anirban Mandal
Department of Electronics and Communications Engineering
Associate Professor
Future Institute of Engineering and Management
Sonarpur, Kolkata, India, PIN 700150
Email-amandalfiem@ieee.org

ABSTRACT:-To counter the increase in bank robberies and house break-ins, we've devised a smart security system utilizing image recognition technology. This system ensures access to bank vaults, house doors, and safes which is limited to authorized individuals, effectively deterring unauthorized entry. The setup involves a SONAR-equipped door or vault, activating a camera here ESP32 is used upon detecting an individual's proximity. Face detection, facilitated by the ESP32 camera module, captures the individual's face. This image is compared to a database of registered individuals using the **Viola-Jones** object detection and face recognition algorithm. Upon a successful match, an electronic door lock, accompanied by a servo motor controlled by the Arduino, unlocks the door. If there's no match, the individual's image is sent to the owner's smartphone via the Telegram app for approval. Upon owner confirmation, access is granted, and the electronic lock unlocks the door enabling the electronic lock to open the door.

➢ **KEYWORDS:-** Proximity detection, enrollment, access request , authentication, image processing and recognition, Viola-Jones Object Detection and Recognition algorithm.

1. INTRODUCTION:

Smart face recognition-based vault systems employ sophisticated algorithms to identify and authenticate individuals based on unique facial features. By analyzing traits such as facial geometry, distance between eyes, and shape of the nose and jawline, this technology offers high accuracy and security. Unlike keypads or card readers, face recognition provides a seamless and non-intrusive user experience, minimizing the risk of unauthorized access due to lost or stolen credentials.

The adoption of face recognition technology in applications such as bank vaults addresses critical security challenges by ensuring only authorized personnel can gain entry, even under varying conditions or changes in appearance. It also streamlines authentication, allowing faster and more efficient access, crucial in emergencies.

Advanced features like live monitoring and real-time alerts enable continuous surveillance and instant notification of suspicious activities. Additionally, artificial intelligence and machine learning enhance the system's accuracy over time, adapting to new threats and evolving security needs.

2. WORKING PRINCIPLE:

A face recognition-based smart bank vault operates by utilizing advanced biometric technology to authenticate and authorize access to secured areas. The following outlines the key steps in its working principle:

- **Proximity Detection:**
  - The setup involves a SONAR-equipped door or vault, activating a camera (ESP32) upon detecting an individual's proximity.
- **Enrollment:**
  - **Data Capture:** Authorized personnel have their facial features captured using good resolution cameras. Multiple images are taken to account for different angles and lighting conditions.
  - **Feature Extraction:** The system extracts unique facial features such as the geometry of the face, the distance between eyes, the contour of cheekbones, and the shape of the nose and jawline.
  - **Template Creation:** These extracted features are used to create a digital template, a mathematical representation of the individual's face, which is stored in a secure database.
- **Access Request:**
  - **Image Capture:** When an individual attempts to access the door to say, a vault, his or her face is scanned by camera positioned at say, the vault entrance.
  - **Preprocessing:** The captured image is preprocessed to ensure optimal quality by adjusting for lighting, scale, and orientation.
- **Feature Matching:**
  - **Feature Extraction:** The system extracts facial features from the captured image, similar to the enrollment process.
  - **Comparison:** The extracted features are compared to the stored templates in the database. Advanced image processing and recognizing algorithms measure the similarity between the captured features and the stored templates. Here, using the Viola-Jones Object Detection and Recognition algorithm.
- **Authentication and Authorization:**
  - **Decision Making:** If the similarity score between the captured features and a stored template exceeds a predefined threshold, the individual is authenticated as an authorized user. The electronic lock is unlocked.
  - **Access Control:** Upon successful identification, the system triggers the vault's access control mechanisms, such as unlocking the door. If the identification fails, access is denied, and the captured picture is sent to security personnel through telegram, using TCP connection. By sending commands - /lock and /unlock to the telegram bot the owner can lock and unlock the door according to his wish. The owner is able to access the door from any part of the world.
- **Data Security and Privacy:**
  - **Encryption:** All facial data and templates are encrypted to protect against unauthorized access and data breaches.
  - **Access Logs:** The system maintains detailed logs of all access attempts, including successful and failed entries, for auditing and security analysis.

By leveraging these steps, a face recognition-based smart bank vault ensures a high level of security, efficiency, and convenience in protecting valuable assets.

3. ALGORITHM:

- **Initialization**

- **Include Libraries:** WiFi, WiFiClientSecure, soc/soc.h, soc/rtc_cntl_reg.h, esp_camera.h, UniversalTelegramBot.h, ArduinoJson.h
- **Define Constants and Variables:** Define pins for HC-SR04 sensor: TRIG_PIN, ECHO_PIN
- **Define WiFi credentials:** ssid, password
- **Define Telegram bot credentials:** chatId, BOTtoken
- **Define GPIOs for button, lock, and flash LED**
- **Define camera model GPIOs**
- **Initialize lock state and other variables**

- **Functions**
  - **Unlock Door Function:** If lock is currently locked, unlock it and return a message indicating the door is unlocked. If already unlocked, return a message indicating the door is already unlocked.
  - **Lock Door Function:** If lock is currently unlocked, lock it and return a message indicating the door is locked. If already locked, return a message indicating the door is already locked.
  - **Send Photo to Telegram:**
    - **Capture photo using the camera.**
    - **Connect to Telegram API. Send captured photo to the specified chat ID via the Telegram bot.**
    - **Handle and return the response from the Telegram server.**
  - **Handle New Telegram Messages:**
    - Iterate through the new messages received from the Telegram bot.
    - Check if the message is from an authorized user.
    - Process commands: /photo, /lock, /unlock, /start.
    - Send appropriate responses for each command.
- **Void Setup Function**
  - Disable brownout detector.
  - Initialize Serial communication.
  - Set pin modes for HC-SR04 sensor, lock, flash LED, and button.
  - Initialize WiFi connection.
  - Configure and initialize the camera.
  - Drop down the frame size for higher initial frame rate.
- **Loop Function**
  - Trigger the HC-SR04 sensor and measure the distance.
  - If an object is detected within 100 cm, capture and send a photo.
  - If the sendPhoto flag is set or the button is pressed, capture and send a photo.
  - Check for new messages from the Telegram bot at regular intervals and handle new messages.

4. FURTHER ADVANCEMENT:

Additionally, the system can be further modified to trigger an automated alert AI generated voice call to the nearby police station stating the address of the location at the owner's discretion. This comprehensive approach enhances security by utilizing advanced technology to authenticate

individuals and prevent unauthorized access, providing a robust solution to combat theft and burglary.

The system can use machine learning algorithms to improve its accuracy over time. By analyzing successful and failed authentication attempts, it adapts to new conditions, such as changes in authorized users' appearances or new security threats.

5. OUTCOME:

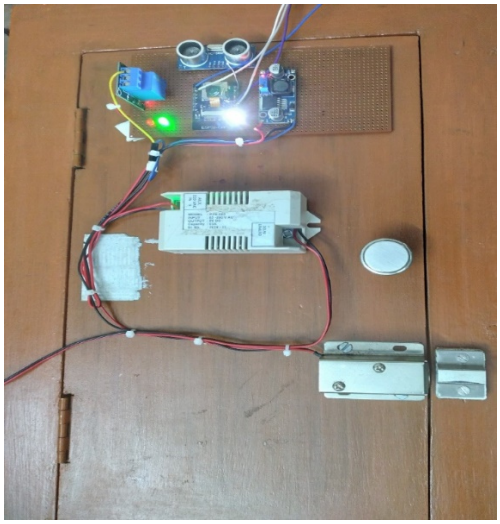

FIGURE 1: ADVANCED SECURITY SYSTEM USING IMAGE PROCESSING

FIGURE 2: A SCREEN-SHOT OF THE CHAT WITH THE TELEGRAM BOT. THE ESP32 CAM SENDS PICTURES TO THE OWNER VIA TELEGRAM USING TCP PROTOCOL. THE OWNER SENDS "/unlock" COMMAND TO UNLOCK THE DOOR

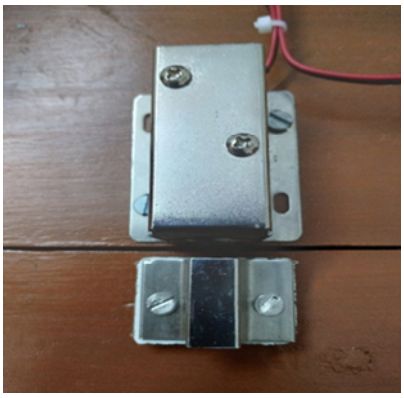

FIGURE 3: THE BOT SENDS COMMAND TO THE ESP32 TO UNLOCK THE DOOR. THE ELECTRONIC LOCK UNLOCKS THE DOOR.

6. CIRCUIT BLOCK DIAGRAM:

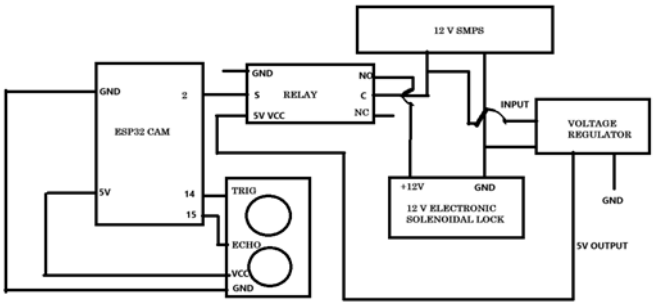

FIGURE 4: CIRCUIT BLOCK DIAGRAM

7. ADVANTAGES:

- **Enhanced Security**: The SONAR-equipped system ensures that the door or vault activates only when an individual is nearby, minimizing false alarms and unauthorized access attempts.
- **Energy Efficiency:** Activating the camera only when proximity is detected conserves energy, extending the lifespan of the system's components.
- **Convenience:** Automatic detection and activation streamline the access process, providing a seamless experience for authorized personnel.
- **Comprehensive Data Capture:** Capturing multiple images from different angles and lighting conditions ensures robust facial recognition, reducing the likelihood of false negatives.

- **Detailed Feature Extraction:** By focusing on unique facial features, the system creates highly accurate digital templates, improving the accuracy of authentication.
- **Secure Template Creation:** Digital templates are mathematical representations, which are more secure and harder to replicate compared to raw images.
- **Automated Image Capture:** Automatic scanning upon access request ensures that the process is quick and efficient, without requiring manual intervention.
- **Image Preprocessing:** Adjusting for lighting, scale, and orientation ensures that the captured images are of optimal quality, enhancing the accuracy of feature extraction and matching.
- **Reliable Comparison:** Advanced similarity measurement algorithms provide reliable and accurate comparisons between captured features and stored templates, minimizing false positives and negatives.
- **High Accuracy:** The predefined similarity threshold ensures that only authorized individuals are granted access, enhancing security.
- **Remote Control:** The integration with Telegram allows the owner to lock and unlock the door remotely, providing flexibility and control from anywhere in the world.
- **Real-time Alerts:** If access is denied, the system immediately notifies security personnel with a captured image, enabling prompt response to potential threats.
- **Encryption:** Encrypting all facial data and templates protects against unauthorized access and data breaches, ensuring privacy and security.
- **Detailed Access Logs:** Maintaining logs of all access attempts allows for comprehensive auditing and security analysis, helping to identify and mitigate potential security risks.

8. CONCLUSION:

The system's advanced image preprocessing and feature matching algorithms further enhance the reliability of authentication. With the added benefits of remote control through Telegram and real-time security alerts, the smart door lock offers unparalleled convenience and control to the owner. Robust encryption safeguards facial data and templates, while detailed access logs provide critical insights for auditing and security analysis. Overall, this smart door lock system represents a significant advancement in secure access technology, offering peace of mind through its sophisticated, layered approach to security and user management.

9. REFERENCES:

[1] Rafael C. Gonzalez "Digital Image Processing" Tata McGraw Hill, 2007

[2] Partha Majumder "Mastering Image Classification Algorithms for Machine Learning" bpb, 2004