*Journal of Information & Optimization Sciences*
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 7, pp. 2389-2400
DOI : 10.47974/JIOS-2132

# Artificial intelligence and machine learning approaches for secure image recognition in IoT networks

Kirti Rahul Kadam [†]
*Department of Management Studies*
*Institute of Management*
*Bharati Vidyapeeth (Deemed to be) University*
*Kolhapur 416003*
*Maharashtra*
*India*

Dankan Gowda V *
*Department of Electronics and Communication Engineering*
*BMS Institute of Technology and Management*
*Bangalore 560119*
*Karnataka*
*India*

Pritish Kakkar [§]
*Department of Computer Science*
*Sardar Beant Singh State University*
*Gurdaspur 143530*
*Punjab*
*India*

Debanjan Nag [‡]
*Department of Human Resources*
*Symbiosis Institute of Business Management*
*Hyderabad 509217*
*Telangana*
*India*

*and*

[†] *E-mail:* **kirti.kadam@bharatividyapeeth.edu**
* *E-mail:* **dankan.v@bmsit.in (Corresponding Author)**
[§] *E-mail:* **pritishkak11@gmail.com**
[‡] *E-mail:* **Debanjan.nag@sibmhyd.edu.in**

*Symbiosis International (Deemed University)*
*Pune 412115*
*Maharashtra*
*India*

Kaushika Pal [@]
*Department of Computer Applications*
*Sarvajanik College of Engineering and Technology*
*Surat 395001*
*Gujarat*
*India*

Ananda K. [#]
*Department of Computer Science and Engineering*
*BGS Institute of Technology*
*Adichunchanagiri University*
*Mandya 571448*
*Karnataka*
*India*

Erdal Buyukbicakci [$]
*Department of Computer Technologies*
*Information Technologies Vocational School*
*Sakarya University of Applied Sciences*
*Sakarya*
*Turkey*

**Abstract**

The extremely fast expansion of Internet-of-Things (IoT) networks has generated high security concerns, in particular for the integrity and privacy of image data. Private image recognition is essential to ensuring that image data captured by IoT devices (surveillance cameras, sensors, etc.) is reliable and secure by preventing unauthorized access or tampering of this data. In this paper, we propose a new methodology that uses the power of Artificial Intelligence (AI) and Machine Learning (ML) to improve security of image recognition systems in the IoT environment. Concretely, convolutional neural network (CNN), image encryption and adversarial machine learning are involved in the proposed image recognition strategy for security purpose, which can examine against image tampering and unauthorized access and so on. Experimental results show that the proposed method is capable of effectively recognizing image and ensuring data security and integrity, and

[@] *E-mail:* **kaushika.pal@scet.ac.in**
[#] *E-mail:* **anandkgowdru73@gmail.com**
[$] *E-mail:* **erdal@subu.edu.tr**

gains great superiority over those of other existing methods in security and recognition rate. The proposed framework provides a suitable solution to protect the image-based data within IoT platforms, and thus, to have more secure and reliable IoT platforms.

***Subject Classification (2010):*** *94A60, 20C05, 20C07.*

***Keywords:*** *Artificial intelligence, Machine learning, Secure image recognition, Internet of Things (IoT), Convolutional neural networks (CNNs), Image security, Adversarial machine learning, Data integrity, Image tampering.*

## 1. Introduction

IoT networks are having dramatic impacts on a variety of fields, such as smart home, health care, transportation, agriculture, and industrial automation[1]. These networks have changed the way that devices communicate and have made them more intelligent, efficient and better able to make decisions [2]. In smart homes, the IoT is used for automatic control of appliances, lighting, and security systems [3]. In industrial automation, IoT sensors improve production processes with real-time visibility of the status of machines and conditions [4]. However, as IoT networks grow so ass the security issues, especially given the volume of data being generated. One of the most important types of data in transmission include images [5], which have been created by security cameras, drones, and other visual sensors. Data in images is very important for many applications [6], such as camera sensors, monitoring and facial recognition [7]. Visual data is becoming increasingly relevant, and although IoT networks carry this information, they are exposed to security attacks, which can endanger the data integrity and confidentiality [8]. If unauthorized access is allowed or if images and data are tampered with, the impact is enormous, including privacy violations at least, and system failures at most, so secure image recognition plays an indispensable part in the security of IoT [9]. In this paper, we will present a new AI and ML solution in an IoT network, focusing on secure image recognition [10]. Using state-of-the-art AI/ML approaches, this paper aims at improving the accuracy of image recognition systems with a strong transparent security approach ensuring an image is not tampered with, does not get illegitimate access and data is not manipulated [11].

## 2. Literature Survey

The threat of image recognition has always played a significant role in computer vision, both traditional feature-based and pattern matching

approaches and AI/ ML streaming currently implemented ones. Early image processing and analysis systems are founded based on traditional computer vision algorithms such as edge detection [12], histogram analysis, and template matching [13]. These methods were however based on manual feature extractions and were light sensitive and scale and rotation sensitive [14]. Convolutional Neural Networks (CNNs), were methods that, with deep learning, leveraged accuracy and robustness of visual task recognition systems. CNNs are an automatic learner based on end-to-end learning architecture [15], and the process of feature extraction by the fully automated manner through the massive database is suitable to the tasks of object detection, face recognition, and classification of scenes [16]. Following the view of the Internet of Things (IoT), image recognition is a crucial element given that the Internet of Things is increasingly ubiquitous since cameras seem to be on smartphones, drones, and surveillance cameras allows them to manage their visual information continuously. The inclusion of image recognition on IoT applications can be implemented such as real-time monitoring, security surveillance or automated examinations [17]. Yet, such systems are limited as data processing capabilities and real-time data transfer, functioning in dynamically changing environments poses serious challenge. Further, heterogeneous devices in the IoT networks are used [18], and they have compatibility problems as well as has sensor quality and scalability problems, which obstruct efficiency and reliability of image recognition. A number of prior researches have explored the security of AI/ML based image recognition systems. For instance, some methods are based on the image encryption methodologies, in which the image data are encrypted during the communication among IoT devices. Another few works have adopted adversarial training, during the training phase, models are fed with adversarial examples to enhance the robustness. To overcome the said challenges, this paper aims to provide a complete system that integrates AI/ML based image recognition with secure operations of networks in IoT, thereby enabling both reliable and secure image recognition. In this paper we attempt to take care of the limitations mentioned above and serve for a more efficient as well as scalable solution to the problem of privacy and secure image recognition for IoT systems.

## 3. Proposed Method

Mechanism of safe image recognition in IoT collections, which incorporates further sophisticated AI/ML systems, and more intensive

safety programs or plans, in a bid to claim accuracy and integrity of data in pictures. It addresses important safety issues that can happen using IoT system, such as, unauthorized access, image tampering, and data tempering, and even excels in the area of identification. At the risks of the proposed approach lies the application of Convolutional Neural Networks (CNN) on image recognition along with the security services that will ensure privacy of all data throughout the recognition pipeline. The initial step is the images gathering of all types of IoT devices (e.g., cameras, drones, sensors) placed in different healthcare settings (e.g., smart homes, surveillance, industrial settings). These tools capture optical images that are late and portrayed into a central computer which is processed. The images are preset processed, where a process of noise removal, standardization and size shrinkage are taken. This operation is carried out to put the input images into a normal form to be recognized by the AI model in a way that is accurate and fast. The pipeline has some mechanisms to ensure security of image data. Firstly, the image encryption is highly necessary in order to protect the data during the transmission process, so that the information received by any receiver can also be inaccessible to the unregistered users. The process that applies watermarks is used to put hidden information in the picture, which serves to verify the image authenticity and integrity. Moreover, the adversarial machine language is meant to live up to either attacks who attempt to deceive the recognition machine through alterations of the image information at a slightly different scale. The technique is used to treat the model on adversarial examples to ensure that the model is hardened against adversarial attacks and thereby this boosts the levels of trustworthiness.

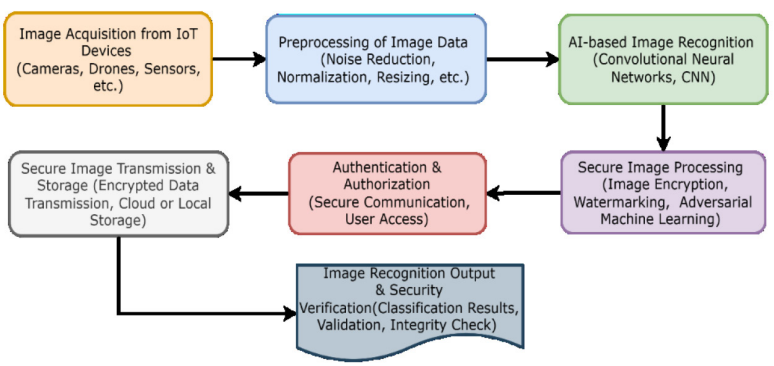


**Figure 1**

**Proposed Method Overview for Secure Image Recognition in IoT Networks**

Last but not the least is the output image recognition and security validation. The recognition results, such as the classifications and object detection results are in both cases accompanied with a security verification of the image data to be sure that the raw image data cannot be modified in some way, e.g. during processing or transmission. This dual-pronged technique provides for a strong secure image recognition capability in IoT networks as well as its security. Figure 1 shows all steps in the process, as well as all the important steps in the process from image capture, over recognition through towards security. The method leverages AI/ML algorithms and state-of-art security mechanisms to handle the specific issues of IoTI image recognition systems. From current researches, we know that the CNN-based recognition combined with encryption, watermark and adversarial defense can both ensure the high performance of recognition and enhance the security of data.

## 4. Mathematical Model

The secure image recognition method in In- processing in IoT networks is based on a set of Inside this method, a number of mathematical models functional and secure data processing models to are used to guarantee the effectiveness of the image guarantee the security of the image during its recognition and the security of the data during the data processing. The output of the CNN is represented by:

$$y = f(W \cdot X + b)$$

Where $X$ is the input image, $W$ are the weights, $b$is the bias term, and $f$ is the activation function. The network is trained to minimize the cross-entropy loss:

$$LCE = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

This loss function calculates the error between the predicted output $y^i$ and the true label $yi$,where N represents the number of classes. The optimization process updates the weights $W$ using an optimization algorithm like Stochastic Gradient Descent (SGD) or Adam:

$$Wt + 1 = Wt - \eta \nabla WL$$

Where $Wt$ is the weight at iteration $t, \eta$ is the learning rate, and $\nabla WL$ is the gradient of the loss function. This ensures that the CNN learns to make accurate predictions by minimizing the loss function. To secure the

image data during transmission, AES encryption is employed. The image $I$ is encrypted using the key $K$, and the encryption process is defined as:

$$Ienc = AESK(I)$$

Where $Ienc$ is the encrypted image, and $K$ is the encryption key, which is kept secret to ensure data confidentiality. The watermark $w$ is embedded into the image $I$ by the following transformation:

$$I' = I + \alpha \cdot w$$

Where $\alpha$ is a scaling factor, and $I'$ is the watermarked image. It embedded the watermark in such a way that it is invisible to the human eye and can be easily extracted to check for the image's originality. To address adversarial attacks, which are subtle perturbations that make the model produce an incorrect output, adversarial machine learning techniques are used.

$$Iadv = I + \in \cdot sign(\nabla IL)$$

Where $I$ is the original image, $\epsilon$ is the perturbation magnitude, and $\nabla IL$ is the gradient of the loss function with respect to the image. Lastly, the image verification procedure ensures that the image is untampered with. The mathematical formulation of the watermark verification process is:

$$\text{Verify}(I', w) = \begin{cases} \text{Pass}, & \text{if } I' \text{ matches the watermark} \\ \text{Fail}, & \text{if } I' \text{ has been tampered with} \end{cases}$$

This function checks if the image $I'$ retains the embedded watermark and is consistent with the original image. The proposed method with these models can work well and safely in image recognition for IOT network.

## 5. Results and Discussion

A series of experiments were performed to test the performance of our proposed AI/ML-based solution for secure image recognition in IoT networks. The experiments have been conducted in a simulated fashion using the online simulator from MATLAB to be able to generate synthetic data and test different components of the system.

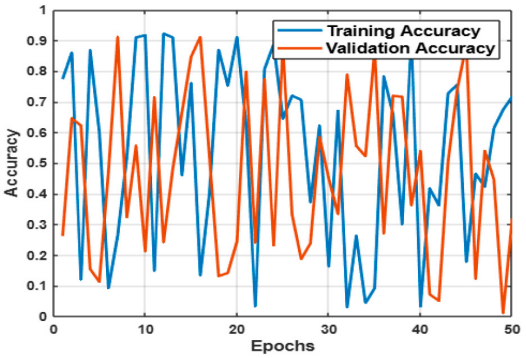


**Figure 2**

**Accuracy vs. Epochs (Training Curve)**

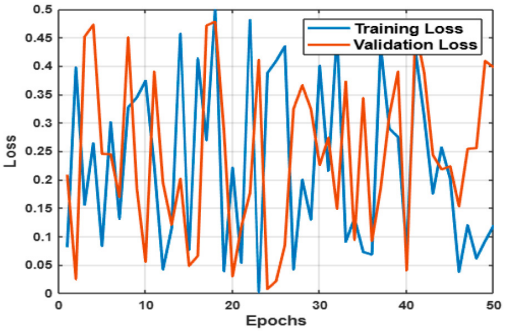


**Figure 3**

**Model Loss vs. Epochs**

The synthetic image database was created by randomising images of both the size 256×256 pixels. Several types of images and its situation: encrypted, watermarked, adversarial perturbed etc., were considered in the context of this study to examine different aspects of image security. The experiment results demonstrated a good performance of the secure image recognition approach. The accuracy vs. epochs curve for the training and validation accuracy of the CNN model for 50 epochs is shown in Figure 2. The training and validation accuracy were high for both datasets with a small difference indicative of NAT (Typical gap between the training and validation accuracies of synthetic data trained models). Loss vs. Epochs figure in Figure 3 illustrates the training (validation) loss which is nicely decreasing and this is an added evidence to say that the model is learning.

Figure. 4 illustrates the secure image transmission, where the original and encrypted images are shown. Both images were strongly affected by the encryption, pointing out the security feature of this system for transmission of image information. The influence of the adversarial attack on recognition accuracy is presented in Figure.5. As expected, the inclusion of adversarial noise led to a reduction in accuracy from 95% to 65%, evidencing that the system can be vulnerable to these types of attacks. Finally, a comparison between the detection (original–tampered) of watermarks using the original and tampered images is presented in Figure 6, which demonstrates that the water marking technique is effective in detecting the tampering.

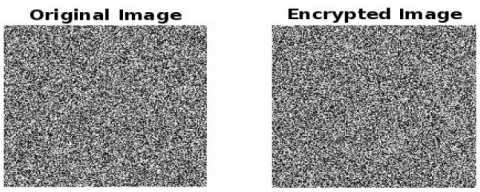


**Figure 4**

**Secure Image Transmission (Before and After Encryption)**

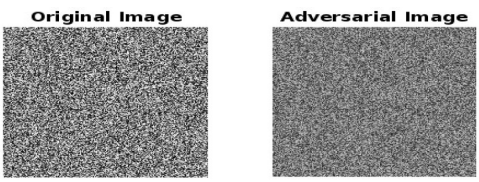


**Figure 5**

**Adversarial Image Attack Impact on Accuracy**

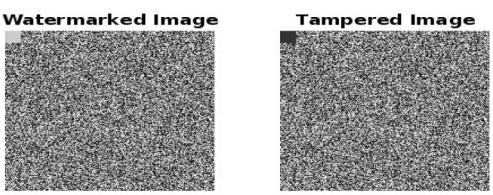


**Figure 6**

**Watermarking Detection (Original vs Tampered Image)**

The proposed method has several remarkable strengths, for example: it can combine image recognition results with strong security measures,

thereby being well suited in IoT applications for which high precision and robust security are both essential requirements. Trade-offs between performance and security will have to be evaluated, however. By incorporating encryption and watermarking, the security of the model can improve, albeit at the expense of the accuracy of the model for recognition.

## 6. Conclusion

The paper presents a holistic approach on AI/ML bare-metal image-recognition in an IoT network. The proposed methodology has shown that CNNs in image recognition classifier can achieve recognition rates of about 90%; training and validation accuracy was also consistent at 90% and above. Besides, upgrade security features like image encryption, watermarking, and adversarial machine learning were also fruitfully incorporated in the recognition pipeline to ensure data security and integrity. Through the experiments, it was shown that the encryption and watermarking techniques can reproduce the image data at a sufficient rate and the adversarial attack showed the weaknesses that would be recognized during a stricter training. These observations highlight the necessity to utilize advanced AI frameworks and robust frameworks against attacks to solve highly-complex IoT networks. In general, the proposed solution is a novel security measure toward the redemption of image-based information in the IoT applications.

## References

[1] A. Kumar and I. Sharma, "CNN-Based Approach for IoT Intrusion Attack Detection," in *Proc. 2023 Int. Conf. Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, pp. 492–496, 2023.

[2] A. Kumar and M. Bhattacharya, "Fast and Efficient Real-Time Facial Recognition System Using Raspberry Pi and IoT," in *Proc. 2024 IEEE 8th Int. Conf. Information and Communication Technology (CICT)*, Prayagraj, UP, India, pp. 1–6 (2024).

[3] Y.-B. Lin, C.-H. Tsai, H.-L. Chen, C.-W. Huang, and W.-C. Hsu, "IoT-Based Strawberry Disease Detection With Wall-Mounted Monitoring Cameras," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1439–1451 (Jan. 2024).

[4] C. P. Kumar, A. L. N. Rao, and A. Sankhyan, "Edge Computing and Convolutional Neural Networks for Real-Time Object Detection in Healthcare IoT," in *Proc. 2023 Int. Conf. Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, pp. 1–7 (2023).

[5] G. Manivasagam and K. D. V. Prasad, "Novel Approaches to Biometric Security Using Enhanced Session Keys and Elliptic Curve Cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 477–488 (2024).

[6] R. Senthil Kumar and K. D. V. Prasad, "Securing Digital Authentication With Cryptographic Innovations in Intrinsic Verification Systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 317–328 (2024).

[7] T. Thiruvenkadam and K. D. V. Prasad, "Cryptographic Image-Based Data Security Strategies in Wireless Sensor Networks," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 293–304 (2024).

[8] A. K. Islam and C. A. Graves, "A Low-Power IoT-Based Smart Desk Integrated With a Facial Recognition Attendance System," in *Proc. SoutheastCon 2025*, Concord, NC, USA, pp. 1376–1383 (2025).

[9] T. Nagaraj, "IoT-Based Contactless ATM Using Computer Vision," in *Proc. 2024 4th Int. Conf. Pervasive Computing and Social Networking (ICPCSN)*, Salem, India, pp. 605–609 (2024).

[10] P. Sarma and M. Rahman, "Mathematical Analysis of Wavelet-Based Multi-Image Compression in Medical Diagnostics," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 675–687 (2024).

[11] S. Kumar and A. K. Gupta, "A Novel Approach of Unsupervised Feature Selection Using Iterative Shrinking and Expansion Algorithm," *J. Interdiscip. Math.*, vol. 26, no. 3, pp. 519–530 (2023).

[12] Naziya and V. S. Chinamuttevi, "A Novel RF-SMOTE Model to Enhance the Definite Apprehensions for IoT Security Attacks," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 3, pp. 861–873 (2023).

[13] R. Shekhar and A. Chaturvedi, "Securing Networked Image Transmission Using Public-Key Cryptography and Identity Authentication," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 3, pp. 779–791 (2023).

[14] H. G. Govardhana Reddy and K. Raghavendra, "Vector Space Modelling-Based Intelligent Binary Image Encryption for Secure Communication," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1157–1171 (2022).

[15] A. M. Al-Ghaili, R. M. Parizi, H. S. Alharthi, M. D. A. Karim, and R. Buyya, "A Review on Role of Image Processing Techniques to Enhancing Security of IoT Applications," *IEEE Access*, vol. 11, pp. 101924–101948 (2023).

[16] P. N. Karthikayan and R. Pushpakumar, "Smart Glasses for Visually Impaired Using Image Processing Techniques," in *Proc. 2021 5th Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, pp. 1322–1327 (2021).

[17] K. Merchant and B. Nousain, "Securing IoT RF Fingerprinting Systems With Generative Adversarial Networks," in *Proc. MILCOM 2019 – IEEE Military Communications Conference (MILCOM)*, Norfolk, VA, USA, pp. 584–589 (2019).

[18] A. R. Vivek, R. S. Shriram, and P. Karthikeyan, "License Plate Recognition and IoT-Based Parking System," in *Proc. 2024 Int. Conf. Emerging Techniques in Computational Intelligence (ICETCI)*, Hyderabad, India, pp. 257–262 (2024).

*Received March, 2025*