IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⋇ Impact Factor 8.066 ⋇ Peer-reviewed / Refereed journal ⋇ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10523

Tracking of Mobile Phones for Piracy Detection

Chandana L[1],Priyanka K[2],Danesh Raju V[3],Surekha Borra[4],Dheemanth KN[5]

Department of ECE,K.S. Institute of Technology,Bangalore, India[1-5]

Abstract: The film industry has faced challenges with unauthorized reproduction and distribution of movies. To combat this issue, we propose an innovative system that employs IP cameras, Python, and a regular computer to detect instances of piracy in real-time and inform the relevant parties. Our solution uses a specialized object detection model trained with a set of images of the item to be detected, particularly mobile phones, which are associated with piracy. We utilized the YOLOv5 repository to construct the model, which can provide precise bounding box data to indicate the object's exact location in the frame. Additionally, the system includes a mail service that notifies the theater owner or other authorized individuals of piracy occurrences and provides them with an image of the incident. This allows them to take prompt action. The system operates in real-time and can monitor live feeds from multiple cameras at once to detect any piracy instances immediately.

Keywords: MoviePiracy, Yolov5, IP camera.

I. INTRODUCTION

Movie piracy is the unauthorized acquisition of copyrighted content without the authorization of film makers. This is a new epidemic that is economically impacting the film industry on a global level. According to a survey, pirated movies gain around 230 billion views every year. It was also reported that Indian media loses about US$2.8 billion to piracy. As per the study conducted by the US-India Business Council (USIBC), the Indian film industry experiences a loss of 11% in employment due to piracy. It also influences content creation by discouraging filmmakers, directors, and producers from making sequels and remakes. Consequently, the national government and entertainment firms have come up with effective strategies and tools to combat piracy. The Indian government implemented one such strategy by passing the Cinematograph Act in 2019. This act declares piracy a crime and penalizes pirates with three years of imprisonment and a fine of 10 lakh rupees [1].

The illegal copying of movies for the purpose of selling them at a lower market price is referred to as movie piracy. Some of the ways in which piracy can occur are camera recording, DVD and VOD ripping, tele sync, digital distribution copy, telecine, and WEB-DL. Camcorder piracy can be classified into pre-release and post-release piracy. In pre-release piracy, the movie is pirated during exclusive screenings for sponsors, reviewers, and VIPs. During this

DOI: 10.17148/IARJSET.2023.10523

time, piracy may occur in two possible ways. In one of the ways, guests can record the movie and make a copy available for unauthorised dissemination. These copies are generally of low audio and video quality. This kind of piracy is known as camcorder piracy [2]. On the other hand, while the movie is being projected, theatre operators can record the film by employing a camcorder mounted on the tripod at the theatre's back end. A telesync system is used to derive sound from the audio system directly. In post-release piracy, both theatre operators and audiences can pirate the movie and sell it at a lower price or share the pirated videos free of charge on social media.

Therefore, an antipiracy system is developed using machine learning techniques by employing cameras in a theatre environment. The proposed approach mainly focuses on finding the presence of active camcorders held by pirates in the theatre.

II. RELATED WORK

Naumovich et al. [3] Concerns concerning data protection have become more urgent as computers become more commonplace. In many instances, an attacker just has to overcome the software program's responsible for securing the data in order to steal or change it. The creation of efficient and effective systems to preserve digital data is urgently needed. Programs and program elements like reusable class libraries should both be covered by software protection techniques. Because anybody with access may modify the software installed on a typical end user's PC, it is inherently unreliable.

The idea of a software application as a standalone product is eliminated as a radical response to the issue of piracy. Most calculations are performed by a server in the well-known application server architecture, which is likely controlled by a reliable company or a software vendor, while clients receive dynamically created content. A software watermarking taxonomy makes a broad distinction between static and dynamic watermarks. In the future, there will be a lot of new advances in the fields of tamper- proofing, obfuscation, and watermarking, as well as cryptography and systems engineering, which are established fields. Real-world applications are unlikely to be served by a single solution; instead, a mix of sound system designs, cryptic primitives, and instead, a mix of sound

system design, cryptic primitives, and several software- and hardware-based approaches will be required.

Fang et al. [4] described a method for recognising hand gestures in real time using "skin colour detection' and "motion detection'. Hand images are defined using histograms of oriented gradients (HOG). PCA-LDA are used to extract HOG features in low-dimensional subspace; the distance between the project features and the centre of each gesture is determined; and finally, the closest neighbour approach is used to acquire the recognition results. The suggested technique achieved a detection rate of up to 91% with real-time performance, according to the experimental data. Adaptive skin colour detection and motion detection are used to find hand areas. Zhao et al. [5] have provided us with an up-to-date review of skin colour modelling and detection methods. Motion detection is another helpful idea that is being extensively used in computer vision to identify and remove regions of interest. Background subtraction is used to detect motion in an image. A hand gesture can be well described by a distinct local distribution of edges or gradients of intensity. It tries to shape the scatter to make it more accurate for categorization. In this way, LDA selects projection matrix W. The scatter factor is maximized as a function of the ratio of between-class scatter to within-class scatter.

Wagner et al. [6] presented two approaches for natural feature tracking using planar targets, mentioning that it is a complex problem to track natural features as it requires high computational power. Targets in real time that allow robust pose estimation are estimated, achieves interactive frame rates of up to 30 Hz for natural feature tracking from textured planar targets on current-generation phones.

Garg et al. [7] reviewed the recognition of hand gestures using vision. The existing methods are categorised as 3D model-based methods and appearance-based methods, highlighting the benefits and drawbacks. Approach based on a 3D hand model, three-dimensional hand model based approaches attempt to estimate hand parameters by comparing input images to the potential 2D appearance projected by the 3-D hand model. This is done by comparing the input images to the 3D kinematic hand model, which has many degrees of freedom (DOFs). This technique is excellent for generating convincing interactions in virtual settings.

T. Kong et al. [8] FoveaBox is an accurate, flexible, and completely anchor-free framework for object detection. It learns the object's existing possibilities and the bounding box coordinates without an anchor reference. The code has been made publicly available. Anchor-based object detection requires the solution of two main tasks: recognition and localization. Most detectors rely on anchors to enumerate the possible locations, scales, and aspect ratios of target objects. The anchor method suggests dividing the box space into discrete bins and refining the object box in the corresponding bin. To achieve a good recall rate, anchors must be carefully designed based on statistics computed from the training or validation set. Anchor-free detectors have been considered unsuitable for generic object detection due to the difficulty of multi-scale object detection and the relatively low recall. It simultaneously predicts the object position and the corresponding boundary and gives a clean solution for detecting objects without prior candidate boxes.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ∺ Impact Factor 8.066 ∺ Peer-reviewed / Refereed journal ∺ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10523

Kim et al. [9] focused on unauthorised reproduction and distribution of works protected by intellectual property without the owner's consent. The study examined the characteristics of pirate sites and suggested an intelligent method for identifying them. A total of 314 websites were evaluated, with a 1:1 ratio of both legal and pirated websites. An accuracy of 95% was achieved when the intelligent identification approach was used for pirate sites, 91% for video streaming websites, and 93% for websites that feature cartoons. An accuracy of 95% was achieved when the intelligent identification approach was used for pirate sites, 91% for video streaming websites, and 93% for websites that feature cartoons. Pulungan et al. [10] detected objects based on colour, shape, edges, and size. By categorising each pixel's grayscale value into the black-and-white and colour classes, object detection was achieved.

The proposed anti-piracy model is detailed in Section 3. The simulation results are presented in Section 4. The conclusion of this study is included in Section 5.

III. PRILIMINARIES

A. IP Camera

IP cameras, also known as network cameras, are video cameras that transmit their signals over a computer network, or the internet. They are commonly used for surveillance purposes in homes, businesses, and public spaces. IP cameras can be accessed and controlled remotely using a computer or mobile device, which allows users to monitor and record footage from anywhere with an internet connection. They can also be integrated with other security systems, such as alarms and access control systems. IP cameras come in a variety of shapes and sizes, from small, discreet cameras that can be placed almost anywhere to large, high-resolution cameras for monitoring wide areas. They can be used indoors or outdoors, and some models are designed to withstand harsh weather conditions. IP cameras are typically classified as fixed, varifocal, or pan-tilt-zoom depending on their capabilities (PTZ cameras). Varifocal cameras may remotely change the image's zoom, in contrast to fixed cameras, which offer a static perspective on the topic. The camera assembly can be remotely moved in any direction with PTZ cameras as well. This can be used to manually change the monitoring area or track motion. IP cameras come in indoor and outdoor versions. To endure external circumstances, outdoor cameras are frequently rated IP65 or IP67.

.

B. Roboflow

Roboflow is a computer vision platform that provides developers with tools to create, deploy, and manage machine learning models for image and video analysis. It simplifies the process of building computer vision applications by offering features like data preprocessing, model training, and deployment. Roboflow supports a wide range of computer vision tasks, such as object detection, image segmentation, and image classification. It also provides access to a large set of pre-trained models that can be customized for specific use cases. Additionally, Roboflow offers integrations with popular machine learning frameworks like TensorFlow, PyTorch, and Keras, making it easy for developers to incorporate computer vision into their existing workflows.

C. YOLOv5

YOLOv5 (You Only Look Once Version 5) is an object detection algorithm that was developed by Ultralytics. It is the latest version of the YOLO family of object detection models, and it is built on PyTorch. YOLOv5 is faster, more accurate, and more efficient than previous versions of YOLO, making it one of the most popular object detection models currently available. YOLOv5 uses a single-stage object detection pipeline, which means that it predicts all object bounding boxes and class probabilities directly from the input image in one go. This makes it much faster than two-stage object detection pipelines, which require separate region proposal and object classification stages.

YOLOv5 comes in several sizes, including YOLOv5s, YOLOv5m, YOLOv5l, and YOLOv5x, with each size having more parameters and higher accuracy than the previous one. YOLOv5 has been trained in several large- scale object detection datasets, such as COCO and Open Images, and it can detect hundreds of different object classes. YOLOv5 is a powerful and efficient object detection algorithm that has a wide range of applications in computer vision, including autonomous driving, surveillance, and robotics.

IV. PROPOSED MODEL

The proposed system operates in real-time and can monitor live feeds from multiple IP cameras installed in movie theatre at once to detect any piracy instances immediately. The system setup is as shown in Fig. 1.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⸎ Impact Factor 8.066 ⸎ Peer-reviewed / Refereed journal ⸎ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10523

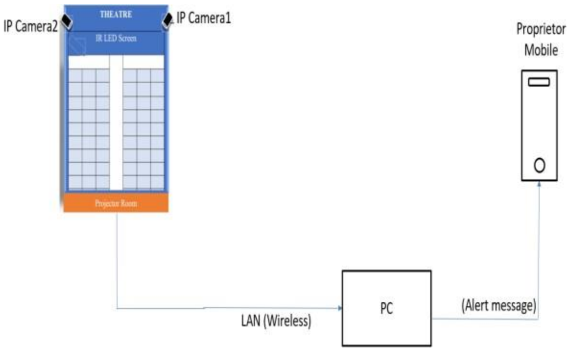

Fig. 1 IP Camera setup in Theatres for piracy detection

The proposed system utilized the YOLOv5 repository to construct the model, which can provide precise bounding box data to indicate the mobile/camcorder object's exact location in the frame. Additionally, the system includes a mail service that notifies the theater owner or other authorized individuals of piracy occurrences and provides them with an image of the incident. This allows them to take prompt action.

A. Establish connection with IP camera using RTSP

The protocol is used for establishing and controlling media sessions between end points. In short, RTSP is one- way cameras and recorders transfer information back and forth. RTSP allows to see the stream of the recorder or camera through an application like VLC.

B. Convert live feed into multiple frames

Open the video feed: Libraries and tools are used to open the video feed, depending on the source of the feed and the format of the video. The frame rate of the video feed will determine the number of frames per second that are captured. Using the time interval between frames, frames from the video feed are extracted at regular intervals and are saved as individual image files, which are processed further using computer vision algorithms.

C. Detection and localization of mobile phones

Feed the video to detection model and using a loop, each frame of the video is read and passed to the detection model. The frames are resized and are converted to a specific colour space. Once the frames have been pre-processed, they are passed to the detection model to perform object detection. The model analyses each frame and return information about any objects it detects. OpenCV libraries are used to visualise the results of the detection model, such as bounding boxes around detected objects or labels indicating the type of object detected. The object detection model will return a list of detected objects and their corresponding bounding boxes.

D. Capture and send the detected mobile phones to owner of theatre.

The system loops over the detected objects, filter for mobile phones and draw a bounding box around each detected mobile phone. The dataset of images or videos that contain mobile phones are collected and labeled using a pre- trained fine-tuned deep learning model. This involves training the model to recognize and localize mobile phones in images or videos. Once the model is trained, use it to detect mobile phones in new images or videos. The model will output the location of each detected mobile phone as a set of coordinates. The model also draws bounding boxes around each detected mobile phone using the coordinates. Fig. 2 and Fig. 3 show the flowcharts for training the model and real time detection of mobile piracy.

DOI: 10.17148/IARJSET.2023.10523

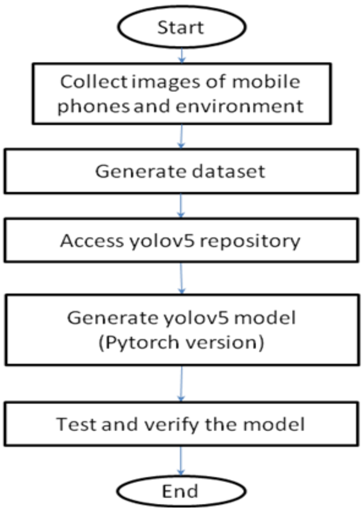

Fig. 2 Training

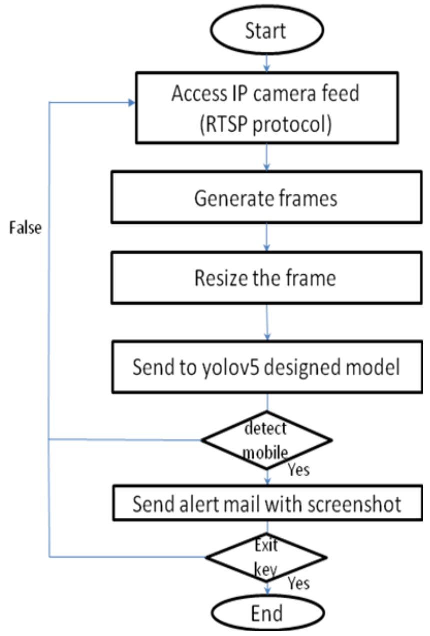

Fig. 3 Flow chart for tracking mobile phones for piracy detection

V. RESULTS

The proposed system is designed to detect and prevent piracy occurrences in a theater environment by utilizing computer vision and machine learning techniques. Specifically, the system employs the YOLOv5 repository to construct an object detection model that can precisely localize and identify mobile phones and camcorders in a video feed. The system first establishes a connection with an IP camera using the RTSP protocol, which allows for the transfer of video feed between the camera and the system. The live feed is then converted into multiple frames, which are processed using computer vision algorithms to detect and localize mobile phones and camcorders in each frame.

Once a mobile phone or camcorder is detected, the system captures the image and sends it to the theater owner or other authorized individuals through a mail service. This allows them to take prompt action and prevent any piracy occurrences from happening. To achieve accurate detection and localization, the system uses a pre-trained deep learning model that is fine-tuned to recognize and localize mobile phones and camcorders. The model outputs the location of each detected object as a set of coordinates and draws bounding boxes around them in the video feed. Overall, the proposed system provides a robust solution for preventing piracy in a theater environment, allowing theater owners and other authorized individuals to take immediate action and ensure that the rights of content owners are protected.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 5, May 2023

DOI: 10.17148/IARJSET.2023.10523

Fig.4 shows the confusion matrix obtained after using the Yolov5 model on the acquired database. The precision (P) curve and recall (R) curve of the custom model generated through Yolov5 are depicted in Fig.5 and Fig.6. Based on the confusion matrix, it can be observed that the true positive rate (TPR) of the machine learning model is relatively high. This suggests that the model is capable of accurately detecting positive instances and minimizing the number of false negatives. Overall, the results indicate that the custom Yolov5 model is a promising approach for object detection tasks.

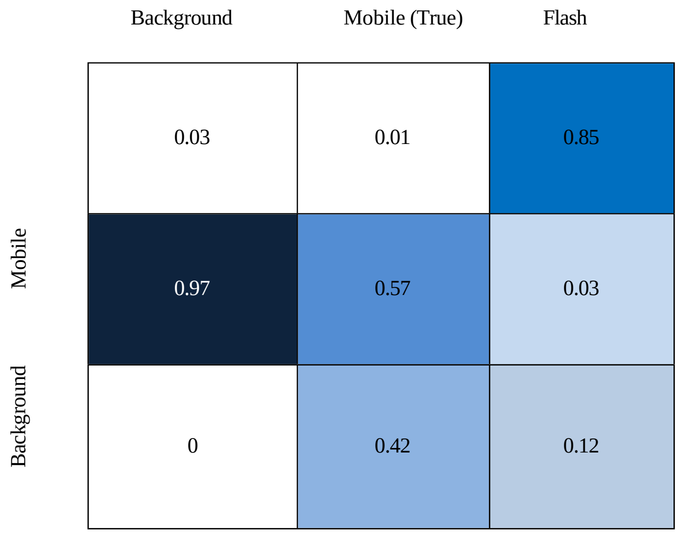

Fig.4 Confusion matrix

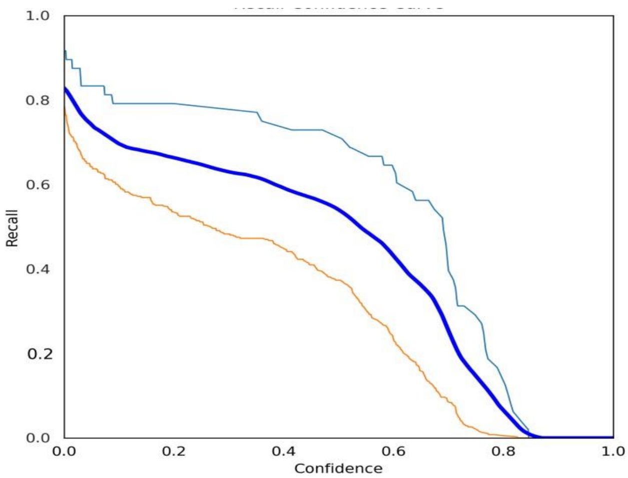

Fig.5 Recall-confidence curve

The YOLOv5 model that was specifically created has a strong recall performance, as evidenced by its R curve. The R curve reaches a value of 0.83 at the threshold value of 0.00, showing that the model can successfully recognize objects in a variety of settings. The ability of the model to identify most of the pertinent objects in the data set is indicated by a high recall rate, which is a desired quality in many applications. Overall, the model's strong performance on the R curve indicates that it has the potential to be a trustworthy tool for object detection tasks.

The model's P curve reaches a value of 1.0 at 0.876 as shown in Fig.6. This number reflects how accurately the model can detect things. The high precision score indicates that the model's identification is precise. As a result, the model's ability to detect objects can be regarded as dependable. The trade-off between recall and precision in a machine learning model is represented by the PR curve. The YOLOv5 model that was specifically created in this instance has an average precision of 0.625mAP at 0.5. This number shows that the model can successfully strike a decent balance between recall and precision when identifying items. Overall, the model is operating well and is appropriate for its intended purpose, according to the high average precision value.

DOI: 10.17148/IARJSET.2023.10523

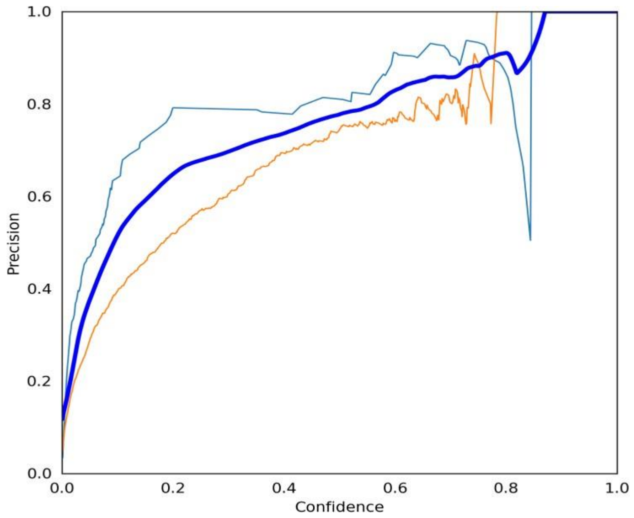

Fig.6 Precision-confidence curve

The harmonic mean of precision and recall is used to create the F1 curve, a metric for model performance. The specialized YOLOv5 model attained an F1 score of 0.66, indicating high overall performance, at a threshold of 0.241 as shown in Fig.7. This shows that the model is capable of successfully balancing recall and precision, two crucial criteria in object detection. Overall, the F1 curve offers a helpful statistic for assessing how well the unique YOLOv5 model performs object detection from IP camera streams.

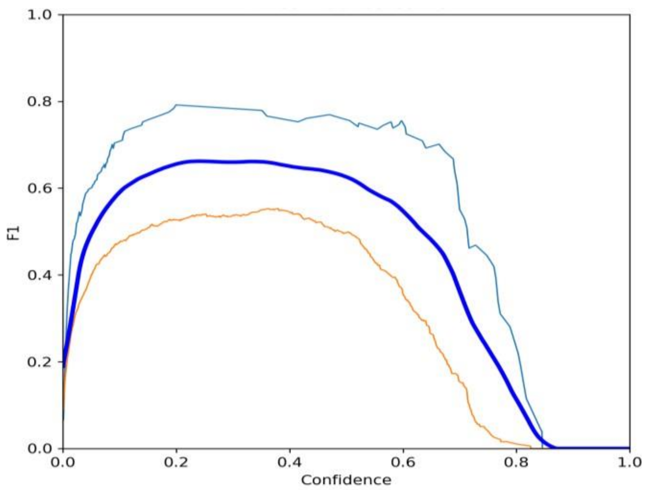

Fig.7 F1-Confidence curve

A dataset of 634 photos is used for yolov5 model's training, which was done using these images. Additionally, used 13 photos to test the model and 53 photographs for the validation procedure. Using the Roboflow website, we produced photos under various circumstances to strengthen our model. These circumstances included scaling the photographs by stretching them to a resolution of 1280x720, blurring the images up to 0.5 pixels, flipping the images horizontally, and varying the brightness of the images between -15% and +15%.

The trained model can recognize things in a few situations, enhancing its accuracy and performance, by using a wide array of photos with various changes. For object detection models to be successfully trained and for the model to be able to generalize well to new, unknown data, a large and diverse data set must be used. A specially created yolov5 model, which was created to recognize

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified ⪤ Impact Factor 8.066 ⪤ Peer-reviewed / Refereed journal ⪤ Vol. 10, Issue 5, May 2023
DOI: 10.17148/IARJSET.2023.10523

objects accurately and reliably in the input photos, was used for training and testing.
A custom yolov5 model has been developed specifically for mobile detection with an accuracy rate of 60%. The model has been incorporated into an algorithm designed to detect objects from IP camera feeds as shown in Fig. 8 and Fig.9. This algorithm has been programmed to trigger an alert message to the owner in case of piracy in a theater. The custom model has the capability to identify the exact location of the piracy activity. By using this system, the entertainment industry can ensure better security.
The system is automated and can function 24/7, providing real-time monitoring and alerting of the situation by sending mails to owner of theater as shown in Fig. 10. As a result, piracy can be effectively prevented by this model and algorithm.

Fig.8 Detected mobile phones

Fig.9 Detected mobile phones and flashes

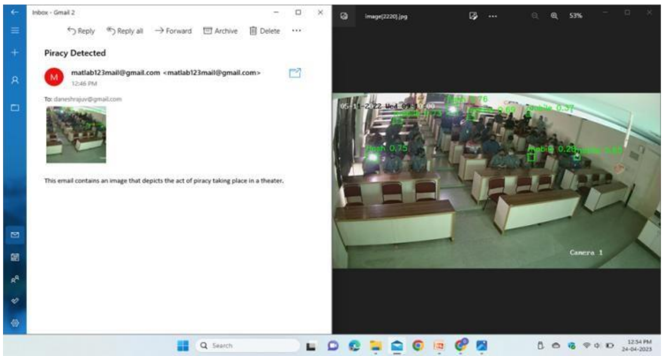

Fig.10 Image of alert message sent through mail

. The system has the following advantages:

- Used to protect the movie from being recorded illegally in theatres, which results in losses for the film industry.
- Curbs criminal acts on the mobile phone network
- Research on target recognition and tracking in mobile augmented reality-assisted maintenance.

VI. CONCLUSION

DOI: 10.17148/IARJSET.2023.10523

The piracy of movies in theatres has been a major issue in recent years. To combat this issue, an innovative system that employs IP cameras and deep learning is proposed to detect instances of piracy in real-time and inform the relevant parties. The solution uses a specialized object detection model trained with a set of images of the item to be detected, particularly mobile phones, which are associated with piracy. The mobile phones that are used for the movie recordings are being captured by the camera and are detected in real time with great accuracy using the proposed model. However, the whole theatre may not be covered. In the future, the model can be enhanced by installing a network of cameras and increasing the number of images in the dataset.

REFERENCES

[1] Sudler, Hasshi. "Effectiveness of anti-piracy technology: Finding appropriate solutions for evolving online piracy." Business Horizons, vol. 56, no. 2, pp. 149-157. 2015.

[2] Choi, Seul-Ki, and Jin Kwak. "Feature analysis and detection techniques for piracy sites." KSII Transactions on Internet and Information Systems (TIIS), vol. 14, no. 5, pp. 2204- 2220. 2020.

Naumovich, Gleb, and Nasir Memon. "Preventing piracy, reverse engineering, and tampering." Computer, vol. 36, no. 7,pp. 64-71. 2003.

[3] Fang, Yikai, Kongqiao Wang, Jian Cheng, and Hanqing Lu. "A real- time hand gesture recognition method." In 2007 IEEE International Conference on Multimedia and Expo, pp. 995-998. IEEE, 2007.

[4] Y. Zhao, W. Wang and Y. Wang, "A real-time hand gesture recognition method," 2011 International Conference on Electronics, Communications and Control (ICECC), Ningbo, China, pp. 2475- 2478. 2011.

[5] Wagner, Daniel, Gerhard Reitmayr, Alessandro Mulloni, Tom Drummond, and Dieter Schmalstieg. "Real-time detection and tracking for augmented reality on mobile phones." IEEE transactions on visualization and computer graphics, vol. 16, no. 3, pp. 355-368. 2009.

[6] Garg, Pragati, Naveen Aggarwal, and Sanjeev Sofat. "Vision based hand gesture recognition." International Journal of Computer and Information Engineering, vol. 3, no. 1, pp. 186-191. 2009.

[7] T. Kong, F. Sun, H. Liu, Y. Jiang, L. Li and J. Shi, "FoveaBox: Beyound Anchor-Based Object Detection," in IEEE Transactions on Image Processing, vol. 29, pp. 7389-7398, doi:10.1109/TIP.2020.3002345. 2020.

[8] Kim, Eui-Jin, and Jin Kwak. "Intelligent piracy site detection technique with high accuracy." KSII Transactions on Internet and Information Systems (TIIS), vol. 15, no. 1, pp. 285-301. 2021.

[9] Pulungan, Ali Basrah, Zhafranul Nafis, and Muhammad Anwar. "Object Detection with A Webcam Using the Python Programming Language." Journal of Applied Engineering and Technological Science (JAETS), vol. 2, no. 2, pp. 103-111. 2021.