A Comprehensive Study on the Homomorphic Encryption for Secure Image Data Processing

Qiang Chen
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia | Dongguan City University, Dongguan, Guangdong, China
48044244@qq.com

Huixian Li
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia | College of Financial Technology, Hebei Finance University, Baoding, Hebei, China
153193723@qq.com

Suriyani Binti Ariffin
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia
suriyani@uitm.edu.my (corresponding author)

Nor Atiqah Bte Mustapa
College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia
atiqah@uitm.edu.my

Received: 22 December 2024 | Revised: 28 January 2025 | Accepted: 31 January 2025

ABSTRACT

In the contemporary digital landscape, the integrity and confidentiality of data have become paramount concerns. This study presents a comprehensive framework for secure image data processing using homomorphic encryption. The proposed approach involves image preprocessing, logistic regression model training, feature extraction, and polynomial approximation to accommodate the constraints of homomorphic encryption algorithms. Sensitive data, encrypted via homomorphic algorithms, is embedded within images to ensure its concealment during computational operations. Subsequent encryption of the image using the asymmetric Rivest-Shamir-Adleman (RSA) algorithm further secures the encapsulated sensitive data. Through experimental data and analysis, the performance and speed of homomorphic encryption are compared against traditional methods, validating its efficacy in encrypted image data processing.

Keywords-homomorphic encryption; logistic regression; information security

I. INTRODUCTION

A. Background and Significance

The growing reliance on digital data storage and transmission has increased the need for robust encryption techniques to ensure data confidentiality and integrity. Traditional encryption methods, while effective, are often unable to provide the granularity and efficiency required for data processing. Homomorphic encryption, which allows computations on encrypted data without decryption, has emerged as a promising solution. This study explores the application of homomorphic encryption in secure image data processing, focusing on its implementation, performance, and comparative advantages over traditional methods.

In the field of data encryption, several studies have made significant contributions. Rajeshkumar et al. in [1] proposed a BHESKD-ODL model that integrates blockchain, homomorphic encryption, and deep learning to achieve secure and accurate skin lesion diagnosis. Jumonji et al. in [2] introduced a privacy-preserving collaborative filtering method using fully homomorphic encryption to address privacy leakage in online recommendation systems. Raisaro et al. in [3] presented a solution to protect the privacy and security of genomic data within the i2b2 framework. Kim et al. in [4] integrated homomorphic encryption and differential privacy to enable secure outsourcing and exploration of large-scale genomic and clinical datasets. Clet et al. in [5] provide guidelines for using three popular homomorphic cryptosystems (BFV, CKKS, and TFHE) within the Chimera framework, enabling switching between them. They compare the performance of these systems in evaluating feed-forward neural networks on the MNIST database, considering both encrypted queries and models, and evaluate the precision, memory usage, and execution time for 128-bit security, providing insights into which system to use for different secure computation scenarios in the cloud. Shekhawat et al. in [6] proposed safeguarding sensitive user data on untrusted cloud servers, providing an overview of various encryption techniques, including homomorphic encryption, to ensure data confidentiality and integrity while maintaining efficiency and scalability. This study proposes a secure logistic regression method based on homomorphic encryption, which allows learning from encrypted data through an enhanced gradient descent algorithm. The least squares method was utilized to approximate the sigmoid function, thereby enhancing calculation accuracy and efficiency.

Homomorphic encryption in images has significance in several aspects:

- Privacy protection: Homomorphic encryption allows direct computation on encrypted data without prior decryption, ensuring the privacy of the data during processing or analysis, such as feature extraction and classification. This is crucial for sensitive image data like personal identity information and medical images.
- Secure data processing: Data remains encrypted throughout the processing cycle, preserving confidentiality even in insecure environments, such as cloud computing, where users can securely upload encrypted data for processing without data leakage concerns.
- Enhanced data utilization: Unlike traditional methods that require decryption for data processing, homomorphic encryption allows encrypted data to be used directly for analysis and computation, greatly expanding the scope of applications.
- Compliance and standardization: In industries with stringent data privacy regulations, such as finance and healthcare, homomorphic encryption aids in conducting necessary data analysis while complying with regulatory requirements, ensuring data security, and promoting efficient data utilization.
- Facilitating innovative application scenarios: Homomorphic encryption opens new possibilities for application and service development, particularly in domains requiring high levels of data privacy and security, such as inter-institutional data sharing and secure multi-party computing.

In summary, the application of homomorphic encryption to images effectively safeguards sensitive information while enabling diverse data processing and analysis tasks, holding significant implications for secure data analysis, privacy protection, and technological innovation.

B. Concepts and Characteristics of Homomorphic Encryption

Homomorphic encryption is a specialized form of encryption that allows computations to be performed directly in the ciphertext domain, eliminating the need for prior decryption. This feature enables data processing and analysis without compromising the confidentiality of sensitive information. The key characteristics of homomorphic encryption are:

- Protecting data privacy: By encrypting data, homomorphic encryption prevents unauthorized disclosure of sensitive information.
- Supporting computational operations: Homomorphic encryption uniquely enables addition and multiplication operations on encrypted data without requiring ciphertext decryption.
- Realizing fine-grained access control: Homomorphic encryption facilitates access control mechanisms for encrypted data, enabling fine-grained privilege management and ensuring authorized access and manipulation.

II. HOMOMORPHIC ENCRYPTION IN DATA-ENCRYPTED IMAGES

Homomorphic encryption, rooted in the theory of the computational complexity of mathematical problems, supports cryptographic computations on encrypted data that yield decrypted results identical to plaintext computations. This technique exhibits versatility across diverse application scenarios, making it a prominent research direction in privacy-preserving computation. Data encryption serves as a reliable means to protect privacy and ensure data security, effectively mitigating the risk of data breaches.

A. Requirement Analysis of Data Encryption Images

Data-encrypted images refer to images with embedded sensitive data, encrypted to ensure confidentiality. In scenarios such as medical imaging and ID photographs, it is imperative to protect the sensitive information contained within these images to prevent unauthorized access and tampering. Homomorphic encryption technology is emerging as a viable solution for efficient processing and fine-grained control of image data. Its ability to perform computational operations directly on encrypted data allows various operations and analyses to be performed on encrypted images without compromising the sensitive information they contain. With homomorphic encryption, precise control over the encrypted image can be achieved, such as decrypting specific regions or executing targeted operations without revealing the entire content.

By utilizing data-encrypted image techniques, the privacy and integrity of sensitive information can be safeguarded. By embedding data into images and applying encryption algorithms, sensitive information is effectively protected during transmission and storage. Only authorized users have the means to decrypt and access these encrypted images, thereby gaining access to the sensitive information they contain. This approach provides a robust layer of security for sensitive data while meeting the requirements of efficient data processing and privacy.

B. Homomorphic Encryption Implementation in Data-Encrypted Images

The implementation of homomorphic encryption algorithms in data-encrypted images can be achieved through the following steps:

- Image preprocessing: The original image undergoes preprocessing operations, such as compression, resizing, and format conversion, to align with the requirements of the homomorphic encryption algorithm. This stage ensures image consistency and compatibility for effective encryption and data embedding.
- Data encryption: Sensitive data are encrypted using homomorphic encryption algorithms, facilitating computational operations on encrypted data without the need for decryption. This step ensures data confidentiality by rendering them inaccessible to unauthorized users until decrypted.
- Ciphertext embedding: The resulting homomorphic encrypted ciphertext is embedded into a predetermined location within the image. The embedding process must maintain data security and integrity, which can be achieved by fusing the ciphertext with image pixel values or inserting it into a dedicated image region. The choice of location and embedding method must prevent data leakage or tampering during image processing and transmission.
- Image decryption: When access to the data is required, the ciphertext embedded in the image is decrypted using the homomorphic decryption algorithm to retrieve the original sensitive data. The decryption process is the inverse of homomorphic encryption, and only authorized users possess the corresponding decryption key to perform this operation. Through decryption, the original data can be retrieved, allowing the sensitive information to be accessed and used.

By following these steps, homomorphic encryption technology safeguards sensitive data in data-encrypted images while maintaining data security and integrity.

C. Logistic Regression Function

Logistic regression models are highly accurate, easy to understand, and meet regulatory interpretability requirements. Logistic regression is a statistical learning method for modeling binary classification problems. It maps the output of a linear regression model to a probability value and restricts that probability value to between 0 and 1 using a logistic function, making it suitable for predicting probabilities in binary classification problems. The mathematical expression for logistic regression is given below:

$$P(y=1 \mid x)=\frac{1}{1+e^{-z}} \qquad (1)$$

where P is the probability that the output variable y is 1 given the input variable x, z denotes the linear regression model output, which takes values between 0 and 1 and can be thought of as the probability that the sample belongs to a positive class.

Commonly utilized methods and techniques associated with logistic regression include:

- Parameter estimation: Logistic regression typically employs maximum likelihood estimation for parameter estimation. The objective of maximum likelihood estimation is to find parameter values that maximize the likelihood function of the observed data.
- Model training: Logistic regression models are routinely trained utilizing the gradient descent method or its derivatives. This method iteratively adjusts the model parameters to minimize the loss function.
- Feature engineering: In logistic regression, feature engineering is an important aspect. It includes techniques such as feature selection, feature transformation, and feature construction that aim to extract and represent relevant pertinent information from the input variables.
- Regularization: Logistic regression models frequently employ regularization techniques to manage model complexity and mitigate overfitting. Popular regularization methods include L1 regularization and L2 regularization.
- Evaluation metrics: When evaluating logistic regression models, commonly employed metrics include accuracy, precision, recall, F1 score, and the ROC curve.

Logistic regression is a straightforward yet effective classification approach, particularly suited to problems that are linearly separable or nearly linearly separable.

D. Introduction to the BFV and CKKS Libraries

In the Python community, PySEAL and TenSEAL have emerged as prominent libraries, each specializing in the implementation of distinct Fully Homomorphic Encryption (FHE) schemes: PySEAL for the Brakerski-Fan-Vercauteren (BFV) scheme and TenSEAL for the Cheon-Kim-Kim-Song (CKKS) scheme. These libraries offer powerful tools for enhancing data security and privacy protection in a wide range of applications.

- PySEAL (BFV library implementation): PySEAL is a high-level Python library specializing in the BFV fully homomorphic encryption scheme. The BFV scheme, constructed upon a ring of integer polynomials, supports direct addition and multiplication operations on encrypted data, enabling complex computations without decryption. PySEAL simplifies the development process by providing comprehensive APIs for key generation, data encryption, decryption, and homomorphic operations. It is well suited for small to medium-sized datasets requiring high computational efficiency and ease of use.
- TenSEAL (CKKS library implementation): TenSEAL focuses on the CKKS fully homomorphic encryption scheme, which supports operations on complex numbers. The CKKS scheme, based on a ring of complex numbers, enables seamless manipulation of both real and complex data. It supports addition, multiplication, and approximation

operations on encrypted data, making it ideal for large-scale datasets and complex computational tasks in machine learning and data analytics. TenSEAL provides user-friendly APIs for key management, data encryption, decryption, and homomorphic operations, making it suitable for large data volumes.

The two libraries, each tailored to distinct application scenarios and requirements, open up new possibilities for Python developers looking to implement fully homomorphic encryption. They not only advance the application and advancement of cryptography but also provide an effective technical apparatus for safeguarding data privacy. By leveraging PySEAL and TenSEAL, developers can design and implement security protocols that facilitate computations on encrypted data, thereby ensuring the confidentiality and integrity of data throughout its processing, transmission, and storage phases. This not only broadens the horizons of data utilization and analysis, but also meticulously shields user privacy. The key algorithm features of these libraries are summarized in Table I.

TABLE I. COMPARISON OF CHARACTERISTICS BETWEEN BFV AND CKKS

Feature/library	**PySEAL (BFV implementation)**	**TenSEAL (CKKS implementation)**
Encryption scheme base	Based on a ring of integer polynomials for fully homomorphic encryption	Based on a ring of complex numbers for fully homomorphic encryption
Supported data types	Integers	Real and complex numbers
Core advantage	Supports direct addition and multiplication on encrypted data, suitable for small to medium-sized datasets	Supports addition, multiplication, and approximation operations on encrypted data, ideal for large datasets and complex computational tasks
Application scenarios	Suitable for scenarios requiring high computational efficiency and ease of use, such as small to medium data processing	Suitable for large-scale datasets and complex computations, such as machine learning and data analytics
Design focus on performance and usability	High performance and user experience, simplifying the developer's work in performing fully homomorphic encryption computations	Combines high performance and ease of use, providing strong support for fully homomorphic computation on large data volumes
Key operations	Provides APIs for key generation, data encryption, data decryption, and homomorphic addition and multiplication	Provides APIs for key management, encrypting and decrypting data, and performing homomorphic operations, including operations with complex numbers
Target audience	Developers, especially those needing to protect data privacy and perform encrypted computations in their applications	Developers, particularly professionals in large-scale data processing and machine learning application development

III. EXPERIMENTAL DESIGN AND DATA ANALYSIS

A. Dataset Acquisition and Description

For this experiment, we selected a standard set of MATLAB images, including Lena, Cameraman, and Peppers, each with a size of 256×256 pixels. These images are widely used in image processing research due to their standardization and availability.

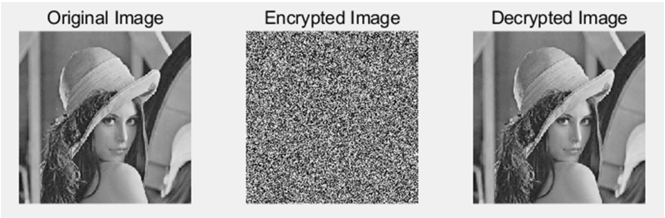
B. Experimental Steps

- Image preprocessing: The selected images were preprocessed using MATLAB 2020 and PyCharm 2023.1. The preprocessing steps included resizing to 256×256 pixels, grayscale, and normalization to ensure data consistency and reduce computational complexity.
- Logistic regression model training: A logistic regression model was trained using the extracted features and their corresponding labels in a plaintext environment. The model parameters (weights and biases) were obtained. Due to the limitations of homomorphic encryption algorithms, a polynomial approximation of the sigmoid function was required.
- Encrypting sensitive data and embedding ciphertext into images: Sensitive data was encrypted using a homomorphic encryption algorithm, and the resulting ciphertext was embedded in the images by integrating the encrypted data with the image pixels.
- Enhancing data protection with Rivest-Shamir-Adleman (RSA) encryption: The same set of images was further encrypted using the traditional asymmetric RSA encryption algorithm to provide an additional layer of security.
- Comparative analysis of encryption methods: A comparative evaluation of the encryption effectiveness and speed between homomorphic encryption and traditional encryption methods, such as RSA, was conducted. The results were analyzed to determine the strengths and limitations of different encryption approaches and their specific impact on image encryption.

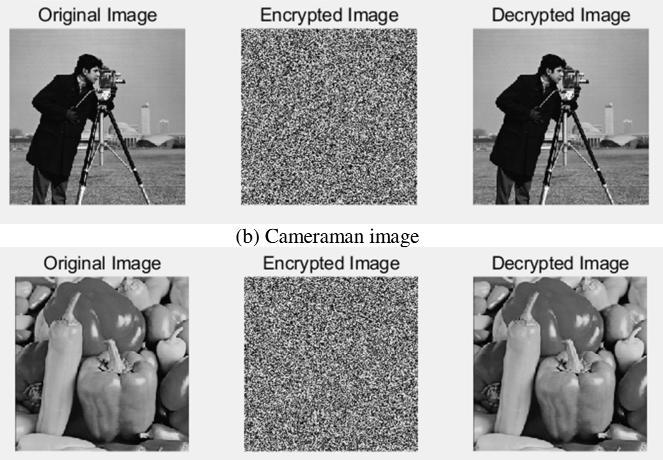
C. Data Analysis and Results

1) Simulation Experiment

The experimental platform is a PC running Windows 10 operating system. The algorithm was implemented on the MATLAB R2020a platform, and the experimental results are shown in Figure 1.



(a) Lena image



(b) Cameraman image

(c) Peppers image

Fig. 1. Simulation results.

2) *Histogram analysis*

Histograms effectively reflect the distribution pattern of image pixel values. In image encryption, a uniform distribution of pixel values after encryption is desirable, as it prevents attackers from inferring information about the original image based on pixel value unevenness. Figure 2 compares the histograms of plaintext and encrypted images. The histogram of the plaintext image shows noticeable regularities and peaks, indicating a biased data distribution. In contrast, the histogram of the encrypted image demonstrates a uniform distribution with no obvious peaks or regularities. This uniformity effectively conceals the original image's information, confirming the effectiveness of the encryption.

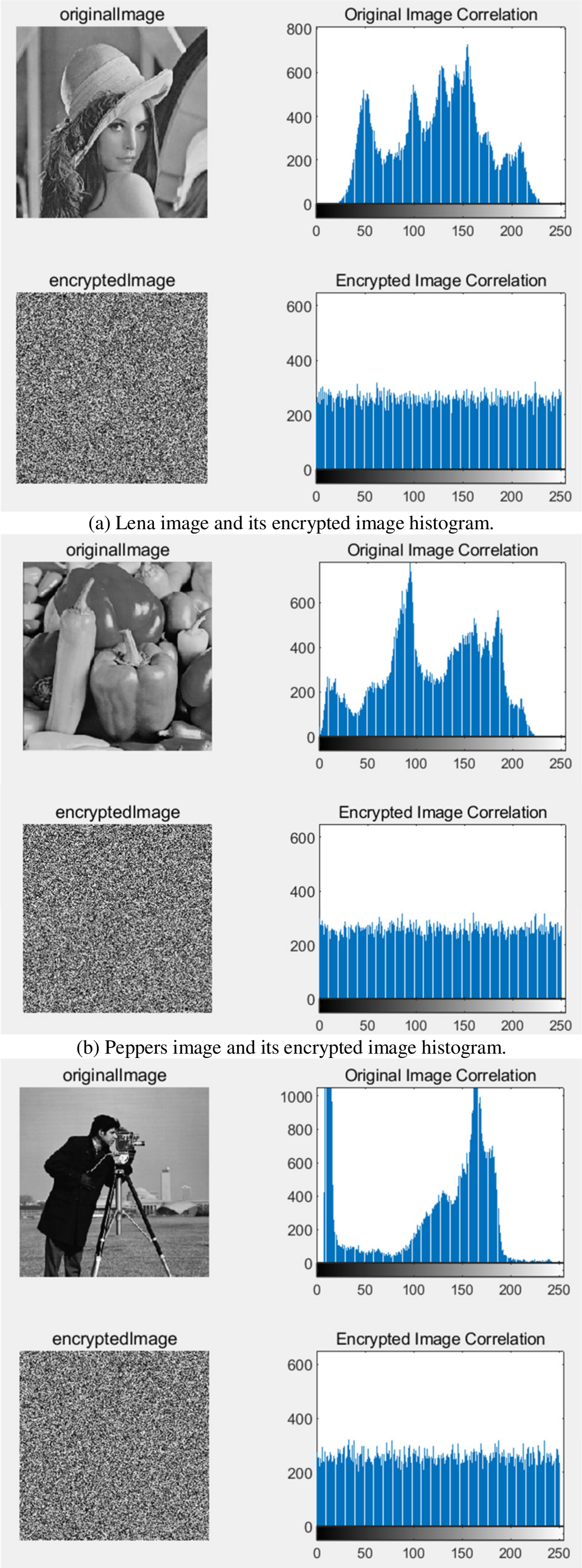
3) *Adjacent Pixel Correlation Analysis*

The correlation coefficient between neighboring pixel points measures the similarity between each pixel and its neighbors. In an image, adjacent pixel points often exhibit strong correlation due to macroscopic continuity. However, encryption disrupts this correlation, resulting in a disordered state. The correlation of adjacent pixel points in the encrypted image should be close to zero.

The following mathematical expression describes the correlation of adjacent pixel points:

$$\begin{cases} E(w) = \frac{1}{N}\sum_{i=1}^{N} w_i \\ D(w) = \frac{1}{N}\sum_{i=1}^{N}[w_i - E(w)]^2 \\ cor_{wv} = \frac{E((w_i - E(w))(v_i - E(v))}{\sqrt{D(w)D(v)}} \end{cases} \quad (2)$$

where w, v denote the pixel values of two adjacent pixels, $E(w)$ denotes the mean of each pixel, $D(w)$ denotes the corresponding variance, and cor_{wv} denotes the correlation coefficient. The pixel correlation coefficients of Lena's original image in different directions are plotted for 1000 randomly selected neighboring pixel points in Figure 3. The calculated correlation coefficients in each direction for Lena's original and encrypted images are presented in Table II.



(a) Lena image and its encrypted image histogram.

(b) Peppers image and its encrypted image histogram.

(c) Cameraman image and its encrypted image histogram.

Fig. 2. Histogram analysis.

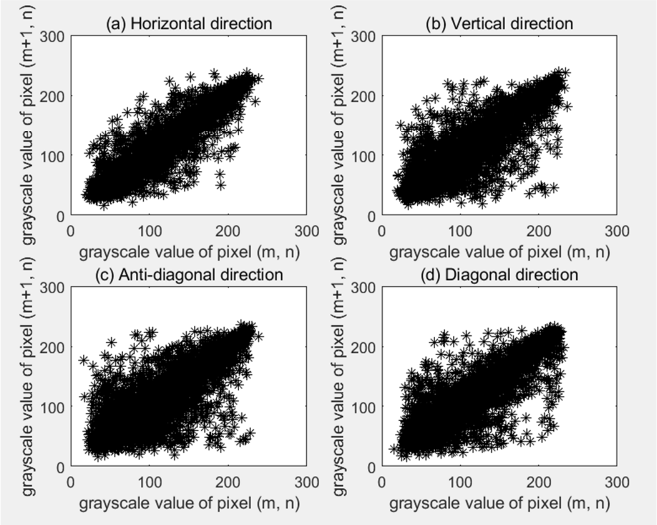


Fig. 3. Correlation coefficient plot of neighboring pixel points in different directions of Lena's original image.

TABLE II. LENA CORRELATION COEFFICIENTS OF NEIGHBORING PIXELS IN DIFFERENT DIRECTIONS

Orientation	Correlation coefficient of adjacent pixels of the original image	Correlation coefficient of adjacent pixels of the ciphertext image
Vertical	7.4519	0.0249
Diagonal	7.5937	-0.0641
Horizontal	7.3583	0.0446

Mean Squared Error (MSE) analysis is a widely used metric for measuring the difference between predicted and actual values. It evaluates the predictive performance of a model by calculating the average of the squared differences between predicted and actual values. The mathematical definition of MSE is as follows:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y_i})^{\,2} \quad (3)$$

where n is the number of data points, y_i is the i-th actual value, and $\hat{y_i}$ is the i-th predicted value. Squaring the errors ensures non-negativity and increased weight for larger errors, making the MSE sensitive to larger errors. The average of all squared errors provides an overall measure of the model's predictive performance. The MSE and the decryption time for several images are shown in Table III. As shown, the minimum MSE obtained is 3.6116, and the fifth image is selected as the output, i.e., the result of the decrypted image.

TABLE III. MSE AND DECRYPTION TIME FOR SEVERAL IMAGES

Image	MSE	Decryption time
1	3465.9665	0.0010
2	5361.7631	0.0020
3	7587.5928	0.0018
4	3179.3718	0.0010
5	3.6116	0.0020

4) Information Entropy Analysis

Information entropy reflects the unpredictability and randomness of information. For digital images, rougher images generally have higher information entropy, whereas uniformly distributed information results in smaller entropy. The experiments in this paper use a 256×256 image as the object of study, and ideally the information entropy of the image should be 8. Therefore, when the information entropy of the image is closer to 8, the image is considered more secure, i.e., it is more difficult to infer information about the original data from the image. The mathematical formula for information entropy is shown below:

$$H(m) = \sum_{j=1}^{N} p(m_j) log_2 \frac{1}{p(m_j)} \quad (4)$$

where m denotes the pixel value size of a pixel point, $p(m_j)$ denotes the probability of occurrence of the pixel m_j.

The information entropies of the original and encrypted images are shown in Table IV.

TABLE IV. INFORMATION ENTROPY ANALYSIS TABLE

Image	Information entropy of the original image	Information entropy of the encrypted image
Lena	7.4519	7.9891
Peppers	7.5937	7.9894
Cameraman	7.3583	7.9893

5) Discussion

Through in-depth analysis and comparison of experimental data, we have drawn a number of robust conclusions that further underscore the significant advantages and application potential of homomorphic encryption in the field of encrypted image data processing.

First and foremost, homomorphic encryption technology exemplifies its unparalleled efficiency in data protection and access control. Specifically, it provides a powerful security barrier around sensitive data, ensuring that only duly authorized users possess the prerogative to decrypt and access specific segments of the data. This capability not only provides a strong technological safeguard for data privacy, but also guarantees that sensitive information remains inviolable from unauthorized parties under any circumstances. By implementing this fine-grained access control mechanism, homomorphic encryption effectively promotes a secure and trustworthy data processing environment for users and organizations alike.

Second, homomorphic encryption technology has distinct advantages over traditional data encryption methods in terms of encryption speed and computational efficiency. Experimental data underscore that homomorphic encryption maintains high processing throughput even when dealing with large image data, significantly reducing the time and computational resources required for the encryption process. This characteristic renders homomorphic encryption particularly well-suited for application scenarios that impose stringent demands on processing speed and resource utilization. Whether it is securely processing vast amounts of image data in a cloud computing environment or performing data encryption tasks on resource-constrained mobile devices, homomorphic encryption offers an efficient and cost-effective solution.

Finally, homomorphic encryption stands out for its formidable privacy and security capabilities. The technology leverages encryption algorithms based on complex mathematical puzzles, thereby significantly bolstering data security and rendering it extremely difficult for adversaries to decipher the contents of the original data, even if they manage to obtain fragments of the encrypted data. This unparalleled level of security provides impregnable protection for the transmission and storage of sensitive image data, effectively mitigating the risks of information leakage and data tampering. Consequently, homomorphic encryption is widely regarded as a powerful tool for maintaining data privacy and security, and is particularly suited for domains that necessitate stringent data confidentiality, such as financial services, healthcare, and government organizations.

In conclusion, through careful analysis and comparison of experimental data, we have not only validated the effectiveness and feasibility of homomorphic encryption in the field of encrypted image data processing, but also highlighted its outstanding advantages in data protection, access control, encryption speed, and security. These findings strongly support the indispensability of homomorphic encryption as a method for safeguarding data privacy and security in the current digital era.

IV. CONCLUSIONS AND OUTLOOK

A. Conclusions

This study validates the feasibility and effectiveness of homomorphic encryption in secure image data processing. The proposed framework provides a robust solution for protecting sensitive information while enabling efficient data processing and analysis. Future research will focus on optimizing homomorphic encryption algorithms for large-scale datasets and exploring its application in other domains, such as video and text encryption.

First, homomorphic encryption technology demonstrates its superiority in preserving data confidentiality and ensuring that sensitive information remains inaccessible to unauthorized third parties, even in public or insecure environments. This encryption method enables computational operations to be performed directly on encrypted data, eliminating the need for decryption, thereby significantly reducing the risk of data leakage.

Second, the study highlights that homomorphic encryption facilitates highly granular access control mechanisms. This implies that system administrators can establish intricate access rights to ensure that only authorized users with the appropriate privileges can decrypt and access specific portions of the data. This flexibility is crucial when managing large databases or image collections containing multiple levels of sensitive information, as it allows for tight restrictions and monitoring of data usage without compromising its availability.

In summary, this paper, through an in-depth investigation of homomorphic encryption in the context of encrypted image data processing, not only validates its merits in protecting data confidentiality, enabling fine-grained access control, and enhancing encryption speed and security but also anticipates its broad application prospects in the field of data protection. Given the increasing importance of data security and privacy, homomorphic encryption, as an efficient and reliable encryption technique, will undoubtedly play an increasingly pivotal role in safeguarding encrypted image data and other sensitive information.

B. Outlook

Although homomorphic encryption has achieved notable results in encrypting images containing sensitive data, we still face several challenges and there is ample room for improvement. Nevertheless, future research holds a promising outlook for advancing homomorphic encryption.

First, we can further enhance the performance and efficiency of homomorphic encryption algorithms to meet the requirements of encrypting large-scale image datasets. By optimizing the algorithms and incorporating more advanced computing techniques, we aim to reduce the time required for encryption and decryption processes, thereby improving the overall system's responsiveness and efficiency.

Second, we can explore the application of homomorphic encryption in other domains, such as video encryption and text encryption. Extending the principles and methodologies of homomorphic encryption to a broader range of data types can provide robust protection for diverse and sensitive information. This endeavor will undoubtedly contribute to the wider adoption and application of homomorphic encryption across various fields.

Furthermore, the security and reliability of encrypted images can be further enhanced by integrating them with other security technologies, such as digital watermarking and authentication mechanisms. By combining homomorphic encryption with these complementary security measures, we can establish a robust security framework that effectively mitigates the risks of data breaches and unauthorized access. This, in turn, will empower users with more reliable data protection solutions and foster the development of robust data privacy protection frameworks.

V. SUMMARY

Data-encrypted images are an important tool for protecting the confidentiality of sensitive information. This paper explores the application of homomorphic encryption to data-encrypted images and demonstrates its feasibility and effectiveness through empirical data and comprehensive analysis. Homomorphic encryption offers a robust solution for achieving efficient data protection and implementing fine-grained access control, all while maintaining high encryption speeds and ensuring security. Looking ahead, future research efforts could extend the exploration of homomorphic encryption to other domains and seek to integrate it with complementary security technologies, thereby continuously enhancing the security and reliability of data-encrypted images.

REFERENCES

[1] K. Rajeshkumar, C. Ananth, and N. Mohananthini, "Blockchain-Assisted Homomorphic Encryption Approach for Skin Lesion Diagnosis using Optimal Deep Learning Model," *Engineering, Technology & Applied Science Research*, vol. 13, no. 3, pp. 10978–10983, Jun. 2023, https://doi.org/10.48084/etasr.5594.

[2] S. Jumonji, K. Sakai, M.-T. Sun, and W.-S. Ku, "Privacy-Preserving Collaborative Filtering Using Fully Homomorphic Encryption," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 3, pp. 2961–2974, Mar. 2023, https://doi.org/10.1109/TKDE.2021.3115776.

[3] J. L. Raisaro *et al.*, "Protecting Privacy and Security of Genomic Data in i2b2 with Homomorphic Encryption and Differential Privacy," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1413–1426, Sep. 2018, https://doi.org/10.1109/TCBB.2018.2854782.

[4] M. Kim, Y. Song, S. Wang, Y. Xia, and X. Jiang, "Secure Logistic Regression Based on Homomorphic Encryption: Design and Evaluation," *JMIR Medical Informatics*, vol. 6, no. 2, Apr. 2018, Art. no e8805, https://doi.org/10.2196/medinform.8805.

[5] P.-E. Clet, O. Stan, and M. Zuber, "BFV, CKKS, TFHE: Which One is the Best for a Secure Neural Network Evaluation in the Cloud?," in *19th International Conference on Applied Cryptography and Network Security*, Kamakura, Japan, 2021, pp. 279–300, https://doi.org/10.1007/978-3-030-81645-2_16.

[6] H. Shekhawat, S. Sharma, and R. Koli, "Privacy-Preserving Techniques for Big Data Analysis in Cloud," in *2019 Second International Conference on Advanced Computational and Communication Paradigms*, Gangtok, India, 2019, pp. 1–6, https://doi.org/10.1109/ICACCP.2019.8882922.

AUTHORS PROFILE

Qiang Chen is studying as a Ph.D. student at the College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia and works as a teacher at the Dongguan City University, China. His areas of expertise are big data and data encryption.

Huixian Li is studying as a Ph.D. student at the College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia and works as a teacher at the College of Financial Technology, Hebei Finance University, Baoding, China. Her areas of expertise are data encryption, privacy protection, and blockchain

Suriyani Binti Ariffin is working as a Professor at the College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia. Her areas of expertise are Information and Communication Technology (ICT) and cryptography for security systems.

Nor Atiqah Bte Mustapa is working as a Professor at the College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia. Her areas of expertise are Information and Communication Technology (ICT), software engineering, and software metrics.