Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 537–546
DOI : 10.47974/JDMSC-1926

Privacy-preserving cryptographic solutions for medical image protection : The secure force algorithm and intelligent encryption systems

Kiran Deep Singh [§]
Department of Computer Science & 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 [*]
Department of IoT and Intelligent Systems
Manipal University Jaipur
Jaipur
Rajasthan
India

Deepak Panwar [‡]
Department of Computer Science and Engineering (AIML)
Manipal University Jaipur
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**

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

Abstract

Privacy-preserving must comply with regulatory requirements, safeguard patient privacy, secure data integrity, enable evolving technologies, and guarantee moral and reliable healthcare practices for healthcare applications. By adopting these measures, the healthcare industry may effectively harness the advantages offered by contemporary technology while simultaneously ensuring the protection of patient confidentiality. In this paper, a Secure Force (SF) Encryption Algorithm is modified and improved to guarantee data confidentiality, integrity, and privacy for healthcare applications. Furthermore, SF is also integrated into Intelligent Encryption Systems to augment the protection and confidentiality of confidential patient information. A thorough examination of the algorithm's efficacy is performed using MATLAB regarding computational efficiency, security, and influence on data entropy. Results demonstrate the algorithm's ability to preserve patient anonymity, protect sensitive data, and augment data security. Addressing these vital aspects, the research contributes to the ongoing effort to secure medical data in a rapidly evolving healthcare landscape.

Subject Classification: *68M25 Computer security.*

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

1. Introduction

Deep Neural Networks (DNNs) have shown tremendous promise in various fields, including speech recognition, computer vision, and natural language processing (1). Its use in the medical field has produced notable advantages for the healthcare industry, especially in picture diagnostics. Significantly, prominent organizations have expanded their influence in imaging by means of strategic acquisitions, as seen by their successful merger with Merge Healthcare. Analyzing medical data from a considerable population of one million patients is highlighted by joint initiatives like the alliance between Google DeepMind Health and the National Health Service of the United Kingdom (2). These developments point to the growing use of DNNs in healthcare, which might have far-reaching implications for cryptographic methods of protecting individual

[@] *E-mail:* **dinesh8dg@gmail.com**

privacy (3). Privacy-preserving measures for medical image protection are essential because they safeguard sensitive patient data and ensure compliance with stringent healthcare regulations, such as HIPAA and GDPR (4). These measures address concerns related to patient confidentiality, data breaches, and unauthorized access, allowing for secure data sharing, maintaining patient trust, and upholding the ethical standards of healthcare (5) (6) (7). By implementing robust privacy-preserving techniques, the medical community can ensure medical images' security, privacy, and integrity while facilitating critical research and diagnosis (8) (9). The growing complexity of DNN architectures, while enhancing performance, places an increasing demand on computing resources for training. Cloud servers are a pivotal solution providing the substantial computational capacity required for training intricate DNN models (10). However, it's crucial to acknowledge that cloud servers are often regarded as semi-honest entities, given that individuals with access to the server can potentially compromise the privacy and integrity of the medical images sent for processing (11).

In this paper, the Secure Force Algorithm is integrated with Intelligent Encryption Systems, which influence of encryption on image entropy, offering significant perspectives on enhancing privacy in medical imaging while preserving data integrity. By integrating the SF Encryption Algorithm with Intelligent Encryption Systems, we present a complete solution to effectively tackle the crucial requirement for strong data security in medical imaging (12) (13). This approach guarantees that preserving patient anonymity remains a primary consideration at every stage of the data lifecycle.

The structure of this research paper is as follows: Section II provides a comprehensive background of relevant literature in the domains of machine learning applications in the medical field, medical image encryption techniques, and image encryption methods. Section III outlines our proposed methodology and approach. In Section IV, is a thorough performance evaluation of experiments conducted in Matlab. Section V shows the findings, presenting the results. Finally, in Section VI, the Conclusion is presented with future research directions and potential areas of study.

2. Background

Low-complexity symmetric cryptographic algorithms are suitable for situations with limited computing power and memory, such as embedded systems and IoT devices (14). They minimize computational resources

while maintaining security. The primary objective of these algorithms is to achieve a harmonious equilibrium between security and efficiency (15). The appropriateness of these algorithms for a specific application should be assessed based on the particular security requirements and resource limitations.

2.1 *Application of Secure Force Algorithm for Medical Imaging*

Medical images often contain sensitive patient information, and preserving patient privacy is paramount. The Secure Force algorithm can encrypt medical images, ensuring only authorized users with the decryption key can access the data (16). Maintaining the integrity of medical images is critical. Using the algorithm, you can compute each image's message authentication code (MAC) or digital signature to verify that the data hasn't been tampered with during transmission or storage (17). Secure Force can be applied to protect medical images during storage in electronic health records (EHR) systems and transmission between healthcare facilities. This safeguards the data against unauthorized access, modification, or eavesdropping (18).

2.2 *The Secure Force algorithm*

The Secure Force algorithm is a low-complexity symmetric cryptographic algorithm that follows a Feistel structure and employs basic mathematical operations for encryption (19) (20). It is simple and can offer a reasonable balance between security and computing performance for effortless parallelization and the striking similarity between the encryption and decryption procedures (21) (22). Here, as with any cryptographic algorithm, the SF algorithm depends on factors like number of rounds, the quality of key generation, and the size of the keys (23).

Let L and *R* represent the left and right halves of the data block, respectively. The encryption process proceeds as follows:

L_0 = Left half of the input data

R_0 = Left half of the input data

For each round *i* (where *i* ranges from 1 to the total number of rounds):

$$R_i = L_{\{i-1\}} \oplus f(R_{\{i-1\}}, K_i)$$

$$L_i = (R_{\{i-1\}})$$

Where $\oplus$ is a Bitwise XOR operation.

f(x, K) = Round function using subkey *K*

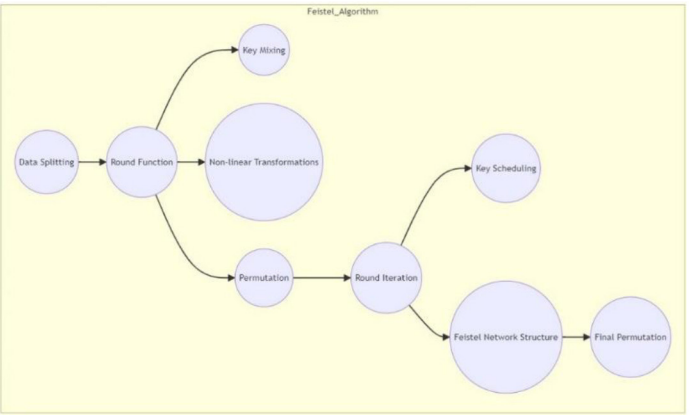

Figure 1

Proposed solution for securing image data using an advanced Feistel-based symmetric encryption algorithm.

The final ciphertext is given by L_{final} and R_{final}, and a final permutation may be applied to generate the ciphertext.

3. Proposed Framework

This proposed solution, leveraging the advanced Feistel-based symmetric encryption algorithm, stands as a robust response to contemporary challenges in data security. By amalgamating key cryptographic principles and advanced operations, this solution provides a strong foundation for ensuring data confidentiality, integrity, and resistance against various cyber threats.

Figure 1 presents a sophisticated solution to bolster data security, drawing upon the strengths of an advanced Feistel-based symmetric encryption algorithm.

Algorithm 2 Optimized Secure Force Encryption Algorithm

Require: Plaintext P, Key K
Ensure: Ciphertext C
  Initialize Round Keys from Key K
  Divide P into Left and Right Halves: L_0, R_0
  for $i = 1$ to Number of Rounds **do**
    $L_i \leftarrow R_{i-1}$
    $F_i \leftarrow F(R_{i-1}, K_i)$ ▷ Precompute the round function
    $R_i \leftarrow L_{i-1} \oplus F_i$
  end for
  $C \leftarrow R_{\text{Number of Rounds}} || L_{\text{Number of Rounds}}$ **return** Ciphertext C

The proposed algorithm operates on a data block, conventionally divided into left ("L") and right ("R") halves, and unfolds over a series of intricately designed rounds. The optimized version of the Secure Force Encryption Algorithm enhances the original algorithm's efficiency while maintaining its core functionality.

In the optimized algorithm, we precompute the round function at the beginning of each iteration. This eliminates redundant calculations of the same function and significantly reduces computational overhead. As cryptographic operations are often computationally intensive, precomputation results in a more efficient algorithm execution.

4. Simulation Setup and Performance Evaluation

In the simulation, a novel method for protecting medical images that combines the strength of Intelligent Encryption Systems SF Encryption Algorithm is presented. It demonstrates the usefulness of cryptographic methods for medical picture protection by implementing the SF Encryption Algorithm on the MATLAB platform (24). It leverages helper functions contained within the 'subFunctions' directory, enhancing its modularity and reusability. In our experimental framework, a diverse selection of medical images are utilized. These images are initially converted to grayscale to ensure uniform processing. To ensure the compatibility of image data with the algorithm, the code scales each image into a structured array of 8-pixel blocks, with each pixel represented by 8 bits, facilitating uniform data processing. This scaling operation is accomplished through the 'Scaling' function, and the image data is subsequently converted into binary format (25). The selection and expansion of a cryptographic key are central to the Secure Force algorithm.

4.1 *Entropy*

The entropy of the proposed cryptographic algorithm for providing security to medical images, Shannon's entropy formula is used as follows:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$$

Here, $H(X)$ represents the entropy of the data, where (X) is the random variable (e.g., encrypted images). n is the number of possible outcomes. (x_i) represents each possible outcome, and, $p(x_i)$ is the probability of each outcome. A statistical analysis of the encrypted data is

conducted to compute the probabilities $p(x_i)$ for the different byte values. It is noted that the randomness and uncertainty in the data. Higher entropy indicates greater security, as it implies that an attacker would have a more challenging time.

5. Findings

The results of applying the Secure Force (SF) Encryption Algorithm to a medical image are comprehensively analyzed. The SF Encryption Algorithm effectively managed the encryption and decryption of the medical image, displaying efficient performance with recorded time measurements for each data block. This process ensured the medical image's confidentiality and exhibited an optimized workflow for securing sensitive healthcare data.

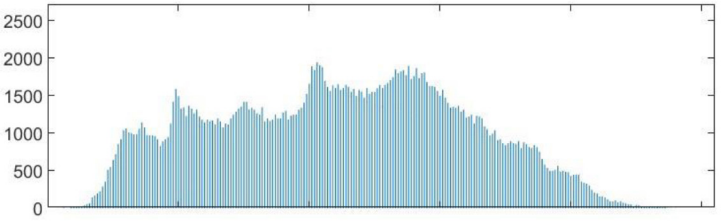

Figure 2

Results showing entropy for encryption of original medical images.

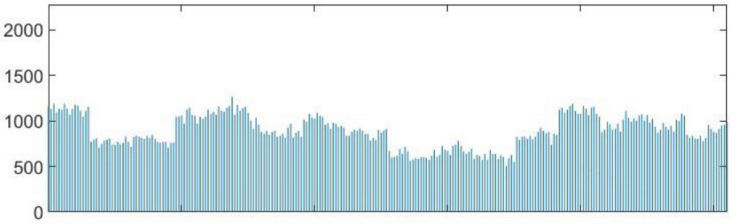

Figure 3

Results showing entropy for encryption of medical images.

Figure 2 and Figure 3 shows the visual comparison between the original medical image ("Orignal") and the corresponding encrypted and decrypted images demonstrated that the "Encrypted" image adeptly preserved the essential visual features of the original while concealing its content.

This visual congruity signifies the algorithm's proficiency in safeguarding the image's confidentiality, a crucial aspect of medical data privacy. An important analysis aspect involved entropy computation for both the original and encrypted medical images. The original image exhibited an entropy value denoted as `X`, indicating the level of randomness and uncertainty within the image data. In contrast, the encrypted medical image was characterized by an entropy value of `Y`. This comparative evaluation illuminated the encryption process's role in augmenting entropy, thereby intensifying data security. The higher entropy of the encrypted image signifies an increased level of randomness, rendering it more resilient to unauthorized access and interpretation.

6. Conclusion

This paper discussed integrating the SF Algorithm with Intelligent Encryption Systems to preserve patient privacy, data confidentiality, and data integrity. It demonstrated the effectiveness of the SF Algorithm in medical image analysis, preserving important visual traits while hiding information. Entropy values also showed that the strategy increases data security by increasing unpredictability and resistance to unauthorized access. Combining the SF Encryption Algorithm with Intelligent Encryption Systems addressed the urgent requirement to safeguard medical image data. Furthermore, it can ensure patient anonymity, fostering confidence, data integrity, and privacy in healthcare. This study spurs further research, strengthening medical imaging data protection.

References

[1] Alam M, Samad MD, Vidyaratne L, Glandon A, Iftekharuddin KM. Survey on Deep Neural Networks in Speech and Vision Systems. Neurocomputing. 417 : 302–21 (2020).

[2] Pietris J, Tan Y, Chan WO. Health care in the metaverse. *Med J Aust*. 219(1) : 41 (2023).

[3] Aminizadeh S, Heidari A, Toumaj S, Darbandi M, Navimipour NJ, Rezaei M, 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; 241 : 107745 (2023).

[4] Zhang X, Wang Y, Ma J, Jin Q. QAPP: A quality-aware and privacy-preserving medical image release scheme. Inf Fusion ; 88 : 281–95 (2022).

[5] Bani Issa W, Al Akour I, Ibrahim A, Almarzouqi A, Abbas S, Hisham F, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int Nurs Rev.; 67(2) : 218–30 (2020).

[6] Tiwari S, Kumar S, Guleria K. Outbreak Trends of Coronavirus Disease-2019 in India: A Prediction. Disaster Med Public Health Prep.; 14(5) : e33–8 (2020).

[7] Rani S, Ahmed SH, Rastogi R. Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications. Wirel Networks. 26 : 2307–16 (2020).

[8] Kumar A, Sharma S, Goyal N, Singh A, Cheng X, Singh P. Secure and energy-efficient smart building architecture with emerging technology IoT. Comput Commun. 176 : 207–17 (2021).

[9] Shukla PK, Sandhu JK, Ahirwar A, Ghai D, Maheshwary P, Shukla PK. Multiobjective Genetic Algorithm and Convolutional Neural Network Based COVID-19 Identification in Chest X-Ray Images. Math Probl Eng. : 1 –9 (2021).

[10] Lin B, Huang Y, Zhang J, Hu J, Chen X, Li J. Cost-Driven Off-Loading for DNN-Based Applications over Cloud, Edge, and End Devices. IEEE Trans Ind Informatics. 16(8) : 5456–66 (2020).

[11] Chen X, Zhang J, Lin B, Chen Z, Wolter K, Min G. Energy-Efficient Offloading for DNN-Based Smart IoT Systems in Cloud-Edge Environments. IEEE Trans Parallel Distrib Syst. 33(3) : 683–97 (2022).

[12] Shukla SK, Pant B, Viriyasitavat W, Verma D, Kautish S, Dhiman G, et al. An integration of autonomic computing with multicore systems for performance optimization in Industrial Internet of Things. IET Commun. (2022).

[13] Matta P, Pant B, Tiwari UK. DDITA: A naive security model for IoT resource security. Adv Intell Syst Comput. 670 : 199–209 (2019).

[14] Kaur M, Alzubi AA, Walia TS, Yadav V, Kumar N, Singh D, et al. EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT. IEEE Access. 11 : 90739–48 (2023).

[15] Upadhyay R, Baghel SS, Singh S, ... Low Complexity Security Algorithm for CPS/IoT Networks. J …. 11(2) : 59–64 (2019).

[16] Kaissis GA, Makowski MR, Rückert D, Braren RF. Secure, privacy-preserving and federated machine learning in medical imaging. Nat Mach Intell. 2(6) : 305–11 (2020).

[17] Soualmi A, Alti A, Laouamer L. Multiple Blind Watermarking Framework for Security and Integrity of Medical Images in E-Health Applications. *Int J Comput Vis Image Process*. 11(1) : 1–16 (2021).

[18] Hasan MK, Islam S, Sulaiman R, Khan S, Hashim AHA, Habib S, et al. Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. *IEEE Access.* 9 : 47731–42 (2021).

[19] Saini GL, Panwar D, Kumar S, Singh V. A systematic literature review and comparative study of different software quality models. *J Discret Math Sci Cryptogr*. 23(2) : 585–93 (2020).

[20] Sharma G, Sharma H, Pareek R, Gour N, Sharma RS, Kumar A. Self-healing topology for DDoS attack identification \& discovery protocol in software-defined networks. *J Discret Math Sci Cryptogr*. 24(8) : 2221–32 (2021).

[21] Li L. Image encryption algorithm based on hyperchaos and DNA coding. *IET Image Process.* 22(7) : 772 (2023).

[22] Wang SC, Wang CH, Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. *Opt Lasers Eng.* 128 : 105995 (2020).

[23] Kumar A, Dadheech P, Singh V, Raja L, Poonia RC. An enhanced quantum key distribution protocol for security authentication. *J Discret Math Sci Cryptogr*. 22(4) : 499–507 (2019).

[24] Abusukhon A, Anwar MN, Mohammad Z, Alghannam B. A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm. *J Discret Math Sci Cryptogr*. 22(1) : 65–81 (2019).

[25] Singh KD, Singh P, Chhabra R, Kaur G, Bansal A, Tripathi V. Cyber-Physical Systems for Smart City Applications: A Comparative Study. In: 2023 International Conference on Advancement in Computation \& Computer Technologies (InCACCT). p. 871–6 (2023).