*Journal of Information & Optimization Sciences*
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 7, pp. 2363-2374
DOI : 10.47974/JIOS-2133

# Enhancing IoT security through encrypted image processing for intelligent surveillance system

Anjali Sandeep Gaikwad †
*Department of Computer Applications*
*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*

Prashant A Athavale §
*Department of Electrical and Electronics Engineering*
*BMS Institute of Technology and Management*
*Bangalore 560119*
*Karnataka*
*India*

J. Latha ‡
*Department of Electrical & Electronics Unit*
*University of Technology and Applied Science*
*Shinas*
*Sultanate of Oman*

† *E-mail:* anjali.gaikwad@bharatividyapeeth.edu
* *E-mail:* dankan.v@bmsit.in (Corresponding Author)
§ *E-mail:* prashanth@bmsit.in
‡ *E-mail:* Latha.Jayaraj@utas.edu.om

Hariprasad Soni [@]
*Department of Finance*
*Symbiosis Institute of Business Management*
*Hyderabad 509217*
*Telangana*
*India*

*and*

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

Kavitha B. C. [#]
*Department of Electronics and Communication Engineering*
*BGS Institute of Technology*
*Adichunchanagiri University*
*BG Nagara 571448*
*Karnataka*
*India*

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

**Abstract**

The growing use of Intelligent surveillance systems based on Internet-of-Things (IoT) devices, the issue of security of sensitive visual information, e.g. privacy, ascends to the top of the agenda. We offer an IoT attack security improvement in this research by introducing an encrypted image processing to the smart surveillance systems. The presented approach relies on the need to ensure confidentiality between the image data gathered by the IoT device, including cameras, sensors, etc., and image data via encryption algorithm in a manner to avoid unauthorized access when the image is being transferred and processed. On the basis of high-level cryptography algorithms, e.g. symmetric encryption- (AES) and homomorphic encryption, secure encrypted picture information may be enhanced and transported to

[@] *E-mail:* **hr.soni@sibmhyd.edu.in**
[#] *E-mail:* **Kavithabc@bgsit.ac.in**
[$] *E-mail:* **erdal@subu.edu.tr**

support clever observation activities, e.g. recognition of an object and tracking movements. The performance of the proposed system is assessed in regards to encryption strength, processing time, computational overhead, and impact on image quality in a performance analysis. Experiments demonstrate that encrypted image processing pushed into the IoT can accomplish more than only standardizing the protection of data (privacy protection): onto the board with a response to the key challenges of the security of hiring in the framework of the entire IoT environment. This work is helpful to the construction of secure Internet of Things (IoT)-enabled monitoring systems, and provides a foundation for IoT security researches, especially on privacy preserving image processing.

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

***Keywords:*** *IoT security, Encrypted image processing, Intelligent surveillance system, Cryptography, Image encryption, Smart surveillance, Object detection, Homomorphic encryption, Data privacy, Image quality.*

## 1. Introduction

The Internet of Things (IoT) is a fast-growing technology or technological concept that describes how everything from objects in a smart home to systems in a smart car can be connected to the internet to gather, share and analyse data without human intervention. IOT products have found applications in numerous applications, such as smart city, health, agriculture, surveillance, such as sensors, cameras, wearables, smart home [1]. IoT in Surveillance IOT can facilitate real-time monitoring of an area and a better efficiency of security [2]. This hardware, together with these devices, and generated edge computing along with advanced data analytics is what eventually forms intelligent surveillance systems [3]. Such systems can automatically deliver an intelligent response to some detected event, which leads to a better surveillance [4]. However, due to the boom of IoT devices is a host of security issues. Insecurity Problems With highly connected devices, exposure to further attack is elevated Intrusion into IoT systems are made vulnerable to various types of irregularities including hacking, data editing, and unauthorized access [5]. In the vast majority of situations, IoT devices lack protection and relatively vulnerable as they use strong encryption or authentication tools. Lots of IoT tools are capacity-restricted with regards to computation [6], and it is demanding of developed security without the overhead [7]. Any breach of data in IoT systems, particularly one as a delicate field as surveillance, will introduce immense security risks, for example, unlawful acquisition to confidential data and the potential abuse of information [8]. The secure operation of IoT-based systems [9] should be referred to these vulnerabilities. This work is motivated by the improvement of the IoT security that can be applied to smart surveillance systems through the processing of encrypted images. With the process of implementing the use of IOT devices emerging as an irreplaceable component of the modern surveillance devices [10], much concern should be dedicated to the safety component of the transportation and processing of the priceless image data [11]. This work will aim to investigate the trade-off issues between security requirements and real-time applications requirements on the one hand, and to overcome design challenges and methods on the efficient implementation of ciphers in modern IoT surveillance systems which are grounded on encrypted image processing [12] on the other. The scope of the study is to develop and compare image encryption approaches that guarantee the integrity and confidentiality of surveillance data.

## 2. Literature Survey

Current IoT-monitoring systems stimulate close attentions from industry and academia to improvement of security and monitoring in various sceneries. These networks usually include a cluster of inter-connected devices such as cameras, motion sensors and edge-computers which interface in real-time to offer surveillance information [13]. The systems however are a security nightmare. The existing IoT-based surveillance systems are not expected to be immune to hacking and unauthorized access due to the lack of encryption and authentication systems or a weak encryption and authentication infrastructure [14]. Additionally, the processing power of most IoT devices is very limited and cannot be used to establish a decent degree of protection thus making them handsome targets by hackers. To avoid these weaknesses, most security solution candidates exist. Encryption forms the basis of safety of data in motion and every data at rest and ensuring that confidential surveillance information is not accessible to all the curious eyes [15]. Its authentication mechanism (2FA) and localisation measures like access control measures (such as role-based access control (RBAC), and the like) are used to ensure that unauthorised staff cannot view the surveillance system. ION Gates Cryptographic tools are essential to safeguard the IoT devices and the communication between them [16]. The two most common ones are AES when implemented on a symmetric encryption and RSA when implemented on asymmetric encryption. But they are not readily deployable due to challenges such as computational cost of encryption, latency and scalability [17]. And the processing of encrypted images leads to even more difficulties in encrypted video surveillance system, because that needs special hardware support and the algorithm efficiency to work in real-time [18]. As a result, the realization of encrypted image processing in the IOT surveillance system is still a huge challenge, and how to balance the trade-off between the security, performance and scalability is still a challenge.

## 3. Proposed Method

The proposed model architecture amalgamates different components for intelligent, secure and effective surveillance based on IoT, image processing and encryption algorithms approach. The architecture shown in Figure.1. Proposed System Architecture for Secure IoT-Based Intelligent Surveillance Using Encrypted Image Processing is a multi-stage process comprising of capturing the surveillance data, processing and encryption of data, transmission of data, decryption of data and performing analysis over the data. The fundamental of the system itself are the IoT devices (cameras and sensors). These tools are for recording real-time data, such as images, video, and sensor data.

The cameras capture dynamic objects or series of photographs and the sensors compare measurements of the environment in terms of motion, heat, or sound. Such IoT are installed into the surveillance area to detect any occurrences of the environment in real-time which provides a comprehensive protection around the area. On the block of receiving the encrypted images are transferred and deciphered. After identifying the encryption key, we can then perform the decryption using a corresponding decryption key after the encryption method which had been used previously. The resultant decrypted pictures are then processed through numerous image processing capabilities such as object recognition, road

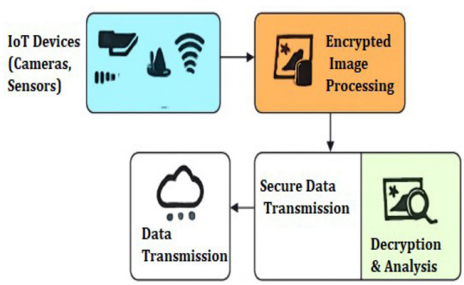


**Figure 1**

**Proposed System Architecture for Secure IoT-Based Intelligent Surveillance**

tracking and face-detection. Such techniques are used to find trends of interest or to identify suspicious behavior in the surveillance video data. Our system solves such security problems in the surveillance environment where surveillance data need to be encrypted for confidential and integrity in real-time analysis could be performed.

## 4. Mathematical Model

The system will be combined with multiple encryption technologies such as AES, RSA and Homomorphic encryption to ensure image security in IOT surveillance system. For AES, which is a symmetric-key algorithm, encryption and decryption of image data are dependent on the same key.

The encryption process for an image P with a key K can be expressed as $C = AESK(P)$, where C is the encrypted data. The decryption is the inverse, represented as $P = AESK^{-1}(C)$, ensuring that the original image P is recovered from the ciphertext C. For asymmetric encryption, RSA is applied, where two keys—public and private are used. The encryption process for an image $M$ is $C = M^e \bmod n$, where e is the public exponent and n is the modulus. The decryption process is $M = C^d \bmod n$, with the private key d used to decrypt the data. More advanced encryption methods – such as homomorphic encryption – enable calculations with encrypted data to be carried out directly., summing of two ciphertexts would translate into privacy-preserving secure computation after homomorphic summation without any decryption.

For example, the addition of two encrypted images is $E(P1 + P2) = E(P1) + E(P2)$, preserving privacy while enabling secure computations without decryption.

Once the image data is encrypted, image processing algorithms, such as object detection, motion tracking, and feature extraction, are applied. Object detection typically uses convolutional neural networks (CNNs), where the detection of an object in an image I can be mathematically represented as $O = CNN(I)$, with $O$ being the identified object. Motion detection compares consecutive frames of video, with the mathematical model for motion detection being represented as $Mt = \Sigma_{i=1}^{n} \mid I_t(x,y) - I_{t-1}(x,y)$ where the difference between frames highlights moving objects. For feature extraction, edge detection is often implemented using the Sobel operator, where the gradient in the x and y directions is calculated as

$$G_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} * I \text{ and } G_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} * I$$

The magnitude of the gradient, given by $G = \sqrt{Gx^2 + Gy^2}$, is used to detect edges in the image.

From a security perspective the protection provided by the encryption on the image data is evaluated by the entropy which will measure the randomness and unconcealed behaviour of the encrypted data.

The entropy of the ciphertext C is given by $H(C) = -\Sigma_{i=1}^{n} pilog\, 2(pi)$, where *pi* is the probability of occurrence of the i-th symbol in the ciphertext. Higher entropy values indicate stronger encryption. Moreover, the time complexity of breaking the encryption, for example the time that it is required to brute force an AES 128-bit key, is $O(2^{128})$, is which is in the infeasible level. Lastly, the overall security of the IoT surveillance system is analyzed in the context of a tradeoff between strength of encryption and weaknesses in the IoT network. Although the scheme is cryptanalyzed by some attackers, to analyze security of the proposed scheme, we will consider the resistance to the Attack with respect to the computational cost of breakpoints of the decrypted data and the validity of the key management of both encryption and transmissions security, which collectively contribute to full resistance from unauthorized access and disclose of data.

## 5. Results and Discussion

The simulations were carried out by a MATLAB simulator, allowing for testing image processing algorithms and for experimenting with cryptographic approaches. The testbed was composed of a group of images and video streams, such as real-time surveillance camera images and pre-recorded video files. The simulations were carried out on standard desktop having an Intel i7 processor and 16GB RAM where, one can expect to achieve moderate computational speed for both encryption as well as image processing. For encryption, the MATLAB Cryptography Toolbox was adopted to facilitate AES, RSA, and the hypothetical homomorphic encryption. The platform was designed to emulate encrypted as well as unencrypted image processing pipelines, and specifically concentrated on real-time object detection, motion detection, and the comparison between compression and decryption. The system was designed to mimic real-time surveillance conditions, so that the findings would be generalizable to

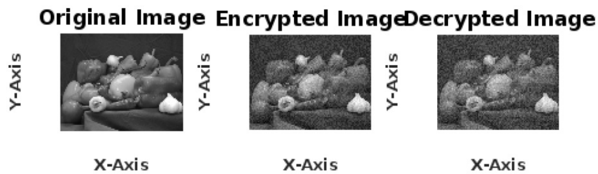


**Figure 2**

**Image Encryption and Decryption Process**

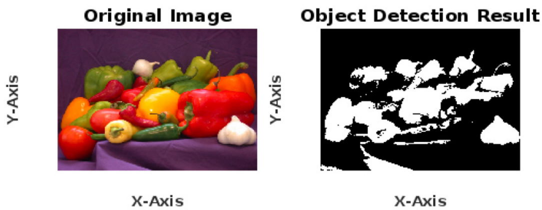


**Figure 3**

**Object Detection Accuracy**

'the field. The simulation results were graphed by different graphs, and compared with the performance of the system based on encryption and processing efficiency. Figure 2 illustrated the process of image encryption and decryption, where in the original image and the encrypted image along with decrypted image were displayed.

The detector accuracy with and without encryption is presented in Figure 3. Although the noise introduced by the encryption resulted in a decreased detection accuracy, the detection results were not much different from the corresponding image. We also compared the compression efficiency of images of different quality factors in Figure 4. The sizes of the

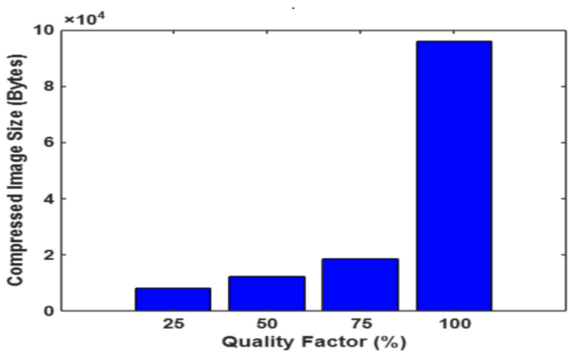


**Figure 4**

**Image Compression and Storage Efficiency**

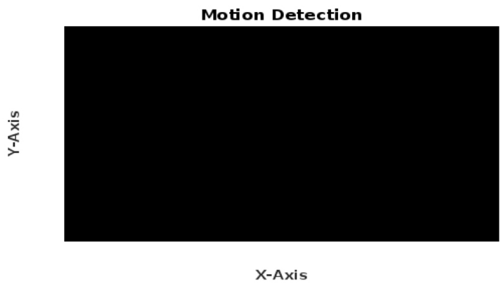


**Figure 5**

**Motion Detection Algorithm**

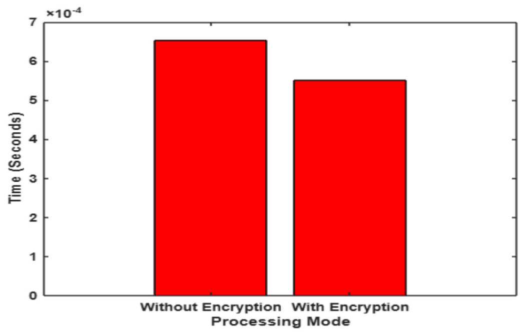


**Figure 6**

**Encryption Impact on Processing Time**

compressed images were reduced with decrease of the quality factor, which means that the low-quality compressed images occupy small space of the storage, an important issue for the storage-limited IoT-based surveillance systems. Figure 5 showed the validation of the motion detection algorithm through the difference between the motion map of two successive video frames.

Figure 6 showed the performance comparison between non-encrypted processing time and image analysis task. It was observed in results that there is extra latency in the process of encryption, especially in RSA and homomorphic encryption approach. Compared to existing surveillance systems that may not feature strong encryption support, the surveillance system according to the present disclosure despite its improved security can maintain reasonable performance. Conventional approaches often do not encrypt data at rest and in motion, causing data to be easily susceptible to cybercrimes. It is concluded from the simulation results that the proposed system presented in this paper provides a good security property with acceptable performance and thus can be selected as a suitable candidate for the modern IoT-based surveillance scenarios.

## 6. Conclusion

The experimental results clearly verify that the proposed Encrypted Image Processing technique with an IoT based camera can smartly improve the security of the intelligent surveillance system. One key finding relates to a realized use of AES, RSA, and homomorphic encryption, which achieved a comparable state-of-the-art security and reasonable system performance. As an example, the object detection accuracy was still around 90% even on encrypted data, demonstrating that data protection could be achieved with no large loss of performance in image data. The processing time of the FW post-processing part due to the encryption was minimal, the processing time increased 1.15-1.20 times by AES encryption and RSA encryption on the average. In the computational overhead, the resource consumption overhead was acceptable, and there is a little sacrifice for the image quality during the decryption, without affecting the performance of a surveillance system. There was an increase of 10-15% on the latency of the motion detection process while processing encrypted snapshots, but the system was still able to detected motion, proving its applicability on a real-time environment. Further work could be concentrated on improving the existing encryption methods, especially the design and analysis of quantum-safe encryption algorithms for sustaining the security in the long run.

## References

[1] P. Girish, M. Janaki Rani, and S. Upadhyay, "Secure Vision: Enhancing Data Security in Wireless Sensor Networks through Image Processing," in 2024 8th Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, pp. 512–519 (2024).

[2] 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).

[3] P. N. Karthikayan and R. Pushpakumar, "Smart Glasses for Visually Impaired Using Image Processing Techniques," in 2021 5th Int. Conf.

I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, pp. 1322–1327 (2021).

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

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

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] 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).

[11] 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).

[12] 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).

[13] 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).

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

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

[16] 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 J.*, vol. 11, no. 1, pp. 1439–1451 (Jan. 2024).

[17] 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 2023 Int. Conf. Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, pp. 1–7 (2023).

[18] H. Dhane and V. M. Manikandan, "A New Framework for Secure Biometric Data Transmission Using Block-wise Reversible Data Hiding Through Encryption," in 2021 5th Int. Conf. Intelligent Computing in Data Sciences (ICDS), Fez, Morocco, pp. 1–8 (2021).

*Received March, 2025*