Poster: FusionCrypt: Enhancing Image Security Through Hybrid Encryption

1st Rahool Dembani
R&D and Innovation Department
SingularLogic
Athens, Greece
rdembani@singularlogic.eu

2nd Ioannis Karvelas
R&D and Innovation Department
SingularLogic
Athens, Greece
ikarvelas@singularlogic.eu

3rd Stamatia Rizou
R&D and Innovation Department
SingularLogic
Athens, Greece
srizou@singularlogic.eu

4th Domenico Tegolo
Department of Mathematics and Computer Science
University of Palermo
Palermo, Italy
domenico.tegolo@unipa.it

***Abstract*—In the digital age, securing image data, particularly in agriculture, is critical to prevent unauthorized access and tampering. This paper presents FusionCrypt, a hybrid encryption system specifically designed for the images of agriculture. The approach incorporates Particle Swarm Optimization (PSO), Elliptic Curve DiffieHellman (ECDH) key exchange, chaotic maps, and Dynamic Intra-block to enhance the robustness of the encryption. Combining two or more maps, such as the Henon and Logistic maps, referred to as sequential map fusion, produces dynamic keys. Also, ECDH provides a secure mechanism for key exchanges needed for applications in distributed farming. Furthermore, a permutation based approach is employed to improve the correctness of the mapping, which makes it feasible to high-resolution images of the crops and soil conditions. Several measures, such as entropy, correlation coefficients, NPCR, UACI, PSNR, and SSIM, that focus on the extent of security risk have been tested on agricultural data sets to assess the framework's efficiency. Preliminary results ensure significant enhancement in encryption strength and resistance against cryptographic attacks related to the confidentiality and integrity of critical agricultural data.**

***Index Terms*—Hybrid image encryption, Chaotic maps, Elliptic Curve Diffie-Hellman (ECDH), Particle Swarm Optimization (PSO), Smart Farming.**

I. Introduction

In the era of smart farming and precision agriculture, the secure transmission and storage of agricultural image data is paramount. These images, vital for crop health monitoring, pest detection, and soil analysis, often contain sensitive information. Unlike general images, agricultural images typically exhibit high degrees of spatial redundancy due to repetitive patterns (e.g., rows of crops, uniform fields) and specific color ranges (e.g., foliage health indicators). These characteristics make them particularly susceptible to statistical and differential attacks if not properly encrypted, amplifying the risks of unauthorized access and tampering in critical agricultural operations. Thus, efficient image encryption techniques are necessary to protect confidential visual information from possible attacks.

To protect information over a wide range of areas, encrypted data has been widely used with the help of the Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), and other traditional encryption algorithms. However, conventional cryptographic algorithms like AES, designed primarily for text, often struggle with image data. Images possess inherent characteristics such as high redundancy and strong spatial/statistical correlations, which, if not properly addressed, can lead to vulnerabilities when these algorithms are applied directly [1], [2]. Lightweight scrambling methods can help, but a robust hybrid approach is often necessary for strong security against advanced attacks. Chaotic systems have become effective at constructing image encryption schemes due to their sensitivity, deterministic random properties, and ergodicity [3]. The use of chaotic maps allows the ability to create pseudo random sequences that can be used to potentially enhance security through the generation of random images, which can easily scramble image pixels [4]. Chaotic maps such as the Henon map, Logistic map, Arnold's cat map, and others have been used in numerous encryption algorithms suggesting their plausibility in producing complex cipher images [5], [6].

The encoded image benefits are accompanied by chaos-based scheme limitations, including key space constraints, vulnerability against selected types of cryptanalysis, and also issues of key distribution and management [7]. In order to avoid these disadvantages, the applied chaotic systems are combined with traditional cryptographic algorithms, forming hybrid encryption schemes [8]. These hybrid methods seek to take advantage of the strong security features of standard algorithms like AES while gaining some measure of complexity due to utilizing chaos systems [9]. In addition, Particle Swarm Optimization (PSO) has been looked into as a means of strengthening image encryption [10]. PSO can address the encryption algorithm parameters and permutation sequences within the algorithm, thus enhancing the diffusion

and confusion characteristics necessary for secure encryption [11]. For example, [12] seen that the hybrid chaotic map was used to encode the parameters of the chaotic system to encrypt an image, which improved encryption metrics. Securely exchanging keys is also important for encryption algorithms, especially so in decentralized and networked settings common in modern agricultural systems. The growing key size security level afforded by ECDH systems has eluded the attention of many users. ECDH is seen as a viable cost, cost effective and fast alternative in key exchanges [13]. The inclusion of ECDH with the image encryption scheme is an advancement for the system by assuring that the encryption keys are exchanged securely [14].

Considering the reliance on image data in the farming sector, it is necessary to formulate a strategy that will help secure the appropriate information. This work is aimed at improving the existing chaotic-based image encryption algorithms with drawbacks in key management and cryptanalysis resistance through a new hybrid image encryption algorithm. This work outlines FusionCrypt, a new hybrid encryption scheme designed for agricultural images. In contrast to the conventional methods of encryption, FusionCrypt employs a combined use of a Henon and Logistic chaotic maps through Sequential Map Fusion (SMF) to create keys that are highly unpredictable keys. The use of Particle Swarm Optimization (PSO) for image permutation overcomes the inherent semi-redundancy and spatial correlation that is typical of agricultural images, and the use of Elliptic Curve DiffieHellman (ECDH) ensures secure key exchanges with other parties. This holistic approach improves encryption capability while at the same time providing an effective means of managing keys; thus, FusionCrypt extends the scope of cryptographic techniques applicable in the context of smart farming systems.

II. Methodology

FusionCrypt utilizes Elliptic Curve Diffie-Hellman (ECDH) for secure and efficient key exchange, enabling the generation of shared AES-256 keys without transmitting them directly. Dynamic and unpredictable keys are generated through Sequential Map Fusion (SMF), integrating the outputs of Henon and Logistic chaotic maps. To effectively disrupt the inherent spatial correlations and redundancy typical of agricultural images, Particle Swarm Optimization (PSO) is employed to optimize the permutation of image subblocks, maximizing entropy and randomness. The encryption process further involves dynamic intra-block operations, including segmentation, SMF driven RGB channel reordering, application of the PSO-optimized permutation map, XORing with a key-derived random matrix, and final encryption using AES-256-GCM to ensure both confidentiality and data integrity.

III. Results

The hardware specifications included an Intel Core i7 processor with 16GB RAM. The experiments were conducted using Python (v. 3.12.4) using the OpenCV, NumPy, and Cryptography libraries. The test was done at first with 3 different agricultural images which were resized to 500x500 pixels each. These images were likely chosen because they represent common scenarios in smart agriculture, such as farm monitoring and soil analysis. Though the initial findings show the promise of the system, work in further studies will involve testing FusionCrypt on larger image datasets with wider varieties of image types, image resolutions, and sets of agricultural mechanisms to validate its effectiveness and expansion possibilities.

A. Visual Analysis

Figure 1 shows the RGB color distributions of original, encrypted, and decrypted images. The encrypted image's uniform histogram reflects effective obfuscation of patterns, while the decrypted image's histogram closely matches the original, demonstrating FusionCrypt ability to secure data without compromising its integrity

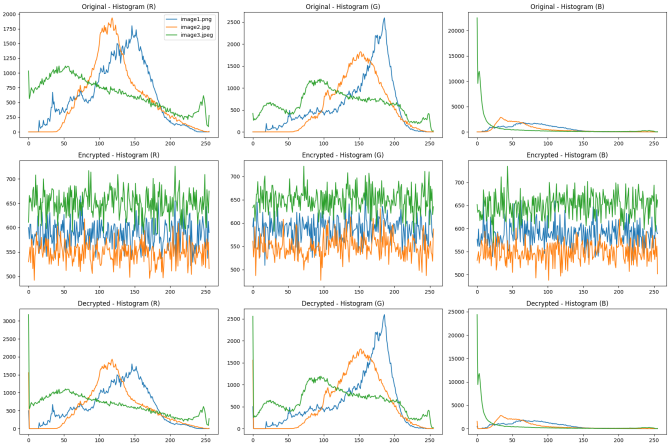

Fig. 1. Histograms of plain and encrypted images

B. Security Analysis

Entropy, a metric describing the randomness or unpredictability in an image, is critical for cryptographic security. For an ideal encrypted image, entropy should approach 8 bits per pixel, as greater entropy correlates with stronger resistance to statistical attacks. Our analysis in Table 1 confirms FusionCrypt's effectiveness in producing high-entropy outputs, with encrypted images exhibiting values between 7.9988 and 7.9991 extremely close to the theoretical maximum. Additionally, FusionCrypt disrupts pixel correlations, a key vulnerability in decryption attempts. As shown in Table 2, the correlation coefficients of encrypted images drop to near-zero values (-0.0005 and -0.0010), confirming that the algorithm effectively eliminates pixel interdependencies. By achieving near maximal entropy and minimizing pixel correlations, FusionCrypt demonstrates robust security against statistical and pattern based attacks.

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) measure the sensitivity to small changes in the plaintext. High values of NPCR (approximately 99%) and UACI (25–35%) point to considerable

TABLE I
ENTROPY VALUES OF ORIGINAL, ENCRYPTED, AND DECRYPTED IMAGES.

Image	Original	Encrypted	Decrypted
Image1	7.0891	7.9988	7.0745
Image2	6.7906	7.9991	6.7514
Image3	5.7620	7.9990	5.7144

TABLE II
CORRELATION COEFFICIENTS OF IMAGES

Image1	Original	0.9822	0.9767	0.9678
	Encrypted	0.0023	0.0012	0.0025
	Decrypted	0.9825	0.9689	0.9601
Image2	Original	0.9029	0.9382	0.9000
	Encrypted	0.0024	0.0023	-0.0005
	Decrypted	0.9045	0.9305	0.8871
Image3	Original	0.9534	0.9677	0.9357
	Encrypted	-0.0011	0.0041	-0.0010
	Decrypted	0.9511	0.9671	0.9326

changes in pixels and intensity. Our findings in Table 3 illustrate that FusionCrypt is quite sensitive to the changes in plaintext, which enables it to withstand differential attacks.

TABLE III
NPCR AND UACI VALUES INDICATING SENSITIVITY TO PLAINTEXT CHANGES.

Image	NPCR (%)	UACI (%)
Image1	99.5894	29.1633
Image2	98.7708	25.2975
Image3	99.6102	35.9727

TABLE IV
PERFORMANCE METRICS.

Image	PSNR (dB)	SSIM	Enc Time (s)	Dec Time (s)
Image1	33.5826	0.9971	2.1240	0.1002
Image2	27.4899	0.9911	2.0554	0.0933
Image3	29.5313	0.9925	2.3073	0.0997

A conventional way of measuring the quality of images has been based on the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). In Table 4, the achieved image quality parameters of PSNR (27.49 to 33.58 dB) and SSIM (0.9911 to 0.9971) suggest that FusionCrypt does not distort the images after decryption, allowing correct data restoration.

IV. RESULTS

This work proposes a hybrid image encryption system for an agricultural imaging framework that effectively integrates chaotic maps, ECDH key exchange, Dynamic Intra-block, and PSO-based permutation to reach high-security standards. Preliminary findings confirm the system's success in improving encryption resilience, showing great potential for safe image transfer and storage uses. Future work will include comprehensive comparative analyses against established baselines, such as direct AES-GCM encryption and AES combined with various lightweight scrambling techniques, to quantitatively demonstrate FusionCrypt's performance advantages. This will also involve in-depth evaluations against specific cryptanalytic and side-channel attacks. These improvements seek to confirm the framework's consistency in providing a dependable means of safe image transmission and storage.

ACKNOWLEDGMENT

This work was funded by the European Commission under the Doctoral Networks Programme (MSCA-DN-101073381–EnTrust) within the Horizon Europe (HORIZON) Marie Skłodowska-Curie Actions.

REFERENCES

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption," World Academy of Science, Engineering and Technolo-gy, International Journal of Computer, Electrical, Automation, Control and Information En-gineering, Mar. 2007, Accessed: Nov. 02, 2024. https://www.semanticscholar.org/paper/A-Modified-AES-Based-Algorithm-for-Image-Encryption-Zeghid-Machhout/fdb3d8263c147362d185d21ee4c2a2aad077055e.

[2] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," Chaos, Solitons & Fractals, vol. 26, no. 1, pp. 117–129, Oct. 2005, doi: 10.1016/j.chaos.2004.11.096.

[3] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosys-tems," Int. J. Bifurcation Chaos, vol. 16, no. 08, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.

[4] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on cha-os," Signal Processing, vol. 92, no. 4, pp. 1101–1108, Apr. 2012, doi: 10.1016/j.sigpro.2011.10.023.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Im-age and Vision Computing, vol. 24, no. 9, pp. 926–934, Sep. 2006, doi: 10.1016/j.imavis.2006.02.021.

[6] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," Signal Processing, vol. 90, no. 9, pp. 2714–2722, Sep. 2010, doi: 10.1016/j.sigpro.2010.03.022.

[7] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an inter-twining logistic map," Neurocomputing, vol. 251, pp. 45–53, Aug. 2017, doi: 10.1016/j.neucom.2017.04.016.

[8] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," Nonlinear Dyn, vol. 62, no. 3, pp. 615–621, Nov. 2010, doi: 10.1007/s11071-010-9749-8

[9] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for im-age encryption," Information Sciences, vol. 297, pp. 80–94, Mar. 2015, doi: 10.1016/j.ins.2014.11.018

[10] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Optics Communications, vol. 284, no. 16, pp. 3895–3903, Aug. 2011, doi: 10.1016/j.optcom.2011.04.001

[11] H. Wen, Y. Lin, S. Kang, X. Zhang, and K. Zou, "Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion," iScience, vol. 27, no. 1, Jan. 2024, doi: 10.1016/j.isci.2023.108610

[12] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hy-brid chaotic map and optimized substitution box," Nonlinear Dyn, vol. 99, no. 4, pp. 3041–3064, Mar. 2020, doi: 10.1007/s11071-019-05413-8

[13] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," Signal Processing, vol. 125, pp. 187–202, Aug. 2016, doi: 10.1016/j.sigpro.2016.01.017

[14] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryp-tography; Applications, challenges, recent advances, and future trends: A comprehensive survey," Computer Science Review, vol. 47, p. 100530, Feb. 2023, doi: 10.1016/j.cosrev.2022.100530