Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 15, No. 2, 2024

Enhancing Security in CNN-Based Travel Recommendation Models Using CKKS Homomorphic Encryption

Tianhao Chen

Quanzhou University of Information Engineering, Quanzhou, China
1151863354@qq.com

Abstract: This study explores the integration of CKKS homomorphic encryption with convolutional neural networks (CNNs) to enhance the security of travel recommendation systems. By adapting CNN architectures to operate efficiently on encrypted data using CKKS, we address the challenge of maintaining the users' privacy without compromising system performance. Key results indicate significant improvements in data security with minimal impact on recommendation accuracy.

Keywords: Homomorphic Encryption; Convolutional Neural Networks; Travel Recommendations; Data Security; Privacy Preservation.

1. Introduction

The rise of personalized travel recommendation systems has led to increasing concerns over user data privacy. Traditional encryption methods secure data at rest but fail to protect data during computation, limiting the functionality of recommendation systems. Travel recommendation systems handle diverse and sensitive data types, including user location, travel history, preferences, budget, personal information, and user-generated content such as reviews and images. This study aims to implement CKKS homomorphic encryption within CNNs to allow computations on encrypted data, enhancing user privacy without sacrificing the accuracy of recommendations. Homomorphic encryption enables secure processing of encrypted data, allowing operations to be performed without revealing the underlying information. By integrating CKKS with CNNs, this study addresses the critical need for privacy-preserving computations in the travel industry, where sensitive data must be safeguarded against breaches. This research's significance lies in its potential to set a new standard for privacy in data-driven industries, particularly in the travel sector, providing a robust framework for secure, privacy-preserving data analysis and recommendation generation.

2. Literature Review

Existing studies have focused on securing recommendation systems either by enhancing data encryption techniques or by modifying machine learning algorithms for better privacy-preserving properties[1]. For instance, less computationally intensive homomorphic encryption schemes like Paillier and ElGamal have been applied but faced limitations in handling the complex data types and operations required by modern CNNs[2]. This study builds on existing literature by integrating CKKS encryption, which supports more complex arithmetic operations on encrypted data, naturally fitting the demands of CNN-based systems.

3. Research Method

The research was conducted in three phases: CNN model adaptation, integration with CKKS encryption and performance evaluation. Each phase involves specific steps and technical details to ensure the feasibility of encrypted computation without compromising recommendation system's performance.

4. CNN Model Adaptation

To make CNN models more compatible with CKKS homomorphic encryption, we implemented the following optimizations:

4.1. Reducing Network Layers and Parameters.

We first optimized the standard CNN architecture by reducing the number of network layers and parameters. The goal of this step is to lower computational complexity, making efficient computation possible in a certain homomorphic encryption environment. The specific steps are as follows:

- Removing Redundant Layers. In the original model, we identified layers that contributed minimally to the final performance through experimental analysis. These redundant layers were removed. For example, the original model had five convolutional layers. Experimental results showed that the last two layers contributed minimally to performance, so they were removed.
- Reducing Convolutional Filters. In the retained convolutional layers, we optimized the number of convolutional filters. For example, the original model's first convolutional layer had 64 filters; we reduced this to 32. Experimental results confirmed that this adjustment had an acceptable impact on model performance.
- Adjusting Convolutional Kernel Size. Reducing the convolutional kernel size further lowers computational complexity. For example, changing the kernel size from 3x3 to 2x2 may slightly impact feature extraction but significantly reduces computational complexity in an encrypted environment.

4.2. Activation Function Adjustment

CKKS homomorphic encryption supports polynomial operations, so non-linear activation functions (such as ReLU) need to be replaced with functions suitable for polynomial approximation[3]. We used Chebyshev polynomials for approximation and performed detailed verification. Chebyshev polynomials are a class of orthogonal polynomials widely used in function approximation[4]. They can be generated using a recursive formula and are known for minimizing the maximum error, making them suitable for approximating complex non-linear functions.

We used a third-order Chebyshev polynomial to approximate the ReLU function. The third-order Chebyshev polynomial is given by:

$$T_3(x) = 4x^3 - 3x \tag{1}$$

By fitting this polynomial to the ReLU function, we can approximate it as:

$$\mathrm{ReLU}(x) \approx \sum_{i=0}^{n} a_i T_i(x) \tag{2}$$

where ai are the coefficients of the Chebyshev polynomials, obtained through least squares fitting.

4.3. Regularization and Normalization

To further enhance model stability and performance, we introduced regularization techniques (Dropout and L2 regularization) and Batch Normalization to ensure convergence and robustness during training.

- Adding Dropout layers in fully connected layers to prevent overfitting. For example, we add a Dropout layer with a rate of 0.5 before the final fully connected layer.
- Adding L2 regularization to the weights of convolutional and fully connected layers with a weight decay coefficient of 0.01.
- Adding Batch Normalization layers after each convolutional layer to accelerate model convergence and improve generalization.

4.4. Multi-modal Data Processing

Travel recommendation needs to process text data, images, and reviews. These data types require different processing methods. We integrated multi-modal data processing into the CNN model to handle encrypted text, images, and reviews, providing more comprehensive recommendation services.

- Preprocessing images with normalization and data augmentation, followed by feature extraction using CNN.
- Tokenizing and vectorizing user reviews, followed by embedding and feature extraction using CNN.
- Merging image and text features in the fully connected layers and validating their effectiveness in an encrypted computation environment.

Through these optimizations, we ensured the efficiency and performance of the CNN model in the CKKS homomorphic encryption environment while minimizing the impact on model accuracy. Specific experimental results and detailed optimization steps will be presented and discussed in the performance evaluation section.

5. Integration with CKKS Encryption

CKKS (Cheon-Kim-Kim-Song) is a homomorphic encryption scheme supporting floating-point operations on encrypted data. Its main advantage is enabling addition and multiplication operations on encrypted data, suitable for complex computational applications[5].

During training and inference, we first encrypted the input data using CKKS. This step includes data preprocessing, encoding, and encryption to ensure the data remains encrypted throughout the computation.

To ensure the entire CNN computation occurs in the encrypted domain, we also encrypted the model's weights and bias parameters. This requires encrypted updates during training and using encrypted parameters during inference.

Using CKKS-encrypted data and parameters, we performed encrypted forward and backward propagation in the CNN. This involved implementing encrypted computations for convolution operations, pooling, and fully connected layers. We utilized the basic operations provided by the CKKS library, combined with polynomial approximation methods, to ensure the correctness and efficiency of the computations.

6. Experimental Validation

Train CNN models on standard datasets, using both ReLU and polynomial-approximated activation functions, and compare their performance. In addition, compare training and validation loss and accuracy to verify the effectiveness of the polynomial activation function. In the optimized CNN, replace ReLU with the polynomial-approximated activation function and retrain and test the model. Compare the training time, computational overhead, and model performance for both activation functions.

- The accuracy metric represents the proportion of correct recommendations, specifically referring to the number of recommended items that align with user preferences. The encrypted model achieves an accuracy rate of 85%, while the unencrypted model attains 87% accuracy.
- The recall rate represents the proportion of recommended items that are actually liked by the user, i.e. the number of recommended liked items out of all liked items. The recall rate for the encrypted model is 82%, while the recall rate for the unencrypted model is 84%.
- The F1 score represents the harmonic mean of precision and recall, serving as a metric to evaluate the overall performance of a recommendation system. The encrypted model achieved an F1 score of 83.5%, while the unencrypted model scored 85%.
- Training time refers to the total duration required for model training. The encryption process adds 10 hours to the training time, whereas training the unencrypted model takes 8 hours.
- The inference time denotes the total duration necessary for the model to generate predictions on the test dataset. The encrypted model requires 5 seconds per prediction for inference, whereas the unencrypted model takes 3 seconds per prediction.
- Encryption time refers to the duration required for data encryption, with each batch of data taking 2 seconds.
- Decryption time refers to the duration needed for decrypting data, with each batch of data requiring 1 second.

The experiments were carried out on high-performance computing platforms, leveraging robust GPUs and multi-core CPUs to ensure efficient handling of the high-complexity encryption-based calculations. We employed deep learning frameworks such as TensorFlow and PyTorch, along with the Microsoft SEAL library supporting CKKS encryption, to

achieve effective implementation and evaluation of encrypted CNN models.

7. Results

The experimental validation demonstrates that using Chebyshev polynomial-approximated activation functions in a CNN model for travel recommendation systems is viable. The approximation maintains the model performance and the generalization capability while enabling encrypted computations. These results validate that the polynomial-approximated activation function can effectively replace the standard ReLU function without significant drawbacks, making it suitable for use in privacy-preserving computations with CKKS homomorphic encryption.

8. Safety Analysis

By employing CKKS encryption, data remains encrypted throughout the entire computation process, ensuring the non-disclosure of sensitive user information. This approach offers enhanced confidentiality compared to traditional encryption methods that only encrypt data in a static or transmission state.

The encrypted CNN model has undergone rigorous testing against a range of potential attacks, including plaintext and ciphertext attacks. The findings demonstrate that the CKKS-based encryption significantly bolsters the system's resilience, rendering it challenging for adversaries to extract meaningful information from the encrypted data.

Despite the computational overhead associated with homomorphic encryption, our optimized CNN model design is aimed at minimizing its impact. We carefully manage the trade-off between security and performance to ensure that the system remains practical for real-world applications.

9. Conclusion

By integrating CKKS homomorphic encryption with optimized CNN models, the travel recommendation system can conduct computations on encrypted data, significantly bolstering its security. The research findings demonstrate that, through meticulous design, it is feasible to achieve robust data protection without compromising system performance. This approach not only contributes to the theoretical framework for secure data processing but also offers a practical roadmap for implementing enhanced privacy protection measures in travel recommendation services.

10. Future Issues

In the future, our research will explore the following avenues to further enhance the security and efficiency of the travel recommendation system using CKKS homomorphic encryption and optimized CNN technology:

- Evaluate the impact of encryption recommendation systems on user experience, ensuring that heightened security measures do not adversely affect user availability and satisfaction[6].
- Exploring advanced optimization techniques to minimize the computational overhead associated with cryptographic computing, such as model pruning, quantization, and efficient hardware utilization, can enhance the scalability and applicability of the proposed methods to larger data sets and more complex models.
- Improved energy efficiency in encrypted computing is the focus of current research. With the growing computational demands of homomorphic encryption, optimizing energy consumption becomes essential for sustainable deployment in large-scale systems.
- Conducting more in-depth robustness and security analysis of encryption models, including both theoretical and empirical research, will help identify potential vulnerabilities and strengthen the overall security framework.

References

[1] Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. Neurocomputing, 384, 21-45.

[2] Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2016, June). Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In International conference on machine learning (pp. 201-210). PMLR.

[3] Akram, A., Khan, F., Tahir, S., Iqbal, A., Shah, S. A., & Baz, A. (2024). Privacy Preserving Inference for Deep Neural Networks: Optimizing Homomorphic Encryption for Efficient and Secure Classification. IEEE Access.

[4] Peijia Zheng, Zhiwei Cai, Huicong Zeng, and Jiwu Huang. 2022. Keyword Spotting in the Homomorphic Encrypted Domain Using Deep Complex-Valued CNN. In Proceedings of the 30th ACM International Conference on Multimedia (MM '22). Association for Computing Machinery, New York, NY, USA, 1474–1483.

[5] N. Jain, K. Nandakumar, N. Ratha, S. Pankanti and U. Kumar, "Optimizing Homomorphic Encryption based Secure Image Analytics," 2021 IEEE 23rd International Workshop on Multimedia Signal Processing (MMSP), Tampere, Finland, 2021, pp. 1-6, doi: 10.1109/MMSP53017.2021.9733620.

[6] Park, J., Kim, D., Kim, J., Kim, S., Jung, W., Cheon, J. H., & Ahn, J. H. (2023). Toward practical privacy-preserving convolutional neural networks exploiting fully homomorphic encryption. arXiv preprint arXiv:2310.16530.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.