The International Society of Precision Agriculture presents the
16th International Conference on
Precision Agriculture
21–24 July 2024 | Manhattan, Kansas USA

Securing Agricultural Data with Encryption Algorithms on Embedded GPU-based Edge Computing Devices

Mohammad Ashik Alahe[1], James Kemeshi[1], Young Chang[1, *], Kwanghee Won[2], Xufei Yang[1], Mazhar Sher[1]

[1]Department of Agricultural and Biosystems Engineering, South Dakota State University, Brookings, SD 57007, USA

[2]Department of Electrical Engineering and Computer Science, South Dakota State University, Brookings, SD 57007, USA

[*]Corresponding Author

A paper from the Proceedings of the
16th International Conference on Precision Agriculture
21-24 July 2024
Manhattan, Kansas, United States

Abstract

Smart Agriculture (SA) has captured the interest of both agricultural businesses and scientific communities in recent years. Overall, SA aims to help the agricultural and food industry avoid crop failures and loss of revenues while using inputs (such as fertilizers and pesticides) more efficiently by utilizing Internet of Things (IoT) devices and computing systems. However, rapid digitization and reliance on data-driven technologies create new security threats that can defeat this goal in the absence of adequate awareness and proper countermeasures. In addition, due to their low memory and power capabilities, many smart devices cannot be safeguarded using traditional cyber security protocols. In a world where data is a valuable asset, securing agricultural data with encryption algorithms on edge computing devices not only strengthens the foundation of data protection, but also paves the way for a resilient and data-driven future in agriculture, ensuring its long-term growth and prosperity in the digital age. Therefore, designing a robust and efficient secure framework for addressing the security challenges faced by the agriculture industry is essential to protect the industry and maintain food security. This study presents a novel approach to secure agricultural data using encryption technology on Embedded GPU-based edge computing devices. In this proposed study, we combined the Jetson Nano's capabilities with advanced encryption techniques, namely Advanced Encryption Standard (AES) to form a

The authors are solely responsible for the content of this paper, which is not a refereed publication. Citation of this work should state that it is from the Proceedings of the 16th International Conference on Precision Agriculture. EXAMPLE: Last Name, A. B. & Coauthor, C. D. (2024). Title of paper. In Proceedings of the 16th International Conference on Precision Agriculture (unpaginated, online). Monticello, IL: International Society of Precision Agriculture.

compelling strategy to combat evolving cybersecurity threats in smart agriculture. We installed a Camera Serial Interface (CSI) camera on the Unmanned Ground Vehicle (UGV) to capture real-time data. Our proposed framework successfully secured the agricultural data using the AES encryption algorithms. In addition, we will implement this approach on Jetson Xavier NX to compare the performance of these two-edge computing devices in terms of cost-effectiveness, processing time and power consumption. Other encryption algorithms, including Rivest-Shamir-Adleman (RSA), Homomorphic Encryption (HE), Elliptic Curve Cryptography (ECC), and Selective Encryption (SE) combined with 2-D Discrete Wavelet Transform (DWT) will also be utilized to compare the performance of our proposed systems with these encryption techniques. This framework provided full control of real time image acquisition, image processing, image encryption and decryption, and image transmission. The proposed framework demonstrated computational efficiency and resilience against resource exhaustion and cyberattacks.

Keywords.
Smart Agriculture, Internet of Things, Image Encryption, Edge Computing, Jetson Nano.

1 Introduction

Agriculture is the major economic activity across the world as well as the most important provider of food currently. Considering today’s ongoing human population expansion, climate change, and limited food supply, global food security is seen as a challenging task. The Food and Agriculture Organization (FAO) estimates that by 2050, there will be a 70% rise in food demand (Gupta et al., 2020; Rettore de Araujo Zanella et al., 2020; Yazdinejad, Zolfaghari, et al., 2021). In addition, it will be more difficult to meet the global demand because arable land areas, as well as natural resources, will decrease with the population increase (Canton, 2021). To keep pace with these issues we need to improve our cultivation process and adopt cutting-edge technologies.

A cutting-edge framework currently referred to as Smart Agriculture, Precision Agriculture, or Agriculture 4.0 is made possible by the fourth industrial revolution and IoT-based systems. Farmers are able to go from field-level management to plant-by-plant or even square-meter-based customized control by utilizing precision agriculture (PA). A variety of technologies have been used to enable PA and Smart Farming (SF), such as artificial intelligence (AI) (Chukkapalli et al., 2020), wireless sensor networks (WSN) (Bayrakdar, 2019), fog computing systems (Malik et al., 2020), and unmanned aerial vehicles (UAVs) (Bacco et al., 2018; Chebrolu et al., 2018). The IoT appears to be a critical technology for both PA (Ahmed et al., 2018) and SF (Huang et al., 2020; Shabadi, 2018; Verdouw et al., 2021). This is because of its remote sensing and autonomous operation capabilities. According to Demestichas et al. (2020) and Roopaei et al. (2017), these IoT-based technologies do, however, bring with them new cybersecurity threats and vulnerabilities. These vulnerabilities could be exploited to gain control over actuators, sensors, and other on-field components, as well as the associated databases and applications, and autonomous vehicles (such as tractors, drones, sprayers, and planters) (Demestichas et al., 2020; Roopaei et al., 2017; Yazdinejad, Parizi, et al., 2021).

Due to the distinctive characteristics of IoT devices, such as heterogeneity, mobility, and resource limitations, the security element of Smart Farming (Chae & Cho, 2018; Gupta et al., 2020; West, 2018) and Precision Agriculture (Chi, 2017; Grgic, 2013; Window, 2019) presents important issues. These characteristics make SF and PA vulnerable to a variety of cybersecurity threats. For instance, illegal data modifications might lead a farmer to make decisions that are bad for the welfare of his or her agricultural land. A serious economic consequence, such as revenue loss and crop failure, will result from the farm owner's inability to take necessary activities, such as targeted pesticide spraying, irrigation changes, and fertilizer application. Therefore, securing sensitive agricultural data is important to protect the smart agricultural framework from a variety of cyber-attacks and maintain food security for rapidly increasing populations.

In recent times, there has been an inadequate amount of study on agricultural data security, despite the implementation of various methodologies used in some studies. Therefore, this study suggested an innovative embedded GPU-based agricultural data security framework that facilitates the utilization of Advance Encryption Standard (AES) encryption algorithms. This study's primary contribution is the development and evaluation of the embedded GPU framework's robustness, which is intended to secure agricultural data by safeguarding its authenticity and integrity. We will secure real-time image data using AES encryption technique. In addition, we will use two different embedded GPU systems including Jetson Nano and Jetson Xavier NX to compare the performance of our proposed system with AES encryption techniques. The remaining portions of this study are organized as follows: Section 2 represents the overview of the proposed system and methodologies for performance evaluation. Section 3 includes the statistical analysis results and comparison of two different GPU systems and in Section 4, we conclude the paper.

2 Materials and Methods

2.1 Description of the Proposed System

In this subsection, we will provide the description of our proposed framework. Fig 1 represents the overall workflow for securing real-time agricultural data using edge computing devices. The proposed framework incorporates a variety of components including a CSI camera, Jetson Nano, or Jetson Xavier NX, a display monitor, and a Wi-Fi module. We installed the CSI camera on the embedded GPU for capturing the real time agricultural data and applied AES encryption algorithm (AES128) immediately to secure the captured image data. OpenCV is used throughout the encryption process, which is executed in the Python environment. To make encryption and decryption processes easier, we have loaded a number of Python libraries. Subsequently, we transferred these secured images to the base station computer for storage. Finally, an end user can retrieve important information about their land by using the decryption process and make decision based on the retrieved data.

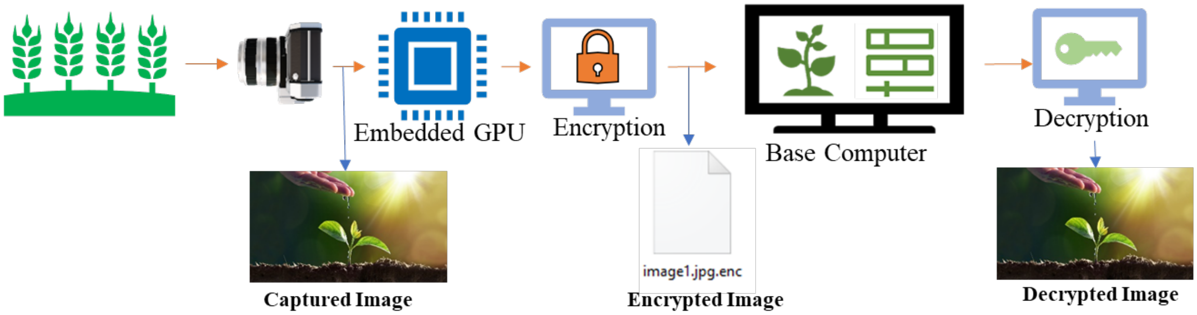


Fig 1. Overall process for securing agricultural data using edge computing devices.

2.2 Design and Development of Proposed Framework

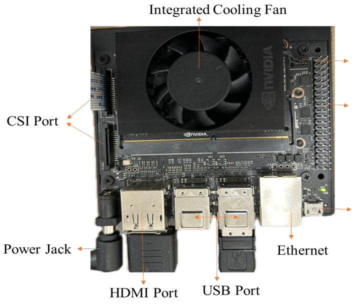
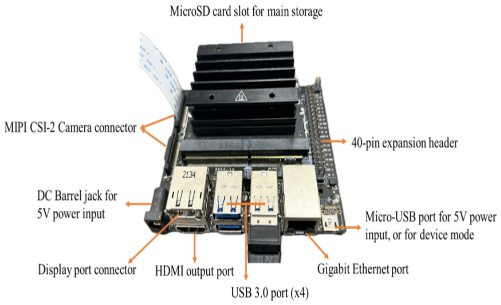
2.2.1 Real-time Data Collection

Our proposed framework involves capturing the real time image data using the CSI camera installed on the Embedded GPUs. We captured images for different frame rates, including 10, 20 and 24 fps, with each image set to a size of 1920×1080 pixels. Afterward, the captured data is processed in the embedded GPU such as Jetson Nano or Jetson Xavier NX.

2.2.2 Overview of Embedded GPU-based Systems

In this study, we utilized two different embedded GPU-based systems for processing real-time images using AES128 encryption algorithms. However, there are some key differences between these two systems in terms of GPU cores, tensor cores, CPU, clock speed, memory, AI performance, and power consumption. Table 1 represents the brief comparison between these two systems.

Table 1. Key differences between Jetson Nano and Jetson Xavier NX.

Feature	Jetson Nano	Jetson Xavier NX
GPU Cores	128 CUDA cores	384 CUDA cores
CPU	Quad-core ARM Cortex-A57	Six-core NVIDIA Carmel ARMv8.2 CPU
Tensor Cores	N/A	48 Tensor Cores
Memory	4GB LPDDR4	8GB LPDDR4x + 16GB eMMC
CPU Clock Speed	1.43 GHz	Up to 1.91 GHz
AI Performance	472 GFLOPs	21Tops (Tensor Operation Per Second)
Power Consumption	5-10W	10-15W
Outlook	 Integrated Cooling Fan CSI Port Power Jack HDMI Port USB Port Ethernet	 MicroSD card slot for main storage MIPI CSI-2 Camera connector 40-pin expansion header DC Barrel jack for 5V power input Micro-USB port for 5V power input, or for device mode Display port connector HDMI output port USB 3.0 port (x4) Gigabit Ethernet port

2.2.3 Encryption and Decryption

Fig 2 illustrates how the image is encrypted and turned to cipher text using the encryption key; the decryption key is required to decode the image back to its original form. Encryption algorithms are a type of mathematical model used in cryptography that is typically used for this operation. In this study, we utilized AES encryption techniques for securing agricultural data.

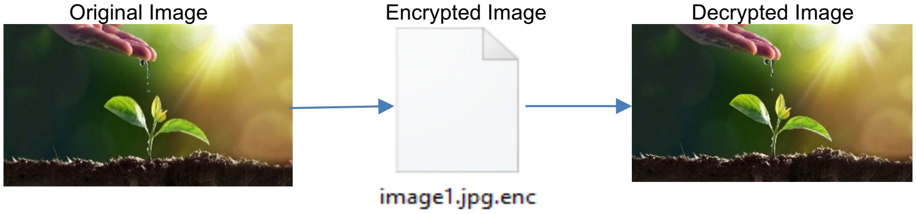


Fig 2. Encryption and decryption for securing data.

2.3 Performance Evaluation

The objective of this research is to evaluate the efficiency of two computing systems, the Jetson Nano and Jetson NX, by comparing their overall processing times for encrypting and decrypting real-time image data at various frame rates. Furthermore, a two-sample t-test will be utilized to assess if there is a statistically significant difference in the mean processing time of the two systems.

The null and alternative hypotheses for the t-test are,

$$H_0\ (\mu_1 = \mu_2)\text{: There is no significant difference between these two systems.}$$

$$H_1\ (\mu_1 \neq \mu_2)\text{: There is a significant difference between these two systems.}$$

Where, $\mu_1$and μ_2 are the population means of the two groups being compared.

Finally, we will compute the average and standard deviation (SD) for each embedded GPU system, providing valuable perspectives on the data's central tendency and variability.

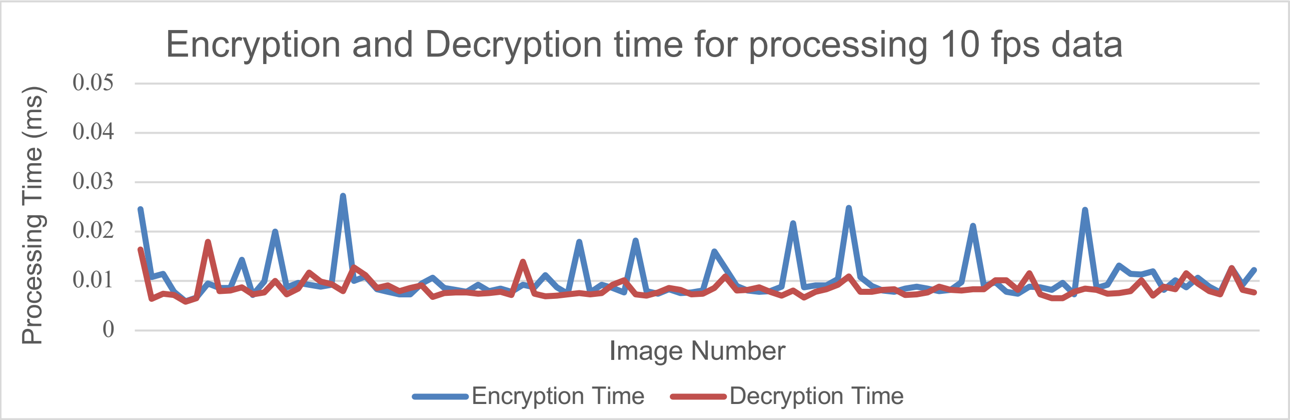
3 Results and Discussion

We successfully captured the real time data using the CSI camera installed on the embedded systems for different frame rates such as 10, 20, and 24 fps. Then our proposed framework with both the embedded GPU systems successfully secured the real time captured data using AES encryption technique. Table 2 represents the statistical data that is utilized to compare the performance of Jetson Nano and Xavier NX based on the processing time and standard deviation.

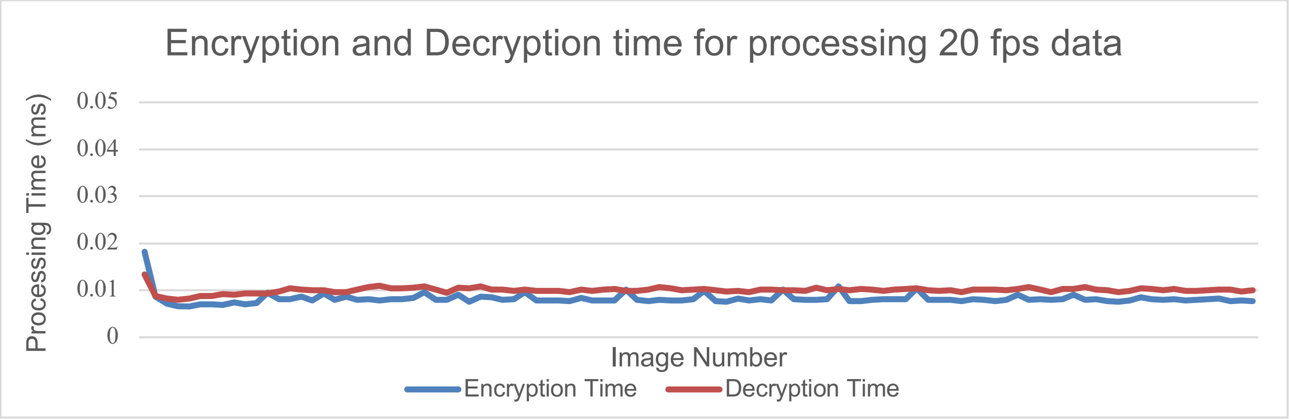
Table 2. Performance evaluating statistical data of Jetson Nano and Xavier NX.

Performance Evaluation Matrices	10 fps		20 fps		24 fps	
	Jetson Nano	Xavier NX	Jetson Nano	Xavier NX	Jetson Nano	Xavier NX
Mean Encryption time (ms)	10.299	7.553	8.208	9.639	9.839	7.447
Mean Decryption time (ms)	8.535	9.404	10.012	8.391	8.484	9.272
Average processing time (ms)	18.833	16.957	18.22	18.03	18.317	16.718
Standard Deviation for Encryption time (ms)	4.178	0.778	1.239	4.425	4.635	0.882
Standard Deviation for Decryption time (ms)	1.906	0.525	0.617	1.82	1.997	1.002

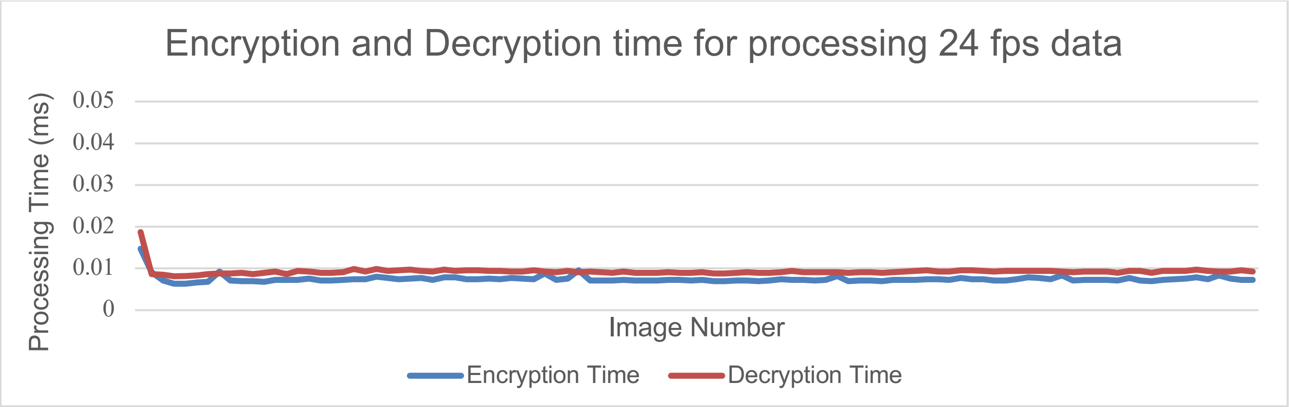
From Table 2, we can see that the mean processing time taken by our proposed system for processing 10 fps image data was 18.833ms (10.299ms for encryption and 8.535ms for decryption) and standard deviation of encryption and decryption time was 4.178ms and 1.906ms. For processing 20 fps image data, the mean processing time was 18.22ms (8.208ms for encryption and 10.012ms for decryption) and standard deviation of encryption and decryption time was 1.239ms and 0.617ms. The mean processing time was 18.317ms (9.839ms for encryption and 8.484ms for decryption) with standard deviation of 4.635ms and 1.997ms for encrypting and decrypting the 24 fps image data. Fig 3 represents the encrypting and decrypting time taken by the Jetson Nano for processing (a) 10, (b) 20 and (c) 24 fps data.



(a)



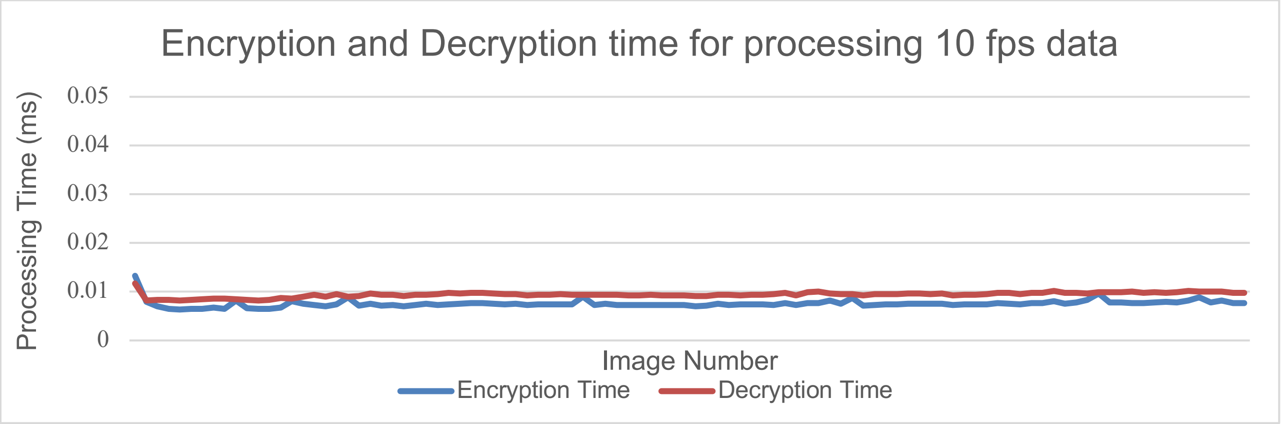
(b)



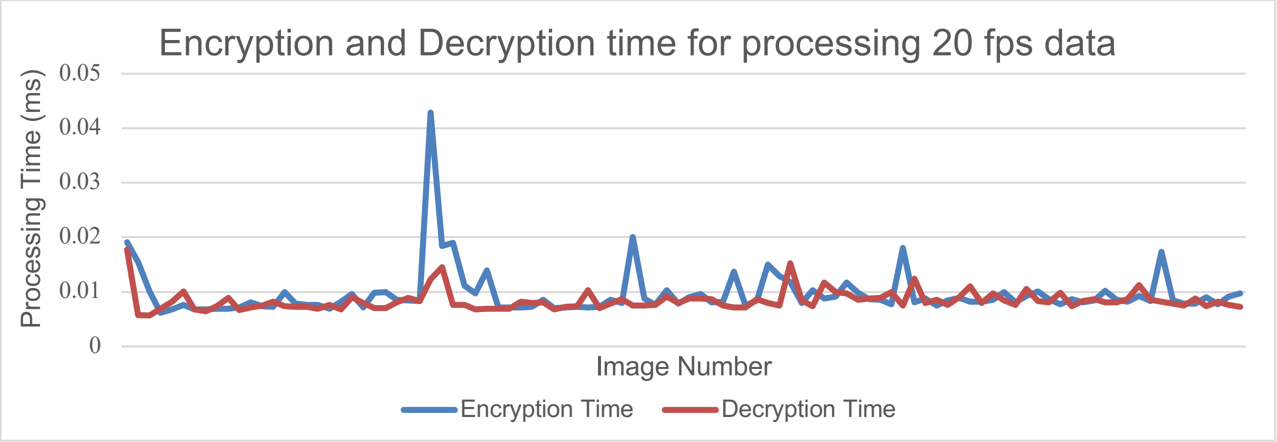
(c)

Fig 3. Encryption and decryption time taken by the Jetson Nano to process (a) 10, (b) 20 and (c) 24 fps data.

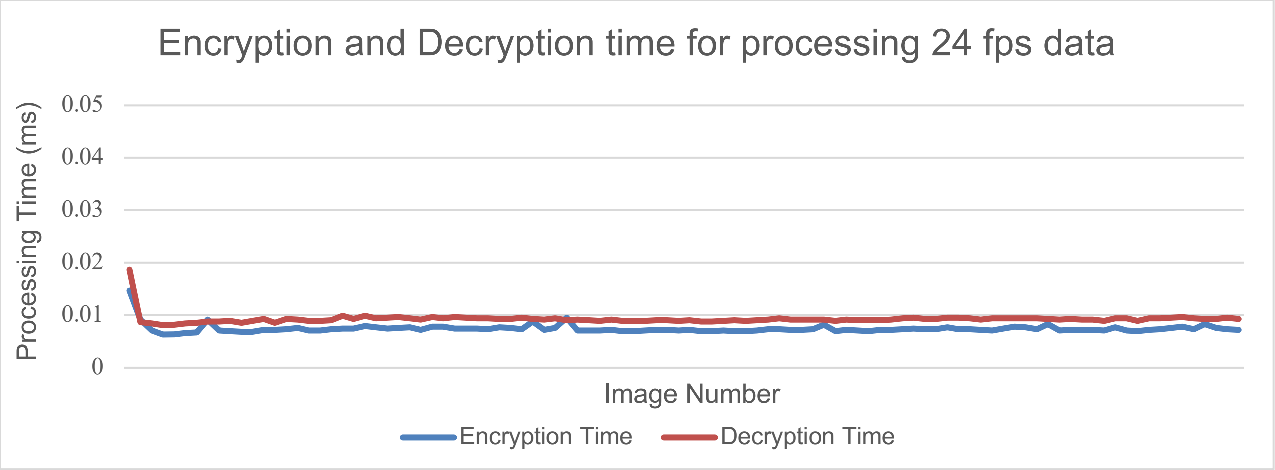
Fig 4 represents the encrypting and decrypting time taken by the Jetson Nano for processing (a) 10, (b) 20 and (c) 24 fps data. For processing 10 fps image data, the mean processing time was 16.957ms (7.553ms for encryption and 9.404ms for decryption) and standard deviation of encryption and decryption time was 0.778ms and 0.525ms. For processing 20 fps image data, the mean processing time was 18.03ms (9.639ms for encryption and 8.391ms for decryption) and standard deviation of encryption and decryption time was 4.425ms and 1.82ms. The mean processing time was 16.718ms (7.447ms for encryption and 9.272ms for decryption) with standard deviation of 0.882ms and 1.002ms for encrypting and decrypting the 24 fps image data.



(a)



(b)



(c)

Fig 4. Encryption and decryption time taken by the Jetson Xavier NX to process (a) 10, (b) 20 and (c) 24 fps data.

Jetson Xavier NX outperformed Jetson Nano in terms of mean and standard deviation value of processing time (encryption and decryption) for 10 fps, 20 fps and 24 fps data.

Table 3. t-test results of encryption time for comparing the two systems.

	10 fps	20 fps	24 fps
t- statistics	5.3160	3.6345	3.8311
p - value	< 0.001	0.00168	0.001028
Conclusion	Reject null hypothesis: There is a significant difference between the systems.	Reject null hypothesis: There is a significant difference between the systems.	Reject null hypothesis: There is a significant difference between the systems.

Table 4. t-test results of decryption time for comparing the two systems.

	10 fps	20 fps	24 fps
t- statistics	13.8027	- 6.3767	- 6.8121
p - value	< 0.001	< 0.001	< 0.001
Conclusion	Reject null hypothesis: There is a significant difference between the systems.	Reject null hypothesis: There is a significant difference between the systems.	Reject null hypothesis: There is a significant difference between the systems.

Tables 3 and 4 represent the t-test result for encryption time and decryption time between the Jetson Nano data and Jetson Xavier NX data. From table 1, we see that the p – value is always less than the alpha (0.05), resulting in rejection of the null hypothesis. That means that there is a significant difference between these two systems.

4 Conclusion

The Jetson Nano and Jetson Xavier NX were utilized in our proposed system to effectively capture, encrypt, and decrypt the image data. The t-test indicates a substantial difference between these two systems. Figs 3 and 4 show that for 10, 20, and 24 frames per second data, the Jetson Xavier NX outperformed the Jetson Nano in terms of processing time (total time for encrypting and decrypting the real-time images). All the experiments were performed in the lab.

In the future, we plan to test and assess the resilience of our suggested system using field data. Additionally, to carry out the entire procedure, including real-time agricultural data collecting, encryption, and decryption, we will deploy our proposed framework on the unmanned ground vehicle. We are currently developing an embedded GPU system that uses Field Programmable Gate Arrays (FPGA) and is reasonably cost-effective. This FPGA-based integrated GPU will be used to secure the Ag and evaluate its resilience instead of the Jetson Nano and Xavier NX. Additionally, in order to assess the performance of the systems, we will apply additional encryption methods, such as 2-D Discrete Wavelet Transform (DWT) combined with Selective Encryption (SE), Rivest-Shamir-Adleman (RSA), Homomorphic Encryption (HE), and Elliptic Curve Cryptography (ECC). Afterward, we plan to transfer and store the encrypted data on the cloud, enabling the user to access it anytime they want to perform any kind of activity, such as applying fertilizer, adjusting irrigation, or spraying certain chemicals.

Acknowledgment

This research was funded by (1) the State of South Dakota - HB1092 SDSU & DSU CyberAg partnership initiative (3A1302) and (2) the Hatch Project (3AH777) and (3) Multi Hatch Project (3AR730) by USDA NIFA through South Dakota Agricultural Experimental Station at South Dakota State University.

Reference

Ahmed, N., De, D., & Hussain, I. (2018). Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas. IEEE Internet of Things Journal, 5(6), 4890–4899. https://doi.org/10.1109/JIOT.2018.2879579

Bacco, M., Berton, A., Gotta, A., & Caviglione, L. (2018). IEEE 802.15.4 Air-Ground UAV Communications in Smart Farming Scenarios. IEEE Communications Letters, 22(9), 1910–1913. https://doi.org/10.1109/LCOMM.2018.2855211

Bayrakdar, M. E. (2019). A Smart Insect Pest Detection Technique With Qualified Underground Wireless Sensor Nodes for Precision Agriculture. IEEE Sensors Journal, 19(22), 10892–10897. https://doi.org/10.1109/JSEN.2019.2931816

Canton, H. (2021). Food and Agriculture Organization of the United Nations—FAO. In The Europa Directory of International Organizations 2021. https://doi.org/10.4324/9781003179900-41

Chae, C.-J., & Cho, H.-J. (2018). Enhanced secure device authentication algorithm in P2P-based smart farm system. Peer-to-Peer Networking and Applications, 11(6), 1230–1239. https://doi.org/10.1007/s12083-018-0635-3

Chebrolu, N., Labe, T., & Stachniss, C. (2018). Robust Long-Term Registration of UAV Images of Crop Fields for Precision Agriculture. IEEE Robotics and Automation Letters, 3(4), 3097–3104. https://doi.org/10.1109/LRA.2018.2849603

Chi, H. and W. S. and V. E. and K. E. (2017). A framework of cybersecurity approaches in precision agriculture. Proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance, 90–95.

Chukkapalli, S. S. L., Mittal, S., Gupta, M., Abdelsalam, M., Joshi, A., Sandhu, R., & Joshi, K. (2020). Ontologies and Artificial Intelligence Systems for the Cooperative Smart Farming Ecosystem. IEEE Access, 8, 164045–164064. https://doi.org/10.1109/ACCESS.2020.3022763

Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on security threats in agricultural iot and smart farming. In Sensors (Switzerland) (Vol. 20, Issue 22). https://doi.org/10.3390/s20226458

Grgic, K. and Z. D. and K. V. (2013). Security in IPv6-based wireless sensor network — Precision agriculture example. Proceedings of the 12th International Conference on Telecommunications, 79–86.

Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and Privacy in Smart Farming: Challenges and Opportunities. IEEE Access, 8. https://doi.org/10.1109/ACCESS.2020.2975142

Huang, K., Shu, L., Li, K., Yang, F., Han, G., Wang, X., & Pearson, S. (2020). Photovoltaic Agricultural Internet of Things Towards Realizing the Next Generation of Smart Farming. IEEE Access, 8, 76300–76312. https://doi.org/10.1109/ACCESS.2020.2988663

Malik, A. W., Rahman, A. U., Qayyum, T., & Ravana, S. D. (2020). Leveraging Fog Computing for Sustainable Smart Farming Using Distributed Simulation. IEEE Internet of Things Journal, 7(4), 3300–3309. https://doi.org/10.1109/JIOT.2020.2967405

Rettore de Araujo Zanella, A., da Silva, E., & Pessoa Albini, L. C. (2020). Security challenges to smart agriculture: Current state, key issues, and future directions. Array, 8. https://doi.org/10.1016/j.array.2020.100048

Roopaei, M., Rad, P., & Choo, K. K. R. (2017). Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging. IEEE Cloud Computing, 4(1). https://doi.org/10.1109/MCC.2017.5

Shabadi, L. S. and B. H. B. (2018). Design and implementation of IOT based smart security and monitoring for connected smart farming. International Journal of Computer Applications, 975(8887).

Verdouw, C., Tekinerdogan, B., Beulens, A., & Wolfert, S. (2021). Digital twins in smart farming. Agricultural Systems, 189, 103046. https://doi.org/10.1016/j.agsy.2020.103046

West, J. (2018). A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. Journal of Agricultural & Food Information, 19(4), 307–330. https://doi.org/10.1080/10496505.2017.1417859

Window, M. (2019). Security in precision agriculture: Vulnerabilities and risks of agricultural systems.

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Karimipour, H. (2021). Federated learning for drone authentication. Ad Hoc Networks, 120, 102574. https://doi.org/10.1016/j.adhoc.2021.102574

Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A. G., Russell, C., & Duncan, E. (2021). A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. Applied Sciences (Switzerland), 11(16). https://doi.org/10.3390/app11167518