Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

A HYBRID CRYPTOGRAPHY-STEGANOGRAPHY FRAMEWORK FOR SECURING IOT-GENERATED AGRICULTURAL DATA FROM SENSOR TO CLOUD

Zahida Parveen[1], Badarqa Shakoor[*2], Maryam Ahmad[3], Shaher Bano[4], Shehar Bano[5], Bira Alam[6]

[1,*2]*University of Agriculture, Faisalabad*
[3]*Quaid-E-Azam University, Islamabad*
[4]*Nust University*
[5]*The University of Faisalabad*
[6]*Riphah International University Faisalabad*

[1]zahidauafcs@gmail.com, [*2]badarqa25@gmail.com, [3]maryamahmadjourney@gmail.com, [4]sbano.msis22seecs@seecs.edu.pk, [5]sheharbano.cs@tuf.edu.pk, [6]bira.alam@riphahfsd.edu.pk

DOI:https://doi.org/10.5281/zenodo.21161133

Keywords
Internet of Things (IoT), Steganography, Cryptography, Precision Agriculture, Data Security, Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR).

Article History
Received: 25 April 2026
Accepted: 08 June 2026
Published: 21 June 2026

Corresponding Author: *
Badarqa Shakoor

Abstract

Agriculture is an important part of the global economy and the use of Internet of Things (IoT)-enabled agri-care devices has greatly improved the efficiency, accuracy and productivity of modern agriculture. These intelligent gadgets gather and send real-time data about soil moisture, crop conditions, weather forecasts and predictions, giving farmers and stakeholders the information they need to make informed decisions. But a number of cyber threats are threatening such agricultural information transmission and storage over the IoT network such as Man-in-the-Middle (MITM), cryptanalysis key management vulnerabilities and unauthorized data interception. In precision agriculture, where IoT devices are often resource-constrained with limited computational power, memory and energy, traditional security measures are often impractical, making the need for lightweight and powerful data protection solutions more critical than ever.To fill this, the current study suggests a lightweight hybrid security framework integrating cryptography and steganography to protect the sensitive data in the precision agriculture context in the IoT environment. The proposed solution selectively encrypts the information related to the crops and embeds it in cover images by Least Significant Bit (LSB) and Most Significant Bit (MSB) steganography technique, thus providing two layers of protection: the encrypting part ensures confidentiality, and the embedding in the cover image ensures that the sensitive information cannot be detected by the adversary. The selective encryption approach reduces the computational burden, making it appropriate for resource-limited IoT devices while maintaining the security strength of the system.The proposed framework has been thoroughly tested in terms of performance metrics such as encryption/decryption time Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and payload capacity to ensure enhanced security and image fidelity. Experimental results show that the hybrid approach has significantly

improved data security reduced stego-image encryption time, and kept the stego-images' distortion level low, all confirming the success of this approach. A comparative analysis also reveals that the proposed method performs better than standard cryptographic/Steganographic methods on processing speed and against common attacks. The results confirm the efficiency and feasibility of the proposed hybrid cryptography–steganography approach as a secure, low overhead solution for the protection of sensitive agricultural information in real-world scenarios for IoT-enabled precision agriculture applications.

1. INTRODUCTION

Agriculture is playing a vital role in liquidity and the global food security and will rely on new Internet of Things (IoT) technologies to improve productivity, sustainability and resource usage. Precision agriculture has been enhanced by the advent of the Internet of Things (IoT) which allows the use of smart sensors, automated irrigation systems, unmanned aerial systems (UAS) and processing to collect data in real time in order to manage the health of crops, optimize resource utilization and enhance overall farm management (Karunathilake et al., 2023). Yet agriculture is also moving into a era of data-driven operations, while also being subject to an increasing number of cyber attacks that threaten the security of data in terms of confidentiality, integrity and availability. There are several interconnected stages to a secure and efficient agri-care system utilizing the Internet of Things, with each step playing a role in the resilience and reliability of the network. The phases are presented in Figure 1 which contains IoT device deployment, crop planning, data analysis, security analysis, monitoring, and cloud security (Fathy & Ali, 2023). Real-time monitoring and security frameworks help maintain the integrity of agricultural IoT networks, ensuring they are secure from unauthorized access, data breaches, and cyber threats. Interdependence between IoT devices in smart farming creates security threats that can result in data breaches and access, as well as manipulation of the system. Agriculture data might be sensitive, which can lead to economic losses and operational disruptions due to threats like operation by a man-in-the-middle (MITM), crypt analysis, and key management exploits (Asif et al., 2021; Yazdinejad et al., 2021). If the IoT network is compromised it could be used to manipulate crop monitoring data, to disrupt automated irrigation or to tamper with precision

agriculture, which in turn would have an impact on food production and food supply chains (Yan et al., 2021). Considering the high dependency on IoT for real-time decision making in agriculture, securing these systems has become more important than ever, to ensure the authenticity of the data and the resilience of the system. Traditional crypto graphic Although methods like RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard) offer strong security features, they frequently have a large processing cost, which makes then inappropriate to IoT gadgets with limited resources. (Rasori et al., 2022; R. K. Singh et al., 2021; S. Singh et al., 2024). Much of the agricultural IoT equipment is deployed in remote areas that have restricted computing power and energy availability such that lightweight security frameworks are required that offer high levels of security by implementing strong encryption without compromising computational efficiency. Moreover, traditional encryption schemes treat all data the same, causing an unnecessary processing burden for less critical data (Clemente-Lopez et al., 2024).This investigation proposes an innovative security model to address these limitations, which entails conventional cryptographic techniques, along with steering to enhance the security of agri-care systems for IoT. While cryptographic techniques are used for ensuring data confidentiality by transforming the data into an unreadable format, steganographic techniques will embed encrypted data within digital images and make them more difficult to intercept or access by an authorized user. The method uses a selective encryption approach, which helps reduce the computational

complexity by encrypting only the information that is critical to the crops, and not entire datasets.A proposed framework is measured with quantitative Performance metrics like Peak Quality of Signal to Noise Ratio (PSNR) mean squared errors (MSE) or encryption/decryption efficiency to evaluate its suitability for data hiding, security level and computational load. The results showed that the hybrid solution not only provides more security but also decreases the encryption time and maintains the fidelity of the data which makes it applicable in the precision agriculture IoT ecosystem where resources are limited.Overall, this research provides a novel and lightweight security strategy that addresses the unique security concerns of agriculture-oriented IoT systems, thereby advancing the field of cyber security in smart farming. This study proposes a robust security framework by combining crypto graphic techniques with steganography to enhance data integrity, confidentiality, and computational efficiency, which would further bolster the trustworthiness of IoT-based precision agriculture solutions. In Section 1 the need for securing agri-care systems with IoT is introduced. The Research Background discusses the latest cryptographic and steganographic methods used in agriculture and IoT. The proposed hybrid framework is described in Section 3 and the Results and Discussion section examines the performance of the framework. Lastly, the Conclusion restates the main findings addresses the limitations and suggests future research.

2.Exisiting Study

Protecting crop images stored digitally is imperative due to their abundance, size, and sensitive content. Given that digital images are typically two-dimensional, the ability to abruptly trace and sever links between pixels is crucial; that's why the authentication assessment presents insights into suitable key-based security techniques (Dev & Prasad, 2023). A new lightweight cryptography approach aimed at enhancing security within the IoT framework. A lightweight cryptography technique has been put forward to enhance IoT security. The effectiveness of precision farming also suggests strong solutions that improve security and confidentiality measures customized to the particular needs About farming industry. Threats to precision agriculture systems' dependability and efficiency include equipment hackingn illegal access, and data leaks (Pauline A. Ongadi, 2024). Several suggested algorithms Such as those with optimized recovery and quicker protection for IoT safety.Data storage and retrieval can be completed faster when there is a reduction in the encryption/decryption time. By reducing the quantity of rotations for decryption as well as encryptio.the suggested approach shortens the encryption time (Mousavi & Ghaffari, 2021). Steganographic techniques based on LSBs (Least Significant Bits) have been around for a very long time and are used to conceal sensitive information when both the embedding efficiency and capacity are very low. LSB-based steganographic technique makes use of a reversible histogram transformation (Mukherjee Ganguly et al., 2018). The system may effectively collect, process, and use data to maximize onion production. Even with the use of these revolutionary technologies, data security and privacy are still crucial. By employing strong encryption protocols for both recording and transfer, protecting confidentiality of producers' data, the system guarantees accuracy in privacy of the gathered data (Khan & Kashem, 2023). This is because trust elements for sharing and accessing agricultural data are absent from the centralized agricultural information systems that are already in place. To do this, the rise of exciting innovations such as facilitates the building of trust (T. et al., 2023).

The transparency of transactions has increased. It is possible to eradicate fraud. Because cryptocurrency relies on contract technology and algorithmic consensus, it allows users to safeguard payments. In live applications, combining IoT and blockchain would increase device effectiveness (Raveena & Shirly Edward, 2021). The current work examines symmetrical, asymmetrical, and mixed encryption techniques for The Wider World of Contents security. To avoid key distribution via an insecure route and to guarantee Asymmetric key encryption is utilized to ensure confidential interaction with multiple users.Security-related variables are used for

evaluating all systems (Mousavi et al., 2021b). To optimise crop output, limit environmental effects, and minimize resource waste, the majority of smart crops need to gather and process real-time agricultural data. This collection and processing of agricultural data is essential for the majority of smart farming apps, which aim to reduce resource waste, minimize environmental impact, and increase crop yields (Zhou et al., 2021). Cryptographic algorithms are utilized as a crucial remedy to ensure the confidentiality and integrity of data transferred between the sending party and the recipient. In order to safeguard sensitive data in Internet of Things-based intelligent fertilizer setups. In this work, the ECC technique encrypts the RC4 key. The suggested approach outperforms alternative encryption algorithms and is safe against several recognized threats, including the Man-in-the-Middle (MiM) attack, according to a thorough study and simulation data (Mousavi et al., 2021a).Furthermore, security concerns related to IoT farming have been brought to light. Additionally, a relationship between IoT-based agricultural systems and pertinent technology has been illustrated, encompassing massive archives of information and data processing (Farooq et al., 2019). The limitations and potential applications of IoT to farming were examined in light of the study's findings. It is anticipated that quicker and more comprehensive An excessive number of crop-related modules operations. This can be achieved by improving the quality of crops and output while cutting labour (Kim et al., 2020). Ranchers gain greatly from the extraordinary ability management provided by agriculture cloud and IT in terms of the growth of yields, calculating, composting, and detailed methods (Systems, 2017). When contrasted with proactive routing, fixed-route systems are safer; however, huge regions and capacity are not suitable for stable algorithm-based systems (Haseeb et al., 2020).Security-related problems and difficulties in this area. To satisfy We propose incorporating low-cost cryptography techniques into the Internet of Things (IoT) framework for smart farming in order to meet the requirements of IoT devices with limited assets. Additionally, we look into implementing the Expeditious Cipher (X-cipher), an affordable encrypting procedure, to establish a secure channel connecting (Fathy & Ali, 2023). The process of precision farming involves applying various technological tools and automating processes to increase output in agriculture. This paper presents a technique based on elliptic curve encryption, which has been proven to be technically private. To increase agricultural productivity, other technologies (Abduljabbar et al., 2023).But as smart farming methods become more widely used, a number of privacy concerns surface that must be addressed to preserve confidentiality, reliability of data, and the farming industry. The safety risks associated with smart farming, such as weak points in IoT devices, non-standard safety protocols, low security knowledge within producers, and difficulties protecting data as well as networks (Martin Otieno, 2023).In terms of agriculture, concerns with water, irrigation techniques, and cutting back on fuel, fertilizes, and pesticides all contribute significantly to lower production costs. Even though WSNs hold a lot of potential for the years to come, issues with coverage and installation still need to be resolved. The implementation of WSNs for IoT networks is presented in this study to implement safety and arrangement, as well as to share data (Saleh, 2020). Agriculture's external field areas necessitate additional security measures, setting it apart from industrial control systems. There is no suitable cybersecurity standard for the agricultural industry (Kristen et al., 2021). There are still a number of issues and difficulties in efficiently learning the traits of large-scale, low-quality, diverse, complex, and rapidly-changing big data (Qureshi et al., 2022).

3.MATERIALS AND METHODS

The following analysis presents cross between security framework that combines cryptography and steganography to secure sensitive crop data in IoT-enabled agricultural environments. The methodology covers the experimental setup, the design of the proposed framework, data handling strategies and encryption process.The indicators of evaluation that are employed to evaluate the efficiency of the structure. The whole system was designed to achieve a data protection-

confidentiality versus system efficiency trade-off in resource-limited IoT settings. A suggested paradigm for study is illustrated in Fig. 1 which shows the overall structure and flow of the suggested study paradigm.

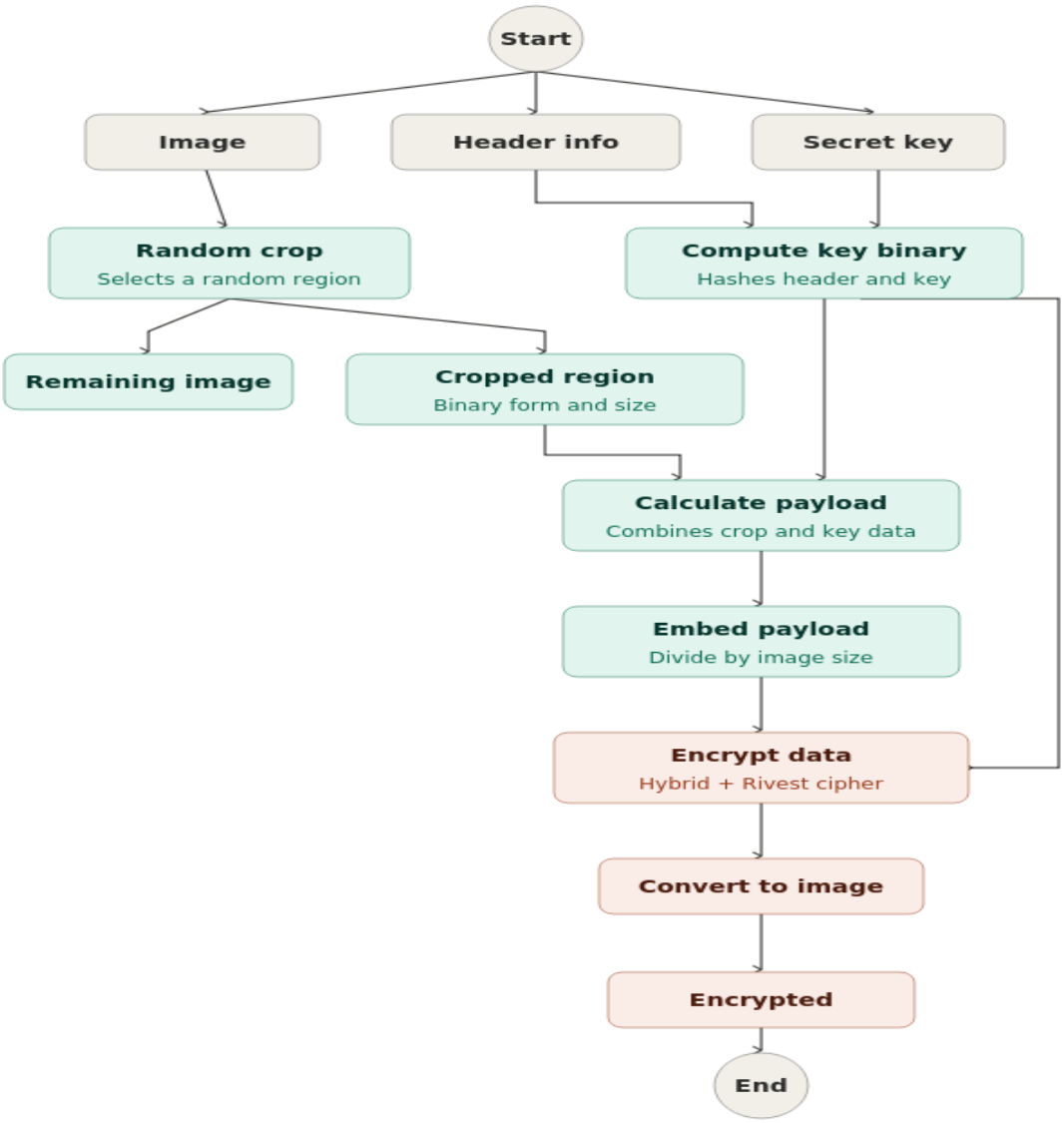

Fig. 1: Research approach

The framework was implemented and tested in a controlled computing environment simulating typical IoT constraints. The processor used was from Intel, the Core i5-10210U processor clocked at 1.6 GHz and having 8 GB of memory, but memory was restricted to 512 MB to simulate the memory limitations of edge device applications in agricultural IoT. The OS used was Ubuntu 20.04 LTS, and the primary programming language was Python 3.8.10, which has a large repository of libraries for cryptographic and image processing. Popular libraries used are Open CV for image processing, PyCryptodome for cryptographic operations and NumPy for handling matrices

effectively. For the purpose of validating the proposed framework, agricultural images of four crop types were used, namely wheat, corn, rice and sunflower. These datasets have been obtained from the University of Agriculture, Faisalabad, and complemented by publicly available repositories.For performance evaluation, each picture was resized to 200x200 pixels to ensure uniformity. The original images were of different sizes and resolution, and wheat images were as large as 576 X 1280 and sunflower images were as small as 640 X 426.Hybrid security model is intended to offer light-weight yet adequate protection to the sensitive agricultural information sent utilizing IoT enabled frameworks. The framework is comprised of a series of well-defined stages, each of which accomplishes a specific preparatory, embedding, encrypting and validating task for secure information in the crop image.The first step in the process is the selection of farming photos from among wheat, corn, rice and sunflowers datasets. To provide diversity and relevance, these images are taken from the University of Agriculture Faisalabad and public repository. The images that are chosen should be in compliance with the following conditions:

- Color Mode: RGB (24-bit) or IT UCM (ITU 24-bit).
- Color Space: RGB (24-bit) or IT UCM (ITU 24-bit).
- Formats: Lossless image formats (PNG or BMP)
- Content: Distributed colour information for better steganographic embedding capacity

After the selection, each image goes through a pre-processing phase which aims to improve the quality and uniformity of the data to facilitate the manipulation by steganography.

This includes:

- You must resize and normalize all of the images to the same dimensions 200×200 pixels.
- Convert BGR to RGB.Colour Space Conversion BGR to RGB.
- Noise Removal with Gaussian filter with 3×3 kernel
- Contrast Enhancement in Luminance Channel (Y) of YCrCb colour space using histogram equation.

This pre-processing removes noise and optimises the image for embedding, while avoiding artefacts that could affect its stenographic imperceptibility. The image is preprocessed and a Region of Interest (ROI) is extracted from the image. The ROI is normally the portion of the crop that is visually rich and has enough entropy to effectively conceal binary data. This area is then converted to binary. The channels (R, G, B) in each pixel of ROI are 8-bit quantity, which are converted into 2-bit binary quantity for each channel. Embedding is done in the resulting binary stream which acts as the carrier medium.

A single pixel employed to embed the information (usually 1-3 bits).If the size of the payload (header+secret message) is larger than C, then a larger ROI is chosen, or the message is compressed prior to being embedded. Some scenarios of selected ROIs are shown in Fig. 4.

Fig. 2: image of corn, rice, sunflower, wheat

The embedding process is based on a hybrid steganographic algorithm which combines the traditional Least Significant Bit (LSB) algorithm with dynamic bit position selection in both LSB and Most Significant Bit (MSB). The technique is adaptive and random, and hence is resistant to usual steganalysis attacks. Some of the logic embedded in the key components is:Bit Position Selection: Instead of always using the 1st LSB, the method uses a using a secret key as the seed for an arbitrary number algorithm (PRNG) to select between LSBs, mid-bits, or MSBs for each byte.The changes to the image are not noticeable to human observers because of the adaptive embedding, while at the same time providing strong embedment of the payload. After embedding, the stego image undergoes a light-encryption phase with RC4 encryption algorithm. This ensures that, if the image is intercepted, it is unable to be read without the decryption key. RC4 is a symmetric stream cipher that is known for its fast and simple operation, making it suitable for use in IoT devices that have limited resources.

4.Results and Discussion

To evaluate the efficacy of the steganographic and cryptographic processes, two widely accepted measures for quality of pictures were used: Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).These measurements.provide a quantifiable measure of visual distortion between the original and stego images after data embedding and encryption.MSE evaluates the mean faced variation between an initial and altered (stego) picture's value of pixels. It serves as a direct indicator of distortion introduced during the data hiding and encryption process. A lower MSE value suggests that the pixel-wise differences are minimal, meaning the image quality is better preserved. In the context of steganography, maintaining a low MSE is critical because it ensures that the embedded message does not significantly alter the visual characteristics of the image. For images used in agricultural applications where analysis might be performed visually or algorithmically, preserving fidelity is essential.

PSNR provides a logarithmic measure of the ratio between the maximum possible pixel value and the magnitude of distortion (as measured by MSE). It expresses the perceptual quality of the stego image in decibels (dB). Higher PSNR values indicate that the visual difference between the original and stego images is barely detectable by the human eye. While MSE gives a mathematical measure of error, PSNR is more interpretable in terms of human perception. It is particularly valuable in image steganography because the goal is to embed information invisibly, that is, without raising visual suspicion or affecting image usability.

The hybrid framework was tested across the four crop image categories. Each image was preprocessed, embedded with secret data, encrypted using RC4, and then evaluated. The results reflect the effectiveness of the embedding strategy and the efficiency of the encryption process.

The recorded MSE and PSNR values for each crop image are presented in figure 3.

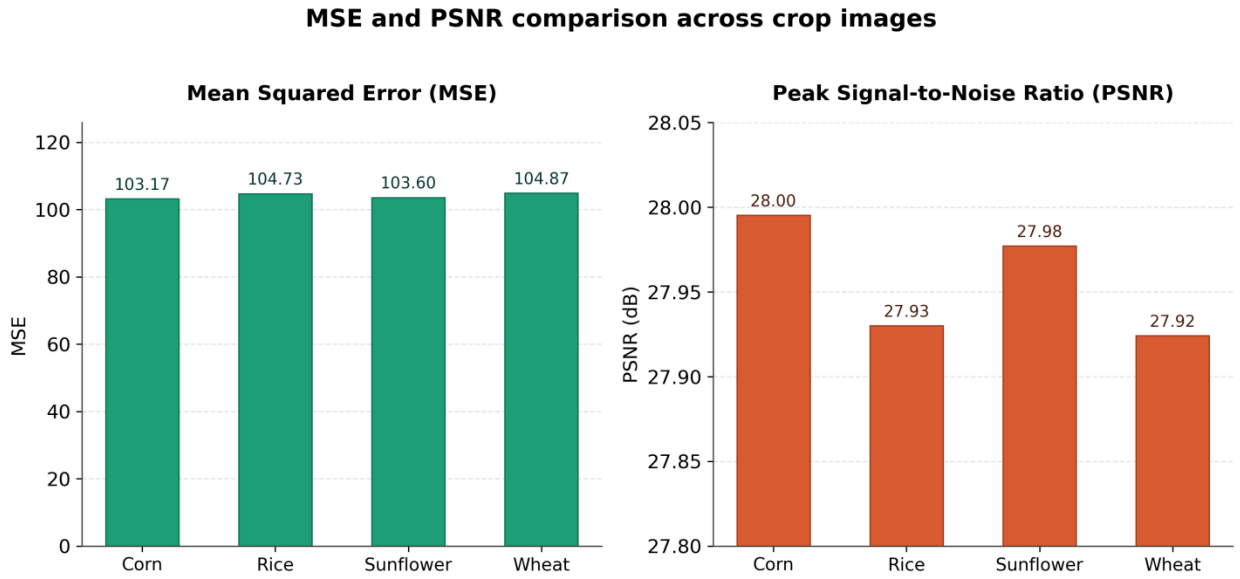

figure 3. Mean Squared Error Values

To further support the quantitative evaluation, the MSE and PSNR values for each crop image were visualized through bar graphs. As shown in Fig. 5A, the Mean Squared Error remained relatively consistent across all crop types, indicating minimal pixel-wise distortion introduced by the embedding process. Fig. 5B presents the corresponding PSNR values, all of which remain above 27 dB, reinforcing the conclusion that the stego images are perceptually indistinguishable from the originals. The graphical trends validate the stability and effectiveness of the proposed hybrid steganography method across diverse agricultural image inputs.

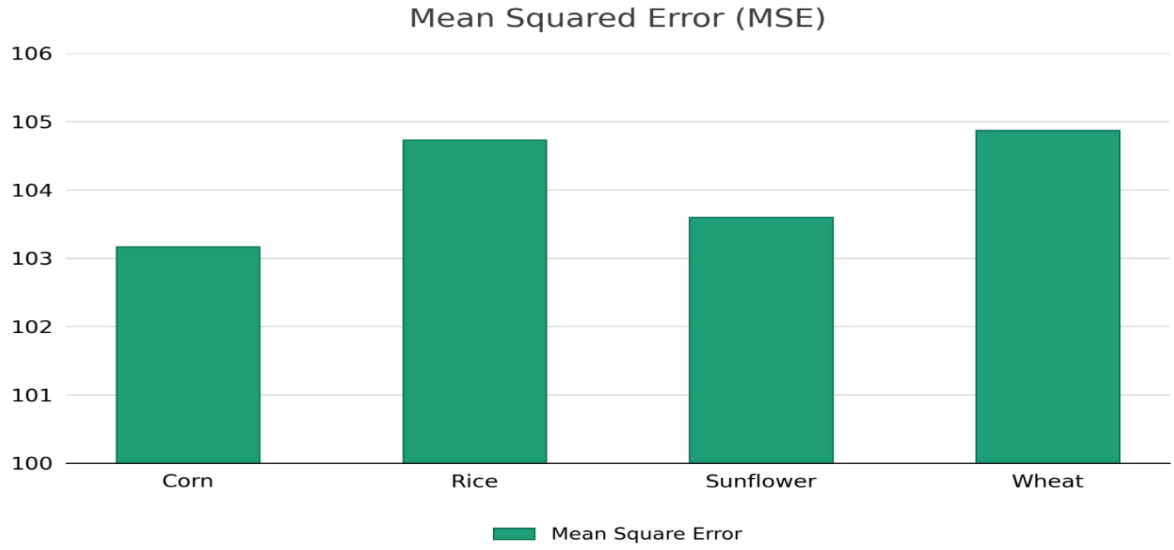

Fig. 4(a): Mean Squared Error (MSE) values for corn, rice, sunflower, and wheat images encryption.

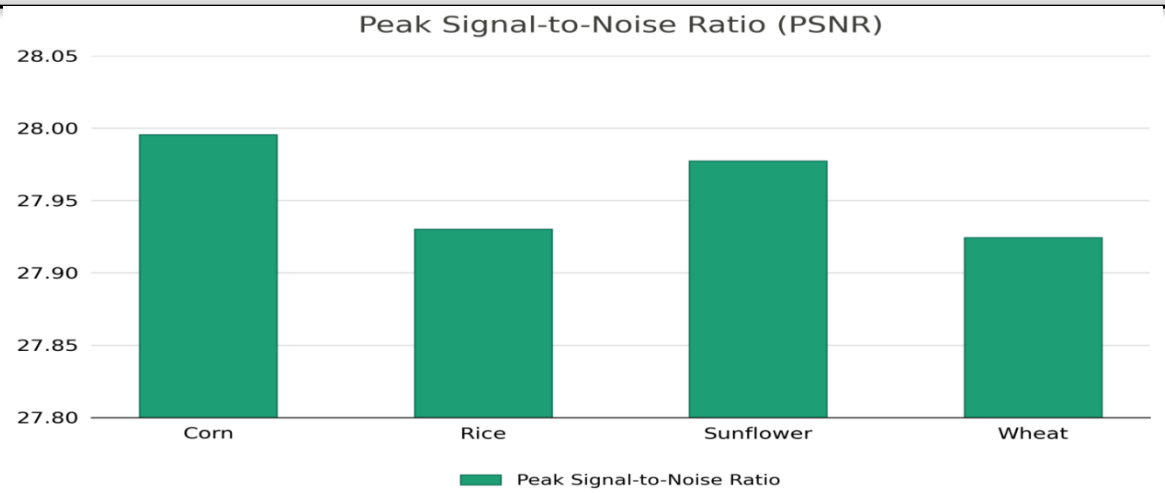

Fig. 4(b): Peak Signal-to-Noise Ratio (PSNR) values for the same images, indicating perceptual image quality.

In order to evaluate the suggested structure's computing accuracy,encryption time was measured for each crop image after the embedding process. Rather than summarizing this data in tabular form, individual graphs were generated to visualize the encryption time recorded during each execution cycle. As shown in Fig. 6A and 6B, the encryption time remains minimal across all datasets, confirming the suitability of the RC4 cipher for resource-constrained environments. Each graph plots encryption time (y-axis) against operation instances or run indices (x-axis), highlighting the stability and repeatability of the encryption process under consistent conditions.

- Corn, sunflower, and wheat images consistently show encryption times underneath 1 millisecond, indicating extremely lightweight overhead
- Rice images occasionally exhibit slightly longer times, though still within acceptable bounds for IoT-based operations

These results validate that the proposed framework maintains low computational latency, making It is feasible for in close to or immediate use applications in agricultural monitoring systems. The use of a stream cipher, combined with selective and adaptive embedding, ensures a balance between security and performance.

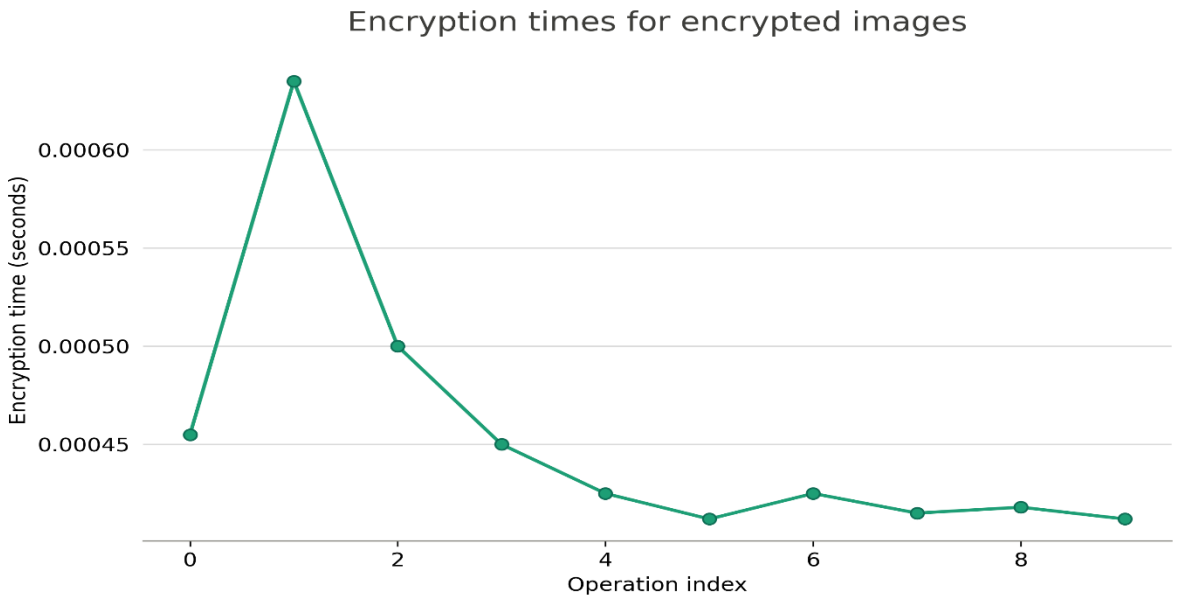

Fig. 5: Encryption time per operation instance for the Sunflower Wheat image dataset's, respectively.

The experimental results of the proposed algorithms have been evaluated in this section. Different datasets, such as rice, wheat, sunflower and corn, with different dimensions and resolutions, are used to perform several experiments. Information is embedded in images to hide the data and securely transfer it. The experimental results are achieved by using different data sets of crop images. The evaluation is totally dependent on real estimation of the figures, charts, along with the typical measurement parameters such as computational complexity, The mean square error and the maximum signal to ratio of noise. This work will also be helpful for researchers and students to evolve the research related to crop image encryption as well as video encryption in future. A comparison of the above 4 graphs is presented in Fig. 6.

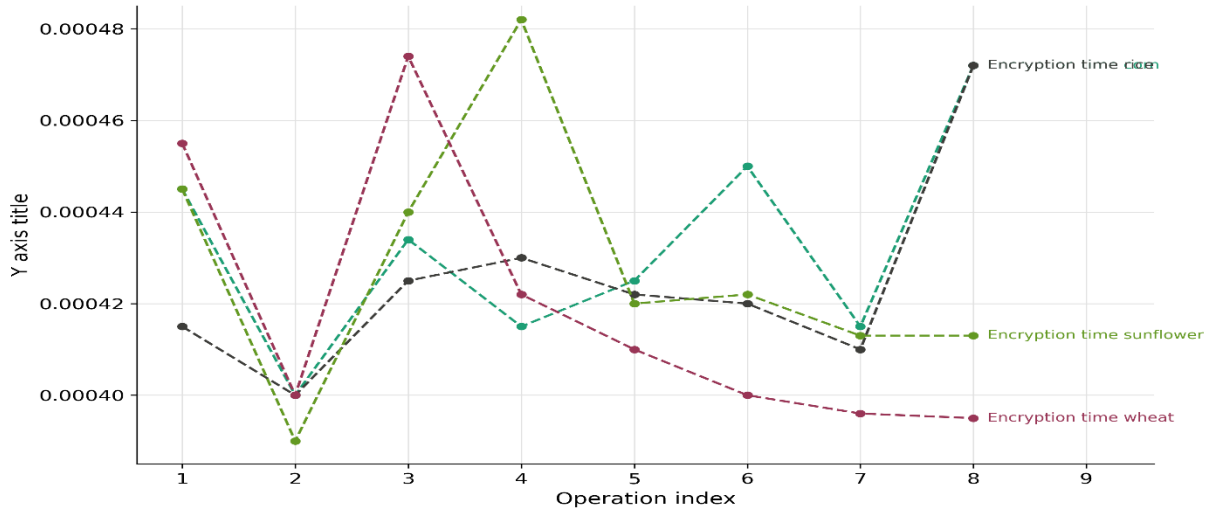

Figure 6. Comparison Encryption time of corn, rice, sunflower and wheat images

To further validate the imperceptibility and embedding quality of the proposed framework, visual comparisons between the original cover images and their corresponding secret images were

conducted. In this context, the cover image serves as the vessel that carries the secret data, while the secret image refers to the information embedded and later extracted from it. The goal of visual steganography is to embed secret data in such a way that the modifications introduced into the cover image remain undetectable to the human eye, preserving both visual integrity and data confidentiality. To achieve this, two primary criteria must be met:

Visual Similarity:
The stego image (cover image with embedded data) should remain visually indistinguishable from the original. Any deviations would compromise the covert nature of the communication.

Capacity and Integrity:
The cover image must have sufficient embedding capacity to hold the secret data without significant degradation in quality. High-resolution images offer greater flexibility in this regard.
The secret image or data, which can be grayscale, a symbol, or encoded text, is first converted to a binary representation before embedding. This process ensures bit-level control and precise manipulation during the embedding phase. To preserve the fidelity of the cover image, only payloads small enough to fit within the available bit space determined during capacity estimation are selected for embedding. Figures 8–11 demonstrate this concept across all four crop datasets used in the study. For each crop, two visualizations are presented:

- The original cover image used for embedding
- The corresponding extracted secret image is recovered after decryption and decoding.

These visualizations confirm the accuracy of the embedding and extraction process. No perceptible artifact are introduced throughout the procedure, into the mask image, and to the hidden image is retrieved with high visual integrity, demonstrating the effectiveness of the hybrid LSB-MSB strategy combined with RC4 encryption.

5. Conclusion

A hybrid security architecture for IoT-enabled agri-care systems is presented in this study that combines adaptive steganography and lightweight encryption to ensure data confidentiality, imperceptibility, and computational efficiency. By embedding sensitive crop-related information within preprocessed agricultural images using a hybrid LSB-MSB technique guided by pseudo-random logic seeded with secret keys, the framework effectively conceals data while preserving image quality, as confirmed by high PSNR and low MSE values. To secure the embedded data, the framework employs the RC4 stream cipher. While RC4 is known to exhibit vulnerabilities in certain cryptographic contexts, its use here is carefully scoped: it operates on already randomized stego-images, minimising exposure to predictable patterns that typically compromise RC4. This layered security strategy aligns with the needs of low-power IoT devices where lightweight encryption remains a practical necessity.
Experimental results across multiple crop datasets validate the framework's robustness, efficiency, and practicality in actual life agricultural monitoring scenarios. In future work, we aim to investigate the integration of advanced cryptographic schemes with stronger theoretical guarantees and enhanced resistance to cryptanalysis, enabling further reinforcement of data security in smart farming infrastructures.

REFERENCES

Ahmed, S., Javaid, N., Qureshi, K. N., & Khan, M. A. (2024). Internet of Things (IoT) for secure and reliable communication in smart agriculture: A survey. Journal of Network and Computer Applications, 234, 103964. https://doi.org/10.1016/j.jnca.2024.103964

Alshamrani A., Alhaidari F., Alghamdi A., Alzahrani B. (2023). Lightweight cryptographic techniques for resource-constrained IoT devices: A review. Electronics, 12(9), 2085. https://doi.org/10.3390/electronics12092085

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Kumar, N. (2022). A safe lightweight authentication protocol for the Internet of Things environments. IEEE Internet of Things Journal, 9(5), 3762–3774.

Boursianis, A. D., Papadopoulou, M. S., Diamantoulakis, P. D., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., Karagiannidis, G. K., Wan, S., & Goudos, S. K. (2023). Smart agriculture and the Internet of Things (IoT): Application, benefits and challenges. Internet of Things, 23, 100821.

Chaudhary, R., Kumar, G., Alazab, M., & Gadekallu, T. R. (2023). Blockchain and Lightweight Crypto for Secure IoT in Agriculture. Future Generation Computer Systems, 145, 410-425.

Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2022). State-of-the-art and future directions toward green IoT based agriculture security and privacy. Computer Networks, 207, 108822.

Gupta, D., Bhatt, C., Gupta, M., & Tosun, A. S. (2022). A survey of lightweight cryptography for IoT and smart agriculture applications. Wireless Personal Communications, 126(2), 1285–1318.

Jabbar, S., Ullah, F., Khalid, S., Khan, M., & Han, K. (2023). Secure IoT architecture for Precision Agriculture with low resource and encryption. Sensors, 23(11), 5059. https://doi.org/10.3390/s23115059

Khan, P. W., Byun, Y. C., Lee, S. J., Kang, Y. T., & Park, N. (2022). Machine learning and Internet of Things for smart agriculture: Security and Privacy aspects Electronics, 11(4), 592.

Kumar R, Tripathi R, Marchang N, Srivastava G. (2024). Enabling data gathering and privacy safeguarding in agriculture IoT. IEEE Access, 12, 54873–54890.

Liu, X., Zhang, Y., Wang, H., & Chen, J. (2023). Lightweight authenticated encryption for resource constrained IoT devices. IEEE Internet of Things Journal, 10(14), 12376–12390.

Mahmood, K., Chaudhry, S. A., Naqvi, H., Shon, T., & Kumari, S. (2023). Lightweight authentication schemes for smart farming environments: A survey. Journal of Information Security and Applications (JISA), 73 (2016): 103407.

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2022). A large-scale IoT deployment in agriculture comparative study of LPWAN technologies. Ad Hoc Networks, 129, 102805.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2023). Recent advances and future research on privacy preserving methods for IOT. IEEE Communications Surveys & Tutorials, 25(2), 1083–1121.

Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2022). Secure communication with the Internet of Things, with lightweight authenticated encryption. ACM Computing Surveys, 55(8), 1–36.

Sharma, V., You, I., Andersson, K., Palmieri, F. (2023). Secure smart agriculture applications in the edge computing architecture. Future Generation Computer Systems, 141, 82-95.

Singh, D., Kumar, V., Verma, A., & Singh, P. (2024). A systematic review of security problems and lightweight cryptographic solutions for precision agriculture IoT. Computers and Electronics in Agriculture, 218 (108595).

Talavera, J. M., Tobón, L. E., Gómez, J. A., Culman, M. A., Aranda, J. M., Parra, D. T., Quiroz, L. A., Hoyos, A., & Garreta, L. E. (2022). An overview of IoT applications for smart agriculture and precision farming. Computers and Electronics in Agriculture, 196, 106878.

Wazid, M., Das, A. K., Rodrigues, J. J. P. C., Shetty, S., & Park, Y. (2023). Recent advancement in lightweight authentication and key management for IoTs. IEEE Access, 11, 11352–11382.

Yadav, G., Kumar, N., & Raw, R. S. (2024). Secure data sharing framework for smart agriculture with privacy preserving and based on blockchain and lightweight cryptography. Journal of King Saud University – Computer and Information Sciences, 36(3): 102031.

Zhang, Y., Ren, J., Liu, Y., & Shen, X. (2023). Agricultural Internet of Things: Secure and Privacy-preserving data collection via edge computing. IEEE Transactions on Industrial Informatics, 19(7), 8215–8227.

Zhou, H., Xu, L. D., Zhao, S., & Wang, C. (2022). Use of edge intelligence to secure IoT solutions for precision agriculture. IEEE Network, 36(6), 182–189.

23.Abduljabbar, Z. A., Nyangaresi, V. O., Jasim, H. M., Ma, J., Hussain, M. A., Hussien, Z. A., & Aldarwish, A. J. Y. (2023). Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability (Switzerland), 15(13). https://doi.org/10.3390/su151310264

24.Asif, Md. R. A., Hasan, K. F., Islam, M. Z., & Khondoker, R. (2021). STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems. 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI), 1–6. https://doi.org/10.1109/STI53101.2021.9732597

25.Clemente-Lopez, D., Rangel-Magdaleno, J. de J., & Muñoz-Pacheco, J. M. (2024). A lightweight chaos-based encryption scheme for IoT healthcare systems. Internet of Things, 25, 101032. https://doi.org/10.1016/j.iot.2023.101032

26.Dev, B. P. V., & Prasad, K. V. (2023). An Adaptive Lightweight Hybrid Encryption Scheme for Securing the Healthcare Data in Cloud-Assisted Internet of Things. Wireless Personal Communications, 130(4), 2959–2980. https://doi.org/10.1007/s11277-023-10411-6

27.Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access, 7, 156237–156271. https://doi.org/10.1109/ACCESS.2019.2949703

28.Fathy, C., & Ali, H. M. (2023). A Secure IoT-Based Irrigation System for Precision Agriculture Using the Expeditious Cipher. Sensors, 23(4), 1–16. https://doi.org/10.3390/s23042091

29.Haseeb, K., Din, I. U., Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. Sensors (Switzerland), 20(7). https://doi.org/10.3390/s20072081