Laboratory Report

On

Behavioural Hazard Assesment & Security Awareness Detector System

ELECTRONICS PRODUCT DEVELOPMENT (EC38001)

Submitted By

ABIR SARKAR (2230057)

ARPIT RATH (2230070)

SWAPNEEL BHATTACHARJEE (2230133)

ANUSMITA MAITI (2230235)

B.Tech Programme in Electronics and Computer Science Engineering

School of Electronics Engineering

Kalinga Institute of Industrial Technology, (Deemed to be University)

Bhubaneswar, India

November 2024

AIM:

In an increasingly complex and dynamic world, public and workplace security is a priority. A "Behavioral Hazard Assessment & Security Awareness Detector System" aims to address potential security risks by analyzing human behaviors that could indicate safety hazards or security threats. The purpose of this project is to create an intelligent system that can assess behavioral cues from individuals in real time using image processing, sensors, and machine learning. By identifying unusual or hazardous behaviors, the system provides an early warning mechanism to prevent potential risks and improve safety.

This system, designed to utilize a camera, Arduino-based microcontroller, and infrared sensor, will continuously monitor a designated area, analyzing body language, movements, and other behavioral indicators that could signal threats. The goal is to develop a scalable solution that can be deployed across various environments such as public spaces, workplaces, and schools, enhancing overall security and creating a safer environment.

PROBLEM STATEMENTS:

- **Introduction to the Problem**: Start with a description of the importance of behavioral analysis for hazard assessment and security.
- **Context and Relevance**: Explain the increasing need for systems capable of detecting security risks through behavior, especially in environments like workplaces, schools, and public places.
- **Specific Aim**: Define the goal of the project—such as developing a system to detect behaviors associated with potential hazards or security threats in real-time.
- **Significance**: Discuss the impact such a system could have on improving security and preempting dangerous situations by detecting suspicious behavior patterns.

EQUIPMENTS REQUIRED

1. **Hardware Components**:

- **Camera**: Captures live video feed of individuals in the monitored area. A high-resolution camera with adequate frame rate is chosen to capture detailed images.
- **Arduino Microcontroller**: An Arduino board is used to integrate infrared sensors and other peripherals. It acts as a processing unit to detect physical movement within its range.
- **Infrared (IR) Sensor**: Detects motion and identifies the presence of individuals. The IR sensor can trigger image capturing when it senses movement, enhancing system efficiency.

2. **Software Components**:
   - **Python**: The primary programming language used to develop the image processing and machine learning modules.
   - **Libraries**:
     - **TensorFlow/Keras**: For building and training the deep learning models used for behavioral recognition and hazard detection.
     - **OpenCV**: For handling image capture and processing tasks. OpenCV helps preprocess the camera feed for the model, including resizing, grayscale conversion, and applying filters.
     - **Serial Communication Libraries**: To facilitate communication between the Arduino and the computer running the Python application.
3. **Dataset**:
   - **Kaggle Dataset**: A pre-existing dataset from Kaggle containing images labeled with various behaviors and emotions is used. This dataset is essential for training and validating the model, allowing it to recognize behavioral patterns indicative of security risks.

METHODOLOGY USED

The development of the Behavioral Hazard Assessment & Security Awareness Detector System involves several phases:

1. **Data Collection**:

    - Relevant behavioral data is collected from a Kaggle dataset containing labeled images with various expressions and actions. This dataset serves as the primary training material for the model.
2. **Data Preprocessing**:
    - The images in the dataset are preprocessed to meet model input requirements. This includes resizing each image to a standard dimension (48x48 pixels), converting it to grayscale, and normalizing pixel values to improve model efficiency.
3. **Model Training**:
    - Using TensorFlow and Keras, a convolutional neural network (CNN) is designed to learn features from the preprocessed images.
    - The model is trained on the dataset, allowing it to identify suspicious or hazardous behaviors, such as aggressive postures or erratic movements.
    - A portion of the data is reserved for validation and testing to ensure model accuracy and robustness.
4. **Integration with Hardware**:
    - The Arduino microcontroller interfaces with the IR sensor to detect motion and prompt the camera to capture images when someone enters the monitored area.
    - The camera continuously feeds images to the computer, where the Python-based detection model processes them.
5. **Real-Time Analysis**:
    - As the system receives images, OpenCV preprocesses them before feeding them into the trained CNN.
    - The model assesses behavior in real-time, and if a potentially hazardous behavior is detected, an alert is generated.

PRINCIPLE ADOPTED

 Machine Learning and CNN for Behavior Detection:

- A convolutional neural network (CNN) is employed due to its proven effectiveness in image classification tasks. CNNs are adept at recognizing spatial patterns, making them suitable for analyzing human behavior based on visual cues.
- The CNN learns various facial expressions and body postures associated with different behaviors. By training on a large dataset, the model generalizes well to detect hazardous behavior accurately.

 Image Processing with OpenCV:

- OpenCV is used for real-time image capture and processing. Preprocessing techniques, such as resizing and grayscale conversion, reduce computational requirements and improve model inference speed.
- OpenCV also helps manage camera feeds and integrate seamlessly with the Arduino system, creating a streamlined image capture pipeline.

 Security Awareness through Infrared Sensors:

- The infrared sensor is a cost-effective solution for detecting movement in the monitored area. When the IR sensor detects motion, it triggers image capture, helping optimize resource usage and ensuring that the model only processes relevant frames.

HOW WILL IT WORK

 System Overview:

- The system is designed to operate continuously, with the IR sensor detecting motion and the camera capturing images. The images are processed through the CNN model to determine if the behavior poses a potential security risk.

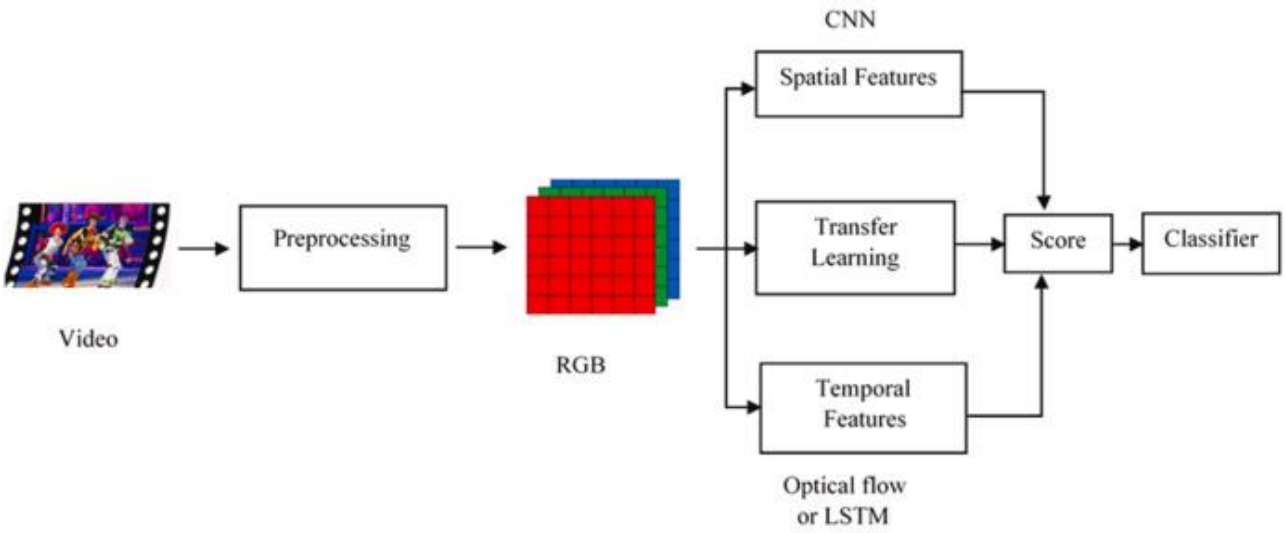
 Process Flow:

- **Step 1**: The IR sensor, interfaced with the Arduino, monitors the designated area for movement. When movement is detected, it signals the camera to capture images.
- **Step 2**: Captured images are sent to the computer where the Python-based application runs. OpenCV preprocesses the images by resizing and converting them to grayscale.
- **Step 3**: The processed images are fed into the CNN model built in TensorFlow/Keras.
- **Step 4**: The model classifies the behavior captured in the image. If the behavior aligns with hazardous or security-threatening categories, the system triggers an alert.
- **Step 5**: The alert system, which could be an alarm or notification, informs security personnel of the potential threat.

 Alert Mechanism:

- Upon detecting a suspicious behavior, the system sends an alert, which could be a visual indicator, sound alarm, or digital notification, depending on the intended deployment setup. This ensures that security personnel can respond promptly.

FLOW CHART OF THE ALGORITHM OF THE SOFTWARE



Explaination of the flow chart of the Algorithm:

Video Input:

- The system begins by capturing or receiving a video input, which contains frames showing people or behaviors that the system needs to analyze.

Preprocessing:

- The raw video data undergoes preprocessing. This step may involve resizing frames, converting to grayscale, normalization, or any other preparation needed to ensure consistency and efficiency in model processing.
- After preprocessing, each video frame is in a standard format, typically as RGB images, making it easier for the model to process.

RGB Frames:

- The frames are separated into RGB components, where each pixel in the frame is represented by red, green, and blue channels. This format is

compatible with CNN (Convolutional Neural Network) models, which can extract spatial features from images.

CNN - Spatial Features:

- The RGB frames are fed into a CNN, which is responsible for extracting spatial features. Spatial features are details within each frame, such as shapes, textures, and patterns. These features help the model understand the static aspects of each frame, which are essential for recognizing the appearance and posture of individuals in the video.

Transfer Learning:

- Transfer learning is used to leverage a pre-trained model, which has already learned relevant patterns from a large dataset. This helps improve the accuracy and efficiency of the model by reusing previously learned features. Transfer learning is especially useful when working with limited datasets.

Temporal Features - Optical Flow or LSTM:

- To capture changes over time, the system uses temporal feature extraction methods. **Optical Flow** calculates motion between frames, providing data about the direction and speed of movement. Alternatively, **LSTM (Long Short-Term Memory)** networks are used to learn temporal dependencies, making the system more adept at identifying behavior patterns across sequences of frames rather than individual frames alone.

Score:

- The outputs from spatial and temporal feature extractors are combined and scored. The score indicates the likelihood of certain behaviors or actions being present in the video.

Classifier:

- Finally, a classifier uses the score to categorize the behavior. This classifier could be a simple fully connected layer or a more complex classification model. It determines the type of behavior, like aggression, calmness, or suspicious activity, and sends this information for further action, like generating an alert if necessary.

SCREEN SHOT OF THE SOFTWARE

[93]:
```
# Emotion classes for the dataset
Emotion_Classes = ['Angry', 'Disgust', 'Fear', 'Happy', 'Neutral', 'Sad', 'Surprise']

# Assuming test_generator and model are already defined
batch_size = test_generator.batch_size

# Selecting a random batch from the test generator
Random_batch = np.random.randint(0, len(test_generator) - 1)

# Selecting random image indices from the batch
Random_Img_Index = np.random.randint(0, batch_size, 10)

# Setting up the plot
fig, axes = plt.subplots(nrows=2, ncols=5, figsize=(10, 5),
                         subplot_kw={'xticks': [], 'yticks': []})

for i, ax in enumerate(axes.flat):
    # Fetching the random image and its label
    Random_Img = test_generator[Random_batch][0][Random_Img_Index[i]]
    Random_Img_Label = np.argmax(test_generator[Random_batch][1][Random_Img_Index[i]], axis=0)

    # Making a prediction using the model
    Model_Prediction = np.argmax(model.predict(tf.expand_dims(Random_Img, axis=0), verbose=0), axis=1)[0]

    # Displaying the image
    ax.imshow(Random_Img.squeeze(), cmap='gray')  # Assuming the images are grayscale
    # Setting the title with true and predicted labels, colored based on correctness
    color = "green" if Emotion_Classes[Random_Img_Label] == Emotion_Classes[Model_Prediction] else "red"
    ax.set_title(f"True: {Emotion_Classes[Random_Img_Label]}\nPredicted: {Emotion_Classes[Model_Prediction]}", color=color)

plt.tight_layout()
plt.show()
```

[91]:
```
train_loss, train_accu = model.evaluate(train_generator)
test_loss, test_accu = model.evaluate(test_generator)
print("final train accuracy = {:.2f} , validation accuracy = {:.2f}".format(train_accu*100, test_accu*100))
```

```
718/718 ━━━━━━━━━━━━━━━━━━━━ 199s 278ms/step - accuracy: 0.5424 - loss: 2.1804
225/225 ━━━━━━━━━━━━━━━━━━━━ 103s 459ms/step - accuracy: 0.5179 - loss: 2.2656
final train accuracy = 53.94 , validation accuracy = 51.18
```

MARKET SURVEY

1. Market Need and Demand

The need for automated behavioral assessment and security awareness systems has surged across various sectors due to rising safety concerns, growing urban populations, and increased emphasis on proactive security measures.

- **Public Security**: Airports, metro stations, and large public venues require security systems that can identify potentially harmful behavior before incidents occur. Governments and organizations are looking for automated solutions to enhance traditional CCTV and surveillance systems.
- **Workplace Safety**: Corporations are adopting technology to mitigate risks associated with workplace violence, harassment, and safety hazards. Behavioral assessment systems can improve workplace safety and reduce liability.
- **Healthcare**: Hospitals and mental health facilities need to monitor patients' behavior to manage aggressive or harmful actions proactively, which is critical for patient and staff safety.
- **Retail and Commercial Spaces**: Retailers are adopting behavior detection technology to prevent shoplifting, fraud, and other malicious activities. Security awareness systems help detect suspicious behavior patterns that may indicate criminal intent.
- **Education Sector**: Schools and universities are increasingly interested in behavior monitoring solutions to prevent bullying, violent incidents, and other security concerns, helping create safer environments for students.

2. Market Growth and Projections

The global market for AI-based behavior detection systems, particularly for security applications, has been growing rapidly and is projected to continue expanding in the coming years.

- **Video Surveillance Market**: The global video surveillance market, which includes AI-driven behavioral detection solutions, was valued at over USD 50 billion in 2023 and is expected to grow at a CAGR of over 10% through 2028.
- **Artificial Intelligence in Security**: The AI security market is projected to grow from USD 8 billion in 2023 to over USD 40 billion by 2030, driven by advancements in machine learning, image processing, and behavior analysis technology.
- **Automation in Public Safety**: Governments and municipalities are increasing investments in AI and automation to improve public safety, creating opportunities for systems that can provide real-time behavior analysis and threat detection.

3. Competitor Analysis

A number of companies and startups are working on similar AI-powered security systems, though few focus specifically on behavioral hazard detection combined with real-time alerting capabilities.

- **Large Security Companies**:
  - **Hikvision** and **Dahua Technology**: These companies offer advanced surveillance solutions, including AI-based video analytics. However, they primarily focus on object detection and face recognition rather than behavior-based hazard assessment.
  - **Honeywell**: Honeywell's security products include AI-driven surveillance and analytics but generally focus on perimeter security, face recognition, and access control.
- **Emerging AI-Driven Security Startups**:
  - **Trueface** and **AnyVision**: These companies focus on face recognition and suspicious activity detection but do not offer comprehensive behavior hazard detection with temporal feature analysis.
  - **Uncanny Vision**: This company provides AI-based vision systems for surveillance but has limited focus on specific behavior assessment.
- **Competitive Advantage for Proposed System**:
  - While many companies provide facial recognition and motion detection, fewer focus on behavior classification based on temporal features (Optical Flow or LSTM-based models) for continuous behavior monitoring. This differentiation offers a unique competitive edge, especially for clients interested in real-time detection of specific hazardous behaviors.

4. Key Market Players: The behavioral assessment and security awareness market is populated by key players in AI security, with most offering some level of behavior detection or motion analysis.

Axis Communications: Known for its high-quality cameras, Axis also offers video analytics software, which includes some behavior analysis functions.

BriefCam: Provides video analytics that can filter through hours of footage in seconds, identifying events like loitering or crowd formation.

COMPARISON WITH EXISTING PRODUCT

Feature/Aspect	Behavioral Hazard Assessment & Security Awareness Detector System	Hikvision & Dahua Technology	AnyVision & Trueface	Kogniz & Axis Communications	BriefCam
Behavior Detection Focus	Specifically designed for detecting hazardous behaviors using temporal (Optical Flow or LSTM) and spatial features.	Primarily focuses on object detection, motion detection, and face recognition, not behavior detection.	Primarily focuses on object detection, motion detection, and face recognition, not behavior detection.	Primarily focuses on object detection, motion detection, and face recognition, not behavior detection.	Detects general activities like crowding or loitering but lacks specific hazardous behavior detection.
Technology Used	Combines CNN for spatial features, transfer learning, and Optical Flow or LSTM for temporal features, improving real-time behavioral hazard analysis.	Uses basic AI models primarily for object and face recognition, with limited temporal analysis capabilities.	Deep learning models for face and activity recognition but lacks complex temporal feature analysis for specific behaviors.	General computer vision AI for detecting activities, without complex temporal feature analysis.	Primarily uses video analytics, with general object tracking and crowd detection, not specific hazardous behaviors.
Real-Time Alerting	Provides real-time alerts for specific hazardous behaviors, like aggression or erratic movement, making it proactive in nature.	Real-time object and motion detection but lacks specific real-time behavioral alerts for hazards.	Real-time face and object recognition; lacks detailed real-time behavior-specific alerts.	Provides real-time monitoring but mostly for tracking and general activity detection, not hazardous behaviors.	Real-time video analytics focused on activity detection rather than specific hazard behavior alerts.
Accuracy in Hazard Detection	High accuracy due to the combination of CNN, transfer learning, and temporal features (Optical Flow or LSTM), allowing for nuanced behavior detection.	High accuracy for object detection and face recognition but limited to basic motion analysis for behavior detection.	Reliable for face recognition and simple activity detection but lacks depth in hazardous behavior analysis.	Accurate in general object tracking but lacks specificity in hazardous behavior analysis.	High accuracy for crowd behavior and general activities, but less effective for specific hazardous behavior.

Scalability	Designed for flexible scalability, supporting various locations and configurations, from small businesses to large public spaces.	Highly scalable with extensive support, especially suited for large-scale surveillance.	Scalable but mostly focuses on face recognition rather than behavior detection, limiting its use cases.	Scalable for general monitoring, often used in enterprise environments and urban settings.	Scalable for general monitoring, often used in enterprise environments and urban settings.
Cost	Moderate to high, depending on the level of customization and deployment size. Cost-effective for clients needing specific behavior monitoring	High, especially for advanced surveillance and face recognition systems with complex setups.	High, as it uses advanced face recognition technology suitable for corporate or high-security environments.	Moderate to high, depending on customization. Known for good support and quality.	Moderate to high, depending on customization. Known for good support and quality.

FUTURE SCOPE

The **Behavioral Hazard Assessment & Security Awareness Detector System** has significant potential for future enhancements and wider applications as technology continues to evolve. Some key areas for future development include:

1. **Enhanced Accuracy through Advanced AI Models**:
    - Future iterations could leverage more sophisticated deep learning models, such as transformers or multimodal neural networks, to improve accuracy in recognizing complex behaviors and predicting potential hazards.
    - Hybrid models combining vision-based analysis with additional sensor data (e.g., audio or environmental sensors) could provide a more comprehensive understanding of context, further improving system performance.
2. **Improved Real-Time Capabilities**:
    - With advancements in edge computing, processing can be moved closer to the data source (e.g., on local devices), reducing latency and making real-time hazard detection even faster. This would be particularly beneficial for high-security environments where immediate responses are critical.
3. **Behavior Prediction and Anomaly Detection**:

- The system could evolve to not only detect hazardous behaviors but also predict potential threats based on patterns over time, alerting authorities before a hazard occurs. Advanced anomaly detection algorithms could help identify unusual behavior patterns that may indicate security risks.

4. **Integration with IoT and Smart City Infrastructures**:
   - Integration with Internet of Things (IoT) devices and smart city infrastructure can broaden the system's application to urban safety and public monitoring. For example, linking with city-wide surveillance and traffic systems could enhance overall safety and traffic management.
5. **Expanded Applications in Different Sectors**:
   - **Healthcare**: The system could be adapted to monitor patients for behaviors indicating mental distress or agitation, helping prevent incidents in mental health or emergency care facilities.
   - **Education**: Implementing this system in schools could help detect bullying or violent behavior, enhancing student safety.
   - **Retail and Banking**: In retail stores and banks, the system could monitor for behaviors associated with theft, fraud, or other malicious intentions, helping businesses mitigate risks.
6. **Enhanced Privacy and Data Protection Measures**:
   - As regulations around privacy tighten, future iterations could focus on privacy-enhanced computation techniques, like federated learning, which allows data to be analyzed without needing to be transmitted to a central server. This would help maintain privacy while improving data security.
   - Implementing ethical AI practices, such as bias mitigation and transparent model interpretability, will be important as adoption increases across various sectors.
7. **Customizable Alerting and Response Systems**:
   - Future versions could allow users to customize alert levels and responses based on specific contexts, enabling greater flexibility in settings with varying security needs, such as corporate offices, public events, and high-security areas.
8. **Enhanced Market Expansion and Cost Reduction**:
   - As the technology matures and becomes more affordable, adoption is likely to increase across smaller businesses and institutions that may currently be priced out. Improved cost-efficiency could make the system accessible to a broader range of clients, including schools, small businesses, and non-profits.

CONCLUSION

The **Behavioral Hazard Assessment & Security Awareness Detector System** represents an innovative approach to security and safety monitoring, using advanced machine learning and image processing techniques to detect and assess potentially hazardous behaviors in real time. By focusing specifically on behavior-based analysis, the system fills a gap in the market where traditional surveillance systems fall short. Current competitors largely focus on face recognition, object detection, and general activity tracking, while this system addresses the need for proactive hazard detection.