Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 559–568
DOI : 10.47974/JDMSC-1890

Cryptographic security for IoT : Leveraging Feistel-permutation network for enhanced encryption

Kiran Deep Singh [§]
Department of Computer Science and Engineering
Chitkara University Institute of Engineering and Technology
Chitkara University
Rajpura
Punjab
India

Prabh Deep Singh [†]
Department of Computer Science and Engineering
Graphic Era (Deemed to be University)
Dehradun
Uttrakhand
India

G. L. Saini *
Deepak Panwar [‡]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur
Rajasthan
India

Dinesh Goyal [@]
Department of Computer Science and Engineering
Poornima Institute of Engineering and Technology
Jaipur
Rajasthan
India

[§] *E-mail:* **kdkirandeep@gmail.com**
[†] *E-mail:* **ssingh.prabhdeep@gmail.com**
* *E-mail:* **glsaini86@gmail.com (Corresponding Author)**
[‡] *E-mail:* **deepakpanwar03@gmail.com**
[@] *E-mail:* **dinesh8dg@gmail.com**

© Taru Publications

Abstract

The emergence of the Internet of Things (IoT) has initiated an era where numerous devices are interconnected, resulting in the generation of significant volumes of data. Data security is an issue raised by this increase in communication, especially when it comes to picture encryption. Traditional encryption methods create considerable challenges in resource-constrained IoT environments. In this paper, a novel encryption-based framework known as the Feistel-Permutation Network Hybrid is proposed. It effectively safeguards IoT image data. A comprehensive performance evaluation by utilizing MATLAB that shows the effectiveness of the algorithm used. The findings offer valuable insights into the efficacy of the algorithm. Also, the areas for further investigation within the ever-evolving field of IoT image encryption are discussed.

Subject Classification: *68M25 Computer Security.*

Keywords: *Privacy-preserving, Cryptography, Secure force algorithm, Intelligent encryption systems, Medical image protection.*

1. Introduction

The Feistel structure plays a key role in the encryption process. It contributes to the security of the IoT image encryption by incorporating non-linear operations, block swapping, and combination operations, enhancing the complexity of the encryption algorithm [1]. IoT image encryption significantly impacts the overall security and privacy of IoT devices and networks. The additional connectivity that would result from the billions of devices that IoT devices are predicted to connect will probably produce enormous volumes of sensitive data, including images [2] [3] [4]. In the context of image data, encryption safeguards visual information from unauthorized access, protecting privacy and preventing tampering. The encryption of IoT image data is essential for maintaining the integrity and confidentiality of visual information in applications such as surveillance, healthcare, and smart environments [5] [6].

IoT applications that need secure image processing benefit from the encryption algorithm's lightweight nature. Processing power, memory, and energy are generally scarce in IoT devices [7]. Traditional encryption algorithms are computationally complex and may waste energy and processing resources on resource-constrained IoT devices . Hybridization with a permutation network boosts algorithm speed and security. The paper's structure includes Section II, which presents IoT and image encryption background. Our proposed framework's architectural design is detailed in Section III. Section IV analyzes Matlab experiments in detail, evaluating performance. Section V analyzes the data and presents the

results. Section VI concludes with a summary of future research and investigation.

2. Background

Cryptographic block ciphers use Horst Feistel's symmetric Feistel structure. It efficiently encrypts and decrypts using the same structure [8]. The Feistel structure's simplicity and efficacy make it ideal for image security [9]. Since it processes data in fixed-size blocks, the structure can handle images and other data kinds. A brief explanation of the Feistel structure follows:

1. Block Division: The Feistel structure divides input data, such as an image or fixed-size data block, into two equal-sized blocks in the first stage [10]. This division is significant because it sets the stage for later round operations.
2. Rounds: After block division, data is rounded. Each round involves dividing blocks and performing operations. The number of rounds depends on the encryption technique, affecting security and efficiency.
3. Operations: Non-linear Operation: Each round, the "left" block undergoes the "round function." This function complicates encryption and prevents reversal.

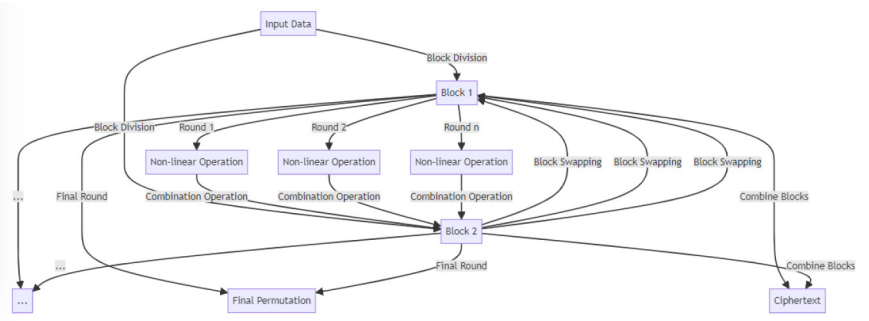


Figure 1

Flow of Feistel Structure for securing imaging.

4. Combination Operation: The non-linear operation effect is combined with the "right" block. XOR (exclusive OR) mixes data from both

blocks. The non-linear block becomes the "right" block, and vice versa, after block swapping. Swapping improves data dissemination.

5. Final Round: Blocks may be permuted after a certain number of rounds. This permutation, often reversible, prepares data for the ultimate combination. The two blocks are merged to create ciphertext, which encrypts the data.

These stages collectively define the Feistel structure, a versatile and widely utilized framework in block cipher design. Figure 1 displays Feistel structure design in block ciphers, where the subkey sequence is the only variation between encryption and decryption [11] [12]. Its symmetry, key expansion, and flexibility are crucial. The Feistel structure, which uses key expansion, divides input data into blocks, applies a non-linear operation on one block, and joins the two blocks with XOR operations. This structure can handle several round functions, making it versatile for cryptographic needs. Feistel-based image encryption methods are used in secure imaging. When choosing round function parameters, security and performance are considered. Feistel networks are promising in picture encryption systems [13] [14].

3. Proposed Framework

The framework employs a lightweight encryption method designed specifically for IoT devices. These round keys are subsequently utilized by the data encryption block to perform substitution and permutation operations on the plaintext. The technique employed exhibits a higher level of simplicity in comparison to conventional encryption algorithms, while concurrently ensuring a robust level of security for Internet of Things (IoT) devices. The mathematical model of the algorithm under consideration is presented below.

1. *Key Expansion Block:*

Let (K) be the original key of length (n) bits. The key expansion block generates a set of round keys $(K_1, K_2, \ldots, K_r)$ using a key expansion algorithm [15] [16]. The expansion process involves applying a series of operations, such as bitwise XOR, substitution, and permutation, to derive the round keys.

Key Expansion Algorithm:

1. Initialization:
   - Set $(K_0 = K)$.
2. Round Key Generation $(\text{for}(i = 1)\text{to}(r))$:
   - Apply a key mixing operation to (K_{i-1}).
   - Perform substitution operations on (K_{i-1}) using a substitution box (S_i).
   - Perform bitwise XOR with a round constant (RC_i).
   - Permute the bits using a permutation function (P_i).
   - The resulting $(K_i)$is the (i)-th round key.
2. Data Encryption Block: Let (P)be the plaintext of length (m) bits. The data encryption block uses the generated round keys to perform a series of substitution and permutation operations on the plaintext.

2. *Data Encryption Algorithm:*

1. Initial Round Key Mixing:
   - XOR the plaintext $(P)$with the initial round key (K_0).
2. Rounds $(\text{for}(i = 1)\text{to}(r))$:
   - Apply a substitution operation using a substitution box (S_i).
   - Perform a permutation operation using a permutation function (P_i).
   - XOR the result with the round key (K_i).
3. Final Round:
   - Apply a substitution operation using a substitution box (S_r).
   - Perform a permutation operation using a permutation function (P_r).
   - XOR the result with the last round key (K_r).
4. Output:
   - The final ciphertext is obtained.

   Here,
   - (r) is the number of rounds in the SIT algorithm.
   - (RC_i) is a round constant for the ith round.
   - (S_i) and (P_i) are substitution and permutation operations are unique to each round.

4. Simulation Setup and Performance Evaluation

The suggested framework was assessed by analyzing the impact of the cipher on the entropy, histogram, and correlation of the image. The algorithm underwent testing to assess its memory use and total computational time for key creation, encryption, and decryption processes. It was also determined how the encryption affected the image's correlation, histogram, and entropy shown in Figure 2 and Figure 3.

4.1 *Analysis of Image Histograms:*

The histogram offers valuable insights into the distribution of pixel intensities within the image subsequent to the encryption process. The presence of a uniform histogram after the process of encryption can be considered as an indication of a robust and safe technique. The evaluation is conducted by computing the histogram of the encrypted image.

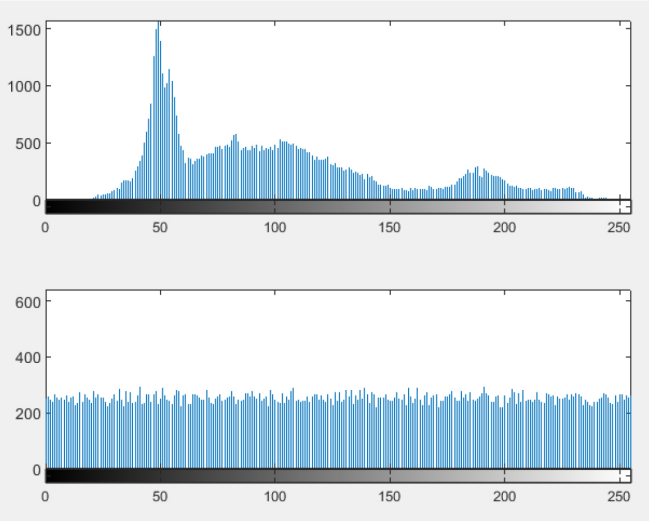


Figure 2

Comparison of Histogram obtained before and after the cryptography.

4.2 *Entropy*

The concept of image entropy refers to the measure of randomness or uncertainty included in an image. Entropy is an empirical concept that is employed to quantify the quantity of information. A higher degree of security algorithm performance is indicated by higher entropy values.

4.3 *Correlation analysis*

It calculates how similar the encrypted and original images are to one other [22]. A scatter plot is produced by establishing a correlation between the respective pixel values in the two photographs [23]. A good correlation shows that the approach is robust in picture encryption and preserves the image's structural integrity.

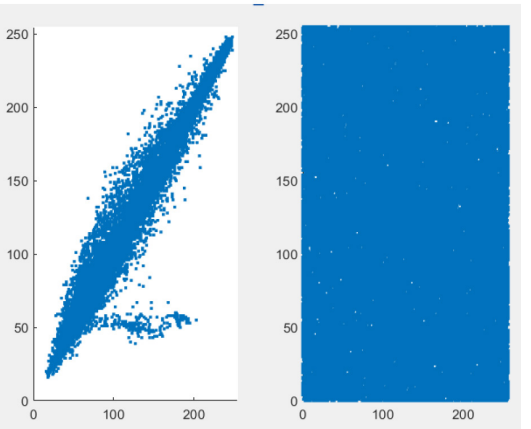


Figure 3

Comparison of correlation obtained before and after the cryptography.

5. Findings

Findings from the results collectively provide a comprehensive evaluation of the image encryption algorithm. They assess the algorithm's impact on image entropy, pixel changes, intensity alterations, encryption time, and correlation between original and encrypted images. The provided results pertain to the evaluation of an image encryption algorithm.

5.1 *Entropy*

The values represent the entropy that is a measure of the randomness or disorder in an image of the original image (7.4509) and the encrypted image (7.9969). The Original Image Entropy (7.4509), Indicates the amount of information in the original image. Higher values suggest a more varied distribution of pixel intensities. Whereas Encrypted Image Entropy (7.9969): Represents the entropy after encryption.

5.2 *NPCR (Number of Pixel Changes Rate)*

NPCR measures the percentage of pixels that change between the original and encrypted images. The obtained value of 99.5972% suggests that a significant number of pixels in the encrypted image that are different from their corresponding pixels in the original image. A high NPCR is advantageous since it signifies that a minor alteration in the original message leads to a substantial modification in the encrypted message, hence improving security.

5.3 *UACI (Unified Average Changing Intensity)*

The UACI metric measures the average magnitude of the intensity variation between the encrypted image and the original image. The value of 14.8724% implies that, on average, the pixel intensity in the encrypted image differs by this percentage from the original image. A lower UACI is generally preferred for better security, as it indicates a higher degree of pixel intensity alteration.

5.4 *Correlation Coefficient of Original Image*

[1.0 0.97 0.97 1.0]

The correlation matrix for the original image indicates the correlation coefficients between pixel values in different parts of the image. A coefficient of 1 suggests a perfect positive correlation, indicating a linear relationship between pixel intensities. Since they show how a pixel correlates with itself, the diagonal values are always 1.

5.5 *Correlation Coefficient of Encrypted Image*

[1.0 –0.01 –0.01 1.0]

The correlation matrix for the encrypted image reveals the correlation coefficients after encryption. A coefficient close to 1 or -1 suggests a high correlation or anti-correlation, respectively. The near-zero values on the off-diagonal indicate a reduced correlation between pixels in the encrypted image, which is desirable for security. They depict the algorithm's capacity to add complexity and obfuscate the original information, as well as the visual influence on image variability.

6. Conclusion

Secure communication between energy-constrained devices and sensors becomes increasingly important as IoT becomes more pervasive in our daily lives. This paper presents a security mechanism that is designed to be lightweight, in order to address resilience against potential future threats, hence guaranteeing its suitability in the dynamic domain of security of IoT images. The combined effect of these attributes provides a comprehensive assessment of the efficacy of the proposed algorithm in guaranteeing the confidentiality of images. The approach is being considered for implementation on hardware and software in different network and compute contexts for future research.

References

[1] M. Alam, M. D. Samad, L. Vidyaratne, A. Glandon, and K. M. Iftekharuddin, "Survey on Deep Neural Networks in Speech and Vision Systems," *Neurocomputing*, vol. 417, pp. 302–321 (2020), doi: 10.1016/j.neucom.2020.07.053.

[2] J. Pietris, Y. Tan, and W. O. Chan, "Health care in the metaverse," *Med. J. Aust.*, vol. 219, no. 1, p. 41 (2023), doi: 10.5694/mja2.51986.

[3] S. Aminizadeh *et al.*, "The applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things," *Comput. Methods Programs Biomed.*, vol. 241, p. 107745 (2023), doi: 10.1016/j.cmpb.2023.107745.

[4] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography,* 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[5] W. Bani Issa *et al.*, "Privacy, confidentiality, security and patient safety concerns about electronic health records," *Int. Nurs. Rev.*, vol. 67, no. 2, pp. 218–230 (2020), doi: 10.1111/inr.12585.

[6] S. Tiwari, S. Kumar, and K. Guleria, "Outbreak Trends of Coronavirus Disease-2019 in India: A Prediction," *Disaster Med. Public Health Prep.*, vol. 14, no. 5, pp. e33–e38 (2020), doi: 10.1017/dmp.2020.115.

[7] S. Rani, S. H. Ahmed, and R. Rastogi, "Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications," *Wirel. Networks*, vol. 26, pp. 2307–2316 (2020).

[8] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng, and P. Singh, "Secure and energy-efficient smart building architecture with emerging technology IoT," *Comput. Commun.*, vol. 176, pp. 207–217 (2021), doi: 10.1016/j.comcom.2021.06.003.

[9] P. K. Shukla, J. K. Sandhu, A. Ahirwar, D. Ghai, P. Maheshwary, and P. K. Shukla, "Multiobjective Genetic Algorithm and Convolutional Neural Network Based COVID-19 Identification in Chest X-Ray Images," *Math. Probl. Eng.*, vol. 2021, pp. 1–9 (2021), doi: 10.1155/2021/7804540.

[10] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.

[11] X. Chen, J. Zhang, B. Lin, Z. Chen, K. Wolter, and G. Min, "Energy-Efficient Offloading for DNN-Based Smart IoT Systems in Cloud-Edge Environments," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 3, pp. 683–697 (2022), doi: 10.1109/TPDS.2021.3100298.

[12] S. K. Shukla *et al.*, "An integration of autonomic computing with multicore systems for performance optimization in Industrial Internet of Things," *IET Commun.* (2022), doi: 10.1049/cmu2.12505.

[13] P. Matta, B. Pant, and U. K. Tiwari, "DDITA: A naive security model for IoT resource security," *Adv. Intell. Syst. Comput.*, vol. 670, pp. 199–209 (2019), doi: 10.1007/978-981-10-8971-8_19.

[14] M. Kaur *et al.*, "EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT," *IEEE Access*, vol. 11, pp. 90739–90748 (2023), doi: 10.1109/ACCESS.2023.3305271.

[15] G. Sharma, H. Sharma, R. Pareek, N. Gour, R. S. Sharma, and A. Kumar, "Self-healing topology for DDoS attack identification \& discovery protocol in software-defined networks," *J. Discret. Math. Sci. Cryptogr.*, vol. 24, no. 8, pp. 2221–2232 (2021).

[16] A. Abusukhon, M. N. Anwar, Z. Mohammad, and B. Alghannam, "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm," *J. Discret. Math. Sci. Cryptogr.*, vol. 22, no. 1, pp. 65–81 (2019).

[22] G. L. Saini, D. Panwar, S. Kumar, and V. Singh, "A systematic literature review and comparative study of different software quality models," *J. Discret. Math. Sci. Cryptogr.*, vol. 23, no. 2, pp. 585–593 (2020).