SciEn
Journal of Engineering Advancements Vol. 05(04) 2024, pp 123-131 https://doi.org/10.38032/jea.2024.04.004

An IoT enabled Artifact Protection System for Museum using Computer Vision

Abu Salman Shaikat[1], Molla Rashied Hussein[2], Rumana Tasnim[3], Md Zonayed[3], Sayma Sultana Jhora[4], Md Mizanur Rahman[3], Anwar Hossain Mokhter[3]*

[1]Bharti School of Engineering and Computer Science, Laurentian University, Canada
[2]Department of Computer Science & Engineering, University of Asia Pacific, Bangladesh
[3]Department of Mechatronics Engineering, World University of Bangladesh, Bangladesh
[4]Faculty of Science & Engineering, Anglia Ruskin University, United Kingdom

Received: September 01, 2024, Revised: November 11, 2024, Accepted: December 16, 2024, Available Online: December 31, 2024

ABSTRACT

Currently, museums lack preventive security measures, leading to the theft of precious artifacts. Safeguarding artifacts and any sacred items in museums is a challenging job, as they need to be secured while at the same time being accessible to all visitors. This calls for an integrated security system to prevent theft and decrease crimes involving artifacts. This paper proposes a novel IoT-enabled, computer vision-based, holistic approach for protecting artifacts in museums. A camera functions as the imaging device that is employed to detect the movement of any artifact from a predetermined position, while the Raspberry Pi 4B manages the processing and operations of the system. This system further utilizes an image processing technique, i.e., the Haar Cascade algorithm and OpenCV, to detect artifact movement. In addition, the device will also record the photos of any authorized or unauthorized individuals anytime it detects any movement of the artifact. The system has produced a high accuracy of 93.33% and high precision of 96.29%, indicating a higher level of reliability with very few false alarms. This method will serve as an efficient mechanism for protecting artifacts at a reduced cost. The proposed system can be implemented at any kind of museum or cultural site.

Keywords: Artifact Protection, Computer Vision, Haar Cascade, OpenCV, Image processing, IoT, Raspberry Pi

1 Introduction

In recent times, a growing interest has been observed in protecting the artifacts and cultural heritage at museums. Generally, museums are required to ensure the protection of cultural heritage and artifacts. Artifacts are objects shaped by humans that have historical, archaeological, or cultural value and include metal objects, pottery, weapons, wooden objects, tools, elements of personal ornamentation, etc. Because museums have variegated characteristics, it is crucial to design an appropriate system for artifacts that guarantees enough protection at reduced costs. Museums should possess robust security measures to safeguard artifacts and to identify any unauthorized individuals, as well as to monitor and regulate access. Many museums in Southeast Asian countries implement security measures that rely on manual methods, including the use of classic keys and locks, as well as the use of closed-circuit cameras. However, the system requires individuals to sit in front of monitors and ensure continuous observation. If the individual in charge fails to detect any instances of theft, a certain priceless antique can be stolen. Furthermore, the clandestine character of these crimes is another significant aspect, as they are often unreported occurrences within museums, taking into account the potential damage to the museums' reputation. The predominant technology employed in museums is the burglar alarm. This approach has been implemented in numerous museums as a means to decrease the occurrence of criminal incidents such as theft. A typical security system is illustrated below in Fig. 1.

To enhance safety measures and reduce gaps in security due to human error and other errors, researchers should come up with a smart security and protection system. A number of researchers looked at the most important security criteria for building the framework for artifacts' most important security needs [1]-[2]. In general, the security of museum objects can be divided into two categories: internal decay over time and exterior risks of theft, both of which demand considerable care. Most research lacks a suifig security mechanism to protect artifacts, thereby requiring the implementation of a systematic method. Computer vision is a rapidly growing discipline that focuses on analyzing, modifying, and understanding images [3]. Security systems often use it as an effective solution. OpenCV is a computer vision image processing toolkit that includes a library for Haar Cascade [4]. The objective of this work is to create an efficient system for protecting artifacts utilizing the Haar-Ada Boost and Cascade algorithms in the context of the Internet of Things (IoT). This system operates using the Raspberry Pi 4B and a Wi-Fi module. The Wi-Fi module establishes a connection to the cloud in order to transmit notifications to a security service PC. OpenCV is utilized for image processing, and a smart alarm is triggered in response to the movements of the artifacts.

The proposed system uses IoT, Raspberry Pi 4B, and computer vision for real-time identification and protection, introducing significant improvements in the surveillance and preservation of cultural heritage. The Raspberry Pi 4B is an affordable, small, and powerful platform with low power consumption compared to larger computers, making this approach feasible for a wide range of museums, including those with limited budgets. The Raspberry Pi is easy to set up & can be quickly deployed in most museums without complex installations. The use of open-sourced software, as demonstrated by the Haar Cascade algorithm, along with low-cost sensors, significantly enhances the economy, making such technologies within the reach of museums. The Haar Cascade technique is an

*Corresponding Author Email Address: rumana@mte.wub.edu.bd Published by: SciEn Publishing Group

efficient, real-time object detection method that enables continuous surveillance of artifacts using pre-trained models. It involves the detection of objects to improve the responses in the time of unauthorized access. Moreover, IoT-enabled devices allow for real-time monitoring of artifacts, including the tracking of their movement and any potential hazards. IoT devices can detect when an artifact is being moved or manipulated, triggering notifications immediately to security personnel. This ensures the prompt detection of any unauthorized activity, which is recognized immediately, thus enabling the proper response to prevent damage or theft in a timely manner.

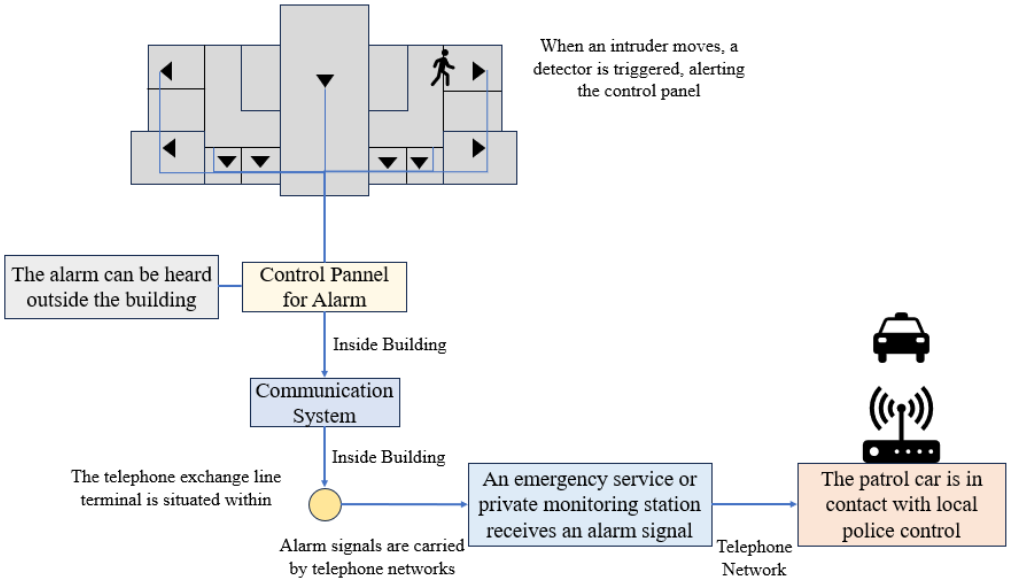

Fig. 1 A typical Burglar Alarm System

2 Related Works

A thorough study of the literature suggests various methods for artifact protection systems. Researchers have previously developed a microcontroller-based laser and motion sensor-based security system, which users can turn ON or OFF using a preset password [5]. With the right password, anyone can gain access to the room containing the artifacts. Having no password control over the alarm and sensors, they would start ringing whenever the sensors sensed any intrusion, and the respective alarm would not be stopped unless the system was reset. However, the password-based system may be vulnerable to forced attacks or interception if poorly encrypted. Occasionally, harmless stimuli may trigger the motion sensors, or they may fail to detect a genuine intrusion.

Some researchers came up with a microwave security system that can find valuable targets and confirm that they are in the places they were supposed to be [6]. Ambient variables and obstacles, like walls or furniture, may affect microwaves and thus create false positives or missed detections. Also, it might not be possible to find out exactly where a target is or how it is moving because of problems with microwave technology, such as low resolution and the chance of interference from other signals. In addition, modern security applications like home security and video surveillance have found outstanding success with facial recognition technology that utilizes digital image or video processing techniques [7].

In recent times, the Internet of Things (IoT), a common and well-known term, has unified all devices and systems inside a unified communication framework, granting us the ability to remotely manage and manipulate any object or process [8]-[11]. Researchers are utilizing advanced data analytics techniques to gather and analyze data from connected devices. Global researchers have projected that the number of interconnected Internet of Things (IoT) devices would reach approximately 100 billion by the end of 2025, with an estimated economic impact of around $11 trillion [12]. Over the past decade, IoT-based museum security systems have been gaining popularity among researchers [13]-[14]. IoT-based anti-theft technology from Museum Cultural Relics suggests an anti-theft program that uses passive RFID readers and writers to determine whether cultural artifacts are inside the safe range. The system is free from the disadvantages of the conventional infrared anti-theft, door magnetic detection, and similar techniques [15]. In recent times, museums have been employing IoT-based architectures to observe their environment and ensure the security of their artifacts. The detailed information is processed, gathered, and transferred to a gateway for storage in the cloud and taking suitable decisions [16]-[17]. Some researchers integrated IoT and RFID to enable an anti-theft technique for checking whether the artifacts are within a safe distance or not. The alarm will sound if the stolen items move far from the RFID identification range. However, for the entire museum, much more equipment will be required, which will ultimately lead to much more energy and power consumption [18]. A gallery anti-stealing device was created using the internet-of-things (IoT) technology that ensures security through passive readers/writers of RFID [19]. Additionally, researchers have developed anti-theft systems that exclusively use RFID [20]. Researchers addressed the applications, advantages, and limitations of RFID technology for maintaining security in Turkish museums [21]. Some researchers used fiber optic sensors to keep an eye on the fiber optic link to keep it safe from people who shouldn't have access to the information and to protect museum artifacts and important infrastructure [22]. Some other researchers also used optical sensors for protecting property like artwork, using a small video camera along with a video processing unit. When the sensor detects any movement in the artwork, it sends a warning signal to any nearby device [23]. However, optical sensors may have

low performance in poor lighting conditions or when there is some obstruction of view. Another work used an IoT-based network of interconnected devices to share real-time data over the internet and Raspberry Pi to detect power theft and transmit a command to a GSM module, which then sends a message to the Electricity Board (EB) with the theft details [24]. In recent times, the domains of computer vision and machine learning have made use of deep learning techniques [25]-[26]. Machine learning (ML) is a domain of artificial intelligence (AI) that emphasizes the development of algorithms and statistical models that allow computers to execute tasks autonomously [27]-[28]. Researchers are applying deep learning-based machine learning techniques to detect archaeological objects [29]. Researchers have proposed a machine learning framework named ARTYCUL, which uses CCTV cameras to display footfall around artifacts in museums. The framework uses video streams to detect human figures and visualizes visitor density around specific items [30]. Another approach used a Haar-cascade classifier, a machine learning algorithm, which was used to build four distinct classes for safety equipment recognition in order to create a safety warning system [31]. Some researchers applied computer vision-based methods for the detection, security, and preservation of priceless items [32]-[33]. A study has been conducted that employed the Local Binary Pattern Histogram and Haar Cascade technique for face detection using the OpenCV library. The findings showed promising outcomes for the application of car theft prevention [34].

It is evident that, the recent works lack of thorough research on artifact protection mechanisms. Given the constraints and lack of research, more work is clearly required to safeguard artifacts in museums. The purpose of this paper is to show how an IoT-enabled Raspberry Pi 4B can be used with the Haar Cascade algorithm to create a computer vision-based artifact detection method. This algorithm can be run in a real-time scenario. The proposed system is a robust, secure, and cost-effective technique that eliminates the need for extra components.

3 Proposed model

Fig. 2 illustrates a block diagram of the Haar-Ada Boost and Cascade algorithm-based artifact detection system.

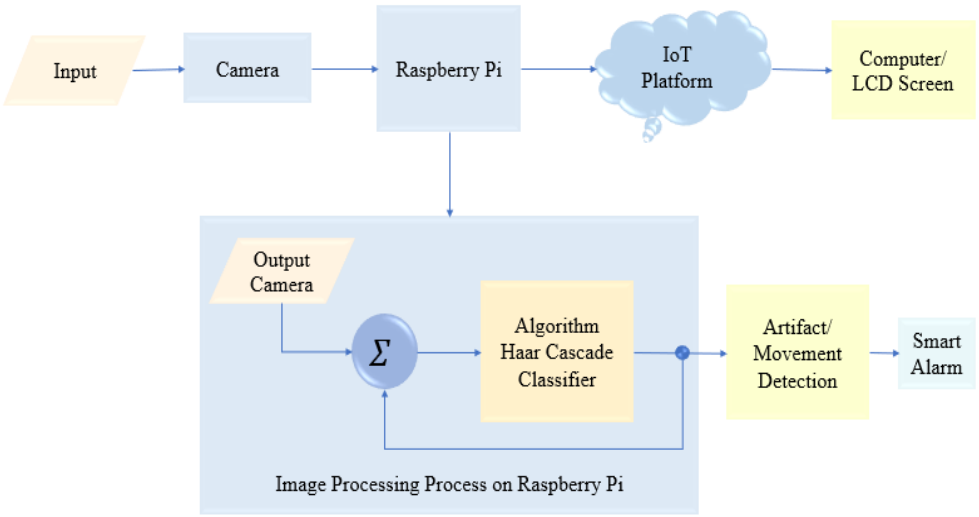

Fig. 2 Block Diagram of IoT enabled Computer Vision Based Artifact Protection System

The system consists of several components, such as a Raspberry Pi, a camera, a security system PC, and a smart alarm. The camera serves as the imaging device, while the Raspberry Pi acts as the microcontroller and image processing platform that handles the processing and operation of the system. Firstly, an image is captured using the camera and processed by the Raspberry Pi. Using the Haar Classifier Cascade, the image data is analyzed to detect any movement of the artifacts. Upon detecting even the slightest movement, the smart alarm is activated. Additionally, the system can capture and process images of both authorized and unauthorized persons. The processed image data will be sent as an alert to the server, along with movement detection information. This is facilitated by the IoT platform, which delivers these alerts from the server and displays them on the security system's PC.

The Raspberry Pi serves as the primary computing device that runs the computer vision algorithms. These algorithms are responsible for processing the image fed from cameras monitoring the artifacts. Via WiFi, the Raspberry Pi is linked to CCTV cameras that capture real-time images of the museum's artifacts. It uses computer vision models that have been trained to analyze these image feeds in order to identify any unauthorized access or questionable activity near the artifacts. By interacting with devices inside the museum, it serves as an IoT gateway. The hardware specification is detailed in the following Table 1.

Table 1 Hardware Specification

Equipment List	Specification
Raspberry Pi	4B model RAM: 4GB
CCTV Camera	1000TVL HD

Haar Cascade Training & Testing Diagram are shown in Fig. 3. In the proposed system, computer vision is applied using OpenCV, and the Haar cascade method is specifically used for artifact detection. OpenCV is a robust and freely accessible computer vision framework that offers a wide range of capabilities for processing images and video. The Haar cascade method is an object detection method in images, regardless of their scale and position. The Haar-like features are basic rectangles that are computed by comparing the average intensities of nearby areas in a picture. To swiftly calculate the total of pixel values in rectangular areas, integral images are utilized. By dividing the total of two regions by each other, Haar-

like features can be quickly computed. Due to the use of integral images, they can compute Haar-like features comparatively quickly while also being successful at spotting objects with different attributes, as shown in Fig. 4. The process begins with the camera acquiring images, which are used as both training samples for the classifier and test samples. Gathering this collection of images is the first step in the Haar cascade approach. Images with labeled items of interest are used as training samples. A large number of both object-containing and non-object-containing images are required to train a Haar cascade classifier. To create an effective Haar Cascade Classifier, images must be carefully prepared. Preparing the training data involves collecting positive and negative samples. In the image segmentation part, the process involves three main steps: image preprocessing, main image segmentation, and segmental image preprocessing. The training process involves two primary elements: the training stage and the detection stage.

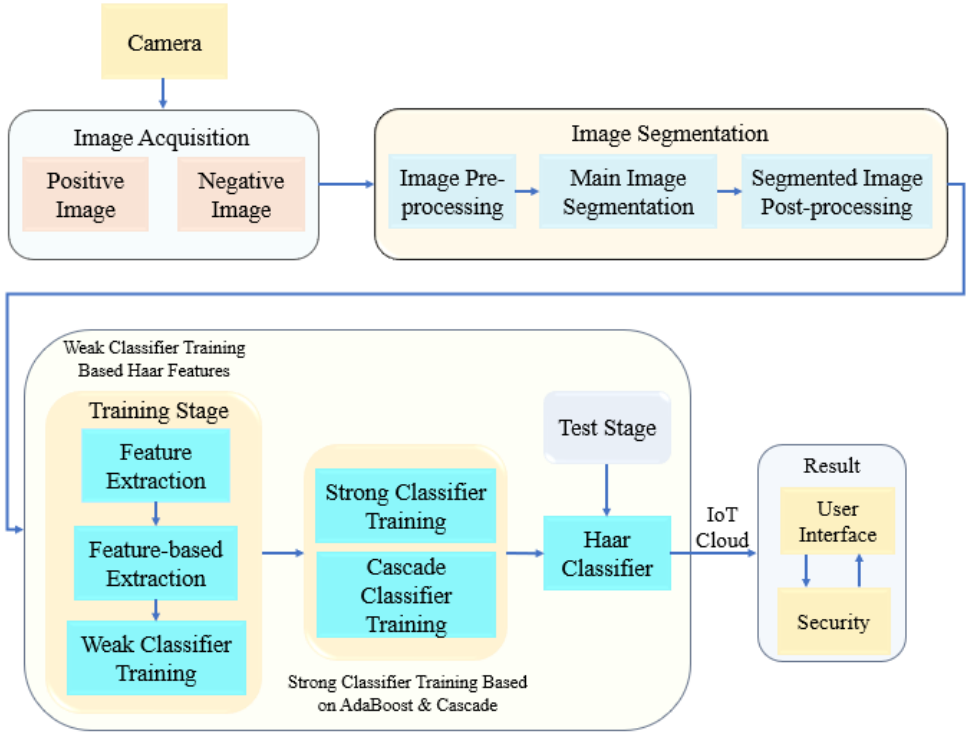

Fig. 3 Haar Cascade Training & Test Diagram

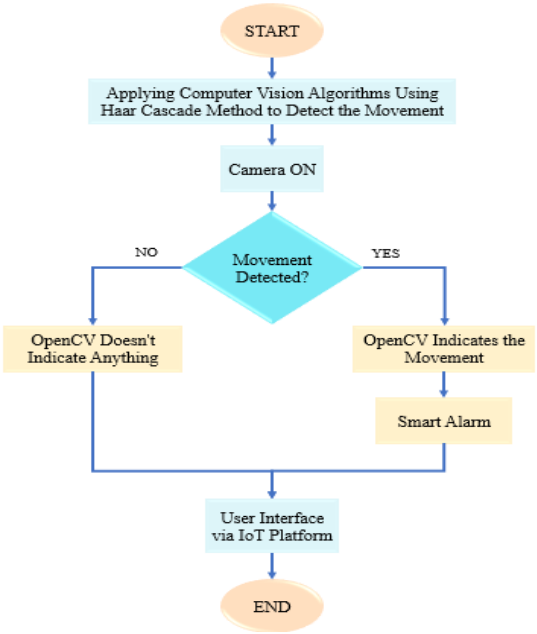

Fig. 4 Flow Chart of Computer Vision based Artifact Detection System

1. Training: In the training stage, a huge number of picture patches, containing both positive and negative images, are generated throughout the sampling phase in order to train the classifier. The object of interest is typically contained in the cropped windows of the positive photos, which are known as positive samples. They are taken out at different sizes and locations. To train the classifier, instances of the object in various sizes and locations must be shown within the image. By definition, a negative sample is a window taken from an image that does not actually contain the object. Typically, huge negative picture data sets are used to randomly choose the negative samples. Due to the variety of these examples, the classifier can figure out which features aren't relevant to the item. The method selects the finest Haar-like features and determines the best threshold values to distinguish between positive and negative samples. During this process, the AdaBoost algorithm is employed to enhance weak classifiers into strong classifiers. By prioritizing samples that are more difficult to identify and adjusting the weights of features, the AdaBoost algorithm also improves the classifiers' performance. These strong classifiers are then used to train a cascade classifier.

2. Detection: Applying the trained cascade classifier can be used on the test images to identify objects in new images once it has been trained. An image is scanned during the detection process using a sliding window with different widths and

positions. The classifier assesses whether the object of interest is present at each window position based on the Haar-like properties that were computed there. The classifier moves to the following scale or location to further enhance the detection if it recognizes a probable object. The software specification is detailed in the following Table 2.

Table 2 Software Specification

Equipment	Specification
Python	Version: 3.10
PyCharm IDE	Version: 2020.2
OpenCV	Cv lib. Version: 4.5.4
Haar-Cascade	Algorithm

The following Fig. 4 illustrates the flow chart of a computer vision-based artifact protection system. Initially, the system starts. Then, computer vision is applied using OpenCV. After that, the Haar Cascade algorithm is applied, and the camera starts to capture images. When the artifact does not move from its location, OpenCV doesn't indicate anything. However, as soon as someone tries to move the artifact from its predetermined position, OpenCV detects the position of the artifact's movement, and the alarm buzzes simultaneously.

The size of the target artifact in the proposed system for museums often depends on the specific type of artifact being safeguarded. The optimal artifact size for the IoT-based artifact security system is contingent upon the particular museum environment and the types of artifacts involved. The utilization of forceps or tweezers can provide difficulties for detection systems. To tackle these issues, the system requires improved camera configurations, sensor integration, and advanced algorithms for guaranteeing its efficacy in handling such situations.

Hardware setups of the proposed artifact protection mechanism are illustrated in the Fig. 5 and Fig. 6 where a PC with a camera is used. Hare, a web camera has been used specifically for testing purposes. Fig. 5 illustrates an image that shows artifact has not been moved whereas Fig. 6 illustrates an image that shows the movement of artifact.

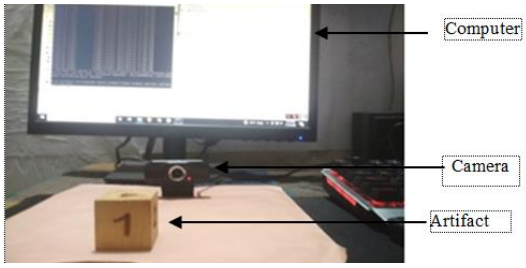

Fig. 5 Hardware Setup of Computer Vision based Artefact Protection System (Artifact not moving)

Fig. 6 Hardware Setup of Computer Vision based Artefact Protection System (Artifact moving)

4 Results and discussions

The computer vision-based artifact protection system is designed specifically for museum use. The Haar cascade method is applied for detecting any movement of objects in an image. This Haar cascade method is a machine-based learning method where large numbers of images are used to train the classifier. The Haar cascade classifiers are regarded as a proficient way to ensure object detection with OpenCV.

In this work, when the artifact is safely located in a museum and not being moved, OpenCV does not specify anything. The protected state of an artifact is represented in Fig. 7.

Fig. 8 represents the OpenCV window when anyone tries to move the artifact from its location. Any movement of artifact from its location will cause the buzzer to go off and send alert notifications to the computer. And Fig. 9 further represents the location of the drive, where all the captured images are located.

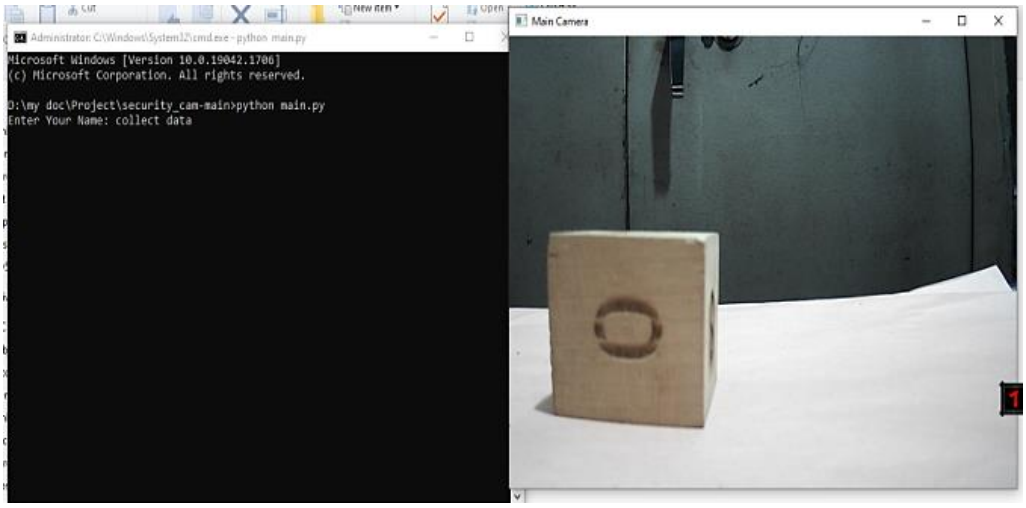

Fig. 7 OpenCV Window When Artifact is Safely Positioned

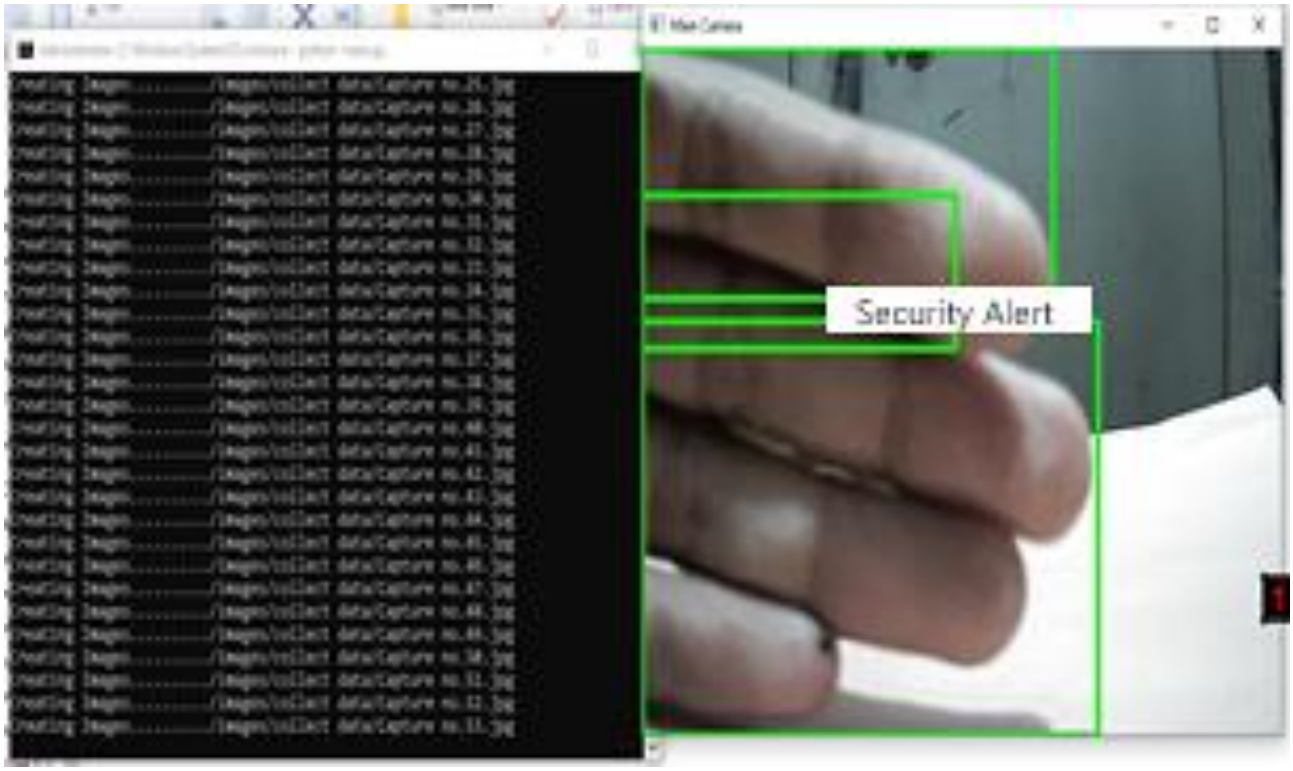

Fig. 8 OpenCV Window When Artifact is moved

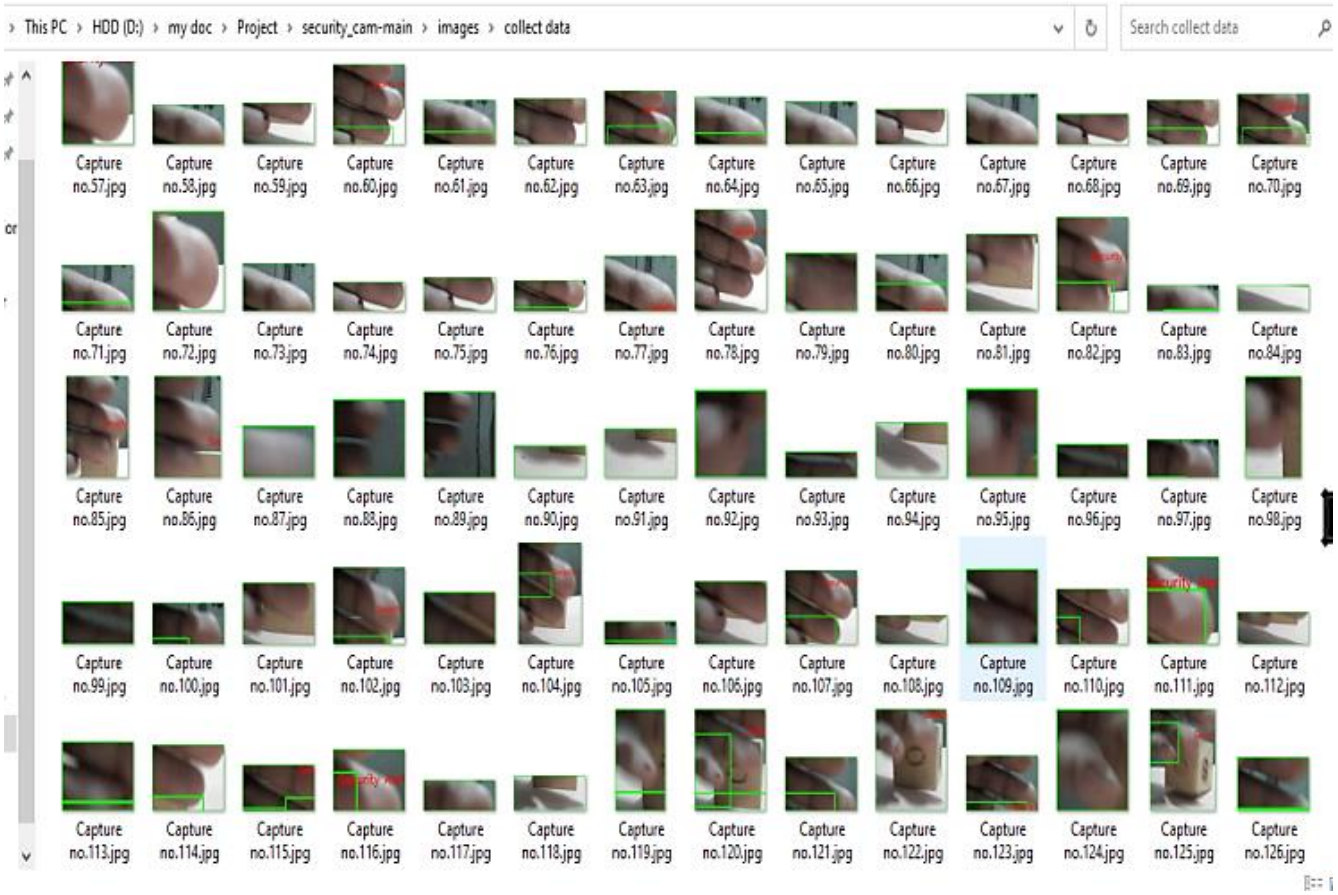

Fig. 9 Captured Images from OpenCV Window

The artifact (object) movement was tested for 30 times as a part of experimentation. In the captured image, the OpenCV window can be viewed for different scenarios due to movement of artifacts. Table 3 presents an evaluation table to assess accuracy by providing True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN) data. Detection results are categorized into successful cases (S) and failure cases (F).

Table 3 Evaluation Table

No of Trials	True Positives (TP)	False Positives (FP)	True Negatives (TN)	False Negatives (FN)	Detection Results	Reason of Failure
1	1	0	0	0	S	
2	1	0	0	0	S	
3	1	0	0	0	S	
4	1	0	0	0	S	
5	1	0	0	0	S	
6	1	0	0	0	S	
7	1	0	0	0	S	
8	1	0	0	0	S	
9	1	0	0	0	S	
10	1	0	0	0	S	
11	1	0	0	0	S	
12	1	0	0	0	S	
13	1	0	0	0	S	
14	1	0	0	0	S	
15	1	0	0	0	S	
16	0	0	1	0	S	
17	1	0	0	0	S	
18	1	0	0	0	S	
19	1	0	0	0	S	
20	1	0	0	0	S	
21	0	0	0	1	F	False Negative
22	1	0	0	0	S	
23	1	0	0	0	S	
24	1	0	0	0	S	
25	0	1	0	0	F	False Positive
26	1	0	0	0	S	
27	1	0	0	0	S	
28	1	0	0	0	S	
29	0	0	1	0	S	
30	1	0	0	0	S	

The accuracy is calculated as follows.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} * 100\%$$

$$= \frac{26+2}{26+2+1+1} * 100\% = 93.33\%$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} * 100\%$$

$$= \frac{26}{26+1} * 100\% = 96.29\%$$

Based on the experimental evidence, it is apparent that the Haar Cascade method was effectively implemented for artifact movement and detection. Moreover, the image of any random person moving the object can be easily extracted from the OpenCV window, as it captures the real-time images instantly. Any authorized or unauthorized person's image moving the object can also be extracted for analysis. The Haar cascade approach demonstrates a commendable level of reliability in detecting movement in this environment, as evidenced by its detection accuracy of 93.33% and precision of 96.29%. The system accurately detected the artifact in 26 trials, as indicated by the true positive results. This demonstrates the efficacy of the Haar cascade method in accurately identifying the artifact when it was indeed present. There was one occurrence in which the system provided a misleading indication of a false alarm, namely false positive data. This implies that the Haar cascade classifier mistakenly identified another object or background noise as the artifact. In addition, the system accurately detected the lack of an artifact in 2 trials. The system accurately determined that there was no artifact present in these circumstances. Furthermore, the algorithm exhibited a failure to detect the artifact in one experiment despite its actual presence. This indicates that the system failed to detect the artifact on one occasion, resulting in false negative data. Examining these examples could yield valuable insights into the environment or factors that impact detection accuracy and precision.

The IoT-enabled, computer vision-based system for artifact security in museums using the Haar Cascade algorithm and OpenCV is a relatively new methodology. However, it has certain limitations. Computer vision approaches, like the Haar Cascade, rely on favorable light conditions for accurate object detection to a great extent. Lighting conditions in a museum vary throughout the day, and even minor changes in light may have a serious impact on the quality of captured images or videos. In low-light conditions it might result in false negatives. Incorporating supplementary sensors can enhance the system's performance under diverse lighting situations. Further, exhibits in museums are more often behind the glass or with other things that may obstruct the visibility of the camera. Some obstructions may block the camera's view from entirely capturing the artifact, making motion detection incomplete or incorrect. This can affect the ability of the system to deliver its effective performance in unauthorized movements or interference with the artifacts. Advanced computer vision methods can enhance accuracy amidst obstacles. In addition, this technology can take pictures or records of fake objects. An attacker may replace the artifact with a replica or forged version of the object. This method may be incapable of distinguishing between the authentic and forged artifacts. When a replica is presented to the museum, the technology will falsely identify unauthorized people accessing it. In this case, an additional authentication method, like embedding sensors within the artifacts, can be added to increase the reliability of verification.

5 Conclusion

In this proposed work, the Haar-AdaBoost and Cascade algorithms-based system capable of ensuring the security of artifacts has been designed and developed. This system introduces a smart artifact protection system implying a Haar cascade algorithm where OpenCV windows can be effectively viewed, and it helps to get the exact output. The OpenCV safety features are also observed. The overall process for protecting artifacts has been monitored and archived in the system. Excel datasheets can store data for future purposes whenever there is any movement of the artifacts. For the applications in museums, this system is quite reliable, robust, and cost-effective compared to the other approaches for artifact protection in museums. The proposed artifact protection system has demonstrated itself to be a powerful tool to protect cultural, archaeological, and historical artifacts in any museum. This system is quite reliable and robust compared to the other approaches for artifact protection in museums. Its capacity to precisely identify and acknowledge persons, along with functionality such as data preservation and Excel data storage, enhances its effectiveness and makes it a

practical option for applications in museums. Future work entails incorporating improved object detection algorithms, such as those based on deep learning, to enhance the reliability of artifact detection and threat recognition. Furthermore, the system's scalability will be evaluated for its ability to handle larger and diverse artifact collections at several museum locations. An additional multilevel monitoring system will be developed to categorize artifacts according to their nature, worth, and placement. Specifically, a distinct monitoring area for various portions, as well as a central monitoring dashboard, can be set up that will give an overview of the entire museum. The dashboard will display real-time status updates for each monitoring area, particularly for sections with a higher number of artifacts, which will also ensure that the system remains versatile and effective in a variety of situations.

References

[1] Naqvi, S.A.A., 2016. Museum security. In Proc. Seminar Museum Secur (pp. 84-89).

[2] Moffett, J.D., Haley, C.B. and Nuseibeh, B., 2004. Core security requirements artefacts.

[3] Shaikat, A.S., Hussein, M.R., Tasnim, R., Farhan, A., Khan, A.M.S., Mokhtar, A.H. and Rahman, M.M., Computer Vision Based Automated Attendance System Using Face Recognition.

[4] Mistry, K. and Saluja, A., 2016. An introduction to opencv using python with ubuntu. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 1(2), pp.65-68.

[5] Muhtadi, T., Amin, N. and Tabassum, M., 2012. Museum security system (Doctoral dissertation, BRAC University).

[6] Elsheakh, D. and Elsadek, H., 2014, July. Microwave security system in museums (design and implementation). In 2014 IEEE Antennas and Propagation Society International Symposium (APSURSI) (pp. 1835-1836). IEEE.

[7] Asaduzzaman, A., Mummidi, A., Mridha, M.F. and Sibai, F.N., 2015, December. Improving facial recognition accuracy by applying liveness monitoring technique. In 2015 International Conference on Advances in Electrical Engineering (ICAEE) (pp. 133-136). IEEE.

[8] Saleheen, R.U., Farhan, A., Ramesha, N.Z., Tasnim, R., Erin, M.T.U.R. and Shahria, S., 2024. Emerging Applications of Mechatronics. In Mechatronics: Fundamentals and Applications (pp. 143-160). Singapore: Springer Nature Singapore.

[9] Tasnim, R., Hussein, M.R., Hasan, M.K., Islam, S., Akhter, F. and Farhan, A., 2024. IOT Architecture and its Integration with Mechatronics. In Mechatronics: Fundamentals and Applications (pp. 101-124). Singapore: Springer Nature Singapore.

[10] Tasnim, R., Hussein, M.R., Farhan, A., Saleheen, R.S., Zonayed, M., Huq, E., Mahbub, F. and Rahman, M.M., 2023, December. IoT and GSM integrated automated water pump controlling system for prevention of water wastage. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Dhaka, Bangladesh: IEOM Society International.

[11] Tasnim, R., Shaikat, A.S., Al Amin, A., Hussein, M.R. and Rahman, M.M., 2022. Design of a Smart Biofloc Monitoring and Controlling System using IoT. Journal of Engineering Advancements, 3(04), pp.155-161.

[12] Mridha, M.F., Abdul Hamid, M. and Asaduzzaman, M., 2020. Issues of Internet of Things (IoT) and an intrusion detection system for IoT using machine learning paradigm. In Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2018 (pp. 395-406). Springer Singapore.

[13] Garzia, F. and Sant'Andrea, L., 2016, October. The Internet of Everything based integrated security system of the World War One Commemorative Museum of Fogliano Redipuglia in Italy. In 2016 IEEE International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.

[14] BV, P.C., Sreekar, G., Jatin, G. and Shah, J., 2021, December. Iot based environment monitoring system to protect heritage artefacts. In 2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT) (pp. 145-150). IEEE.

[15] Liu, Z., Wang, M., Qi, S. and Yang, C., 2019. Study on the anti-theft technology of museum cultural relics based on Internet of Things. IEEE Access, 7, pp.111387-111395.

[16] Alsuhly, G. and Khattab, A., 2018, August. An IoT monitoring and control platform for museum content conservation. In 2018 International Conference on Computer and Applications (ICCA) (pp. 196-201). IEEE.

[17] Maceli, M., 2020. Internet of things in the archives: novel tools for environmental monitoring of archival collections. Records Management Journal, 30(2), pp.201-220.

[18] Liu, Z., Wang, M., Qi, S. and Yang, C., 2019. Study on the anti-theft technology of museum cultural relics based on Internet of Things. IEEE Access, 7, pp.111387-111395.

[19] Gurumoorthy, S., Reddy, L.V. and Periakaruppan, S., 2022. Design and Development of an Internet of Things (IoT)-Based Anti-Theft System in Museum Cultural Relics Using RFID. In Handbook of Research on Advances in Data Analytics and Complex Communication Networks (pp. 168-180). IGI Global.

[20] Hamid, S.B.A., Rosli, A.D., Ismail, W. and Rosli, A.Z., 2012, November. Design and implementation of RFID-based anti-theft system. In 2012 IEEE International Conference on Control System, Computing and Engineering (pp. 452-457). IEEE.

[21] Çayırezmez, N.A., Aygün, H.M. and Boz, L., 2013, October. Suggestion of RFID technology for tracking museum objects in Turkey. In 2013 Digital Heritage International Congress (DigitalHeritage) (Vol. 2, pp. 315-318). IEEE.

[22] Zyczkowski, M., Karol, M., Markowski, P. and Napierala, M.S., 2014, October. Simple fiber optic sensor for applications in security systems. In Unmanned/Unattended Sensors and Sensor Networks X (Vol. 9248, pp. 31-39). SPIE.

[23] Murawski, K. and Murawska, M., 2017, September. Integrated optical sensor for individual protection of artwork. In 12th Conference on Integrated Optics:

Sensors, Sensing Structures, and Methods (Vol. 10455, pp. 36-39). SPIE.

[24] Meenal, R., Kuruvilla, K.M., Denny, A., Jose, R.V. and Roy, R., 2019, November. Power monitoring and theft detection system using IoT. In Journal of Physics: Conference Series (Vol. 1362, No. 1, p. 012027). IOP Publishing.

[25] Amzad Hossain, M., Suvo, I.A., Ray, A., Ariful Islam Malik, M. and Mridha, M.F., 2021. Number plate recognition system for vehicles using machine learning approach. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 2 (pp. 799-814). Springer Singapore.

[26] Tabassum, A., Hassan Ovi, S., Hossain, S., Tonmoy, M.R., Shovon, M.S.H., Hussein, M.R. and Mistry, D., 2024. Privacy Preserving Breast Cancer Prediction with Mammography Images Using Federated Learning. In Data-Driven Clinical Decision-Making Using Deep Learning in Imaging (pp. 227-245). Singapore: Springer Nature Singapore.

[27] Shams, A.B., Hoque Apu, E., Rahman, A., Sarker Raihan, M.M., Siddika, N., Preo, R.B., Hussein, M.R., Mostari, S. and Kabir, R., 2021, February. Web search engine misinformation notifier extension (SEMiNExt): A machine learning based approach during COVID-19 Pandemic. In Healthcare (Vol. 9, No. 2, p. 156). MDPI.

[28] Sutrodhor, N., Hussein, M.R., Mridha, M.F., Karmokar, P. and Nur, T., 2018. Mango leaf ailment detection using neural network ensemble and support vector machine. International Journal of Computer Applications, 181, pp.31-36.

[29] Fiorucci, M., Verschoof-Van Der Vaart, W.B., Soleni, P., Le Saux, B. and Traviglia, A., 2022. Deep learning for archaeological object detection on LiDAR: New evaluation measures and insights. Remote Sensing, 14(7), p.1694.

[30] Varma, G., Chauhan, R. and Yafi, E., 2021. ARTYCUL: a privacy-preserving ML-driven framework to determine the popularity of a cultural exhibit on display. Sensors, 21(4), p.1527.

[31] Phuc, L.T.H., Jeon, H., Truong, N.T.N. and Hak, J.J., 2019. Applying the Haar-cascade Algorithm for detecting safety equipment in safety management systems for multiple working environments. Electronics, 8(10), p.1079.

[32] J. Dorner., Š. Kozák, F. Dietze, “Object recognition by effective methods and means of computer vision”, 2015 International Conference on Process Control (PC), June 9–12, 2015, ŠtrbskéPleso, Slovakia.

[33] Suaib, N. M., Ismail, N. A. F., Sadimon, S., & Yunos, Z. M. (2020, November). Cultural heritage preservation efforts in Malaysia: A survey. In IOP Conference Series: Materials Science and Engineering (Vol. 979, No. 1, p. 012008). IOP Publishing.

[34] Abdurrahman, M. H., Darwito, H. A., & Saleh, A. (2020). Face recognition system for prevention of car theft with Haar cascade and local binary pattern histogram using Raspberry Pi. EMITTER International Journal of Engineering Technology, 8(2), 407-425.