A Data Augmentation Technique for Perceptual Encryption-Based Privacy Preserving Medical Image Analysis

Ijaz Ahmad, Seokjoo Shin*

Korea University, *Chosun University (Corresponding author)

ijaz@korea.ac.kr, *sjshin@chosun.ac.kr

지각 암호화 기반의 개인정보보호 의료영상 분석을 위한 데이터 증강 기법

아흐마드 이자즈, 신석주*
고려대학교, *조선대학교

Abstract

Perceptual Encryption (PE) hides human identifiable information in images while producing cipher images that are machine readable. The encryption steps have low computational complexity which makes them suitable for encrypting large volumes of image data. These methods have been successfully implemented in various domains for protecting privacy sensitive information and the data ownership. However, for privacy-preserving deep learning (PPDL) applications there is a slight degradation in the model performance on cipher images compared to that of the plain images. In this study, we propose to exploit the geometric transformation function of a PE scheme for an offline data augmentation technique. The proposed augmentation can be carried out in the encryption domain on the server side; therefore, does not incur any additional communication cost and avoids the necessity of sharing the secret key information. The simulation analyses have shown that with our proposed augmentation scheme, the error in accuracy for PE-based PPDL scheme is reduced to 1.8% compared to 3.2% for COVID-19 detection in CXR images.

Ⅰ. Introduction

Training a powerful deep learning (DL) algorithm requires high computational resources and depends on a large volume of relevant sample data. This poses challenges in adopting DL-based solutions in domains where it is difficult and expensive to acquire enough data to train a DL model. Cloud services such as computation and storage resources, provide an efficient solution to meet the aforementioned challenges faced in implementing DL solutions. However, with the avail of such third-party owned services there are associated security and privacy risks. For example, the data must be protected during transmission between a client and service provider. In addition, when the data consist of identifiable information then it should be kept protected from the service providers to ensure users' privacy. Though, traditional full encryption techniques are proven to be the most secure choices for protecting image data, they perform encryption in such a way that the images are rendered useless. Therefore, perceptual encryption (PE) schemes [1] are being proposed to hide only perceivable information in images while leaving their intrinsic characteristics intact, which can be used to enable computer vision applications in the encryption domain such as privacy-preserving deep learning (PPDL) for medical image analysis [2].

PE-based PPDL schemes are non-interactive which require only one round of transmission and they are compatible with the state-of-the-art DL models. Despite these advantages, they suffer DL model performance up to 3% [2]. Therefore, we proposed a data augmentation technique that take advantage of geometric transformation of PE schemes. To validate the performance of our method, we considered a PE-based PPDL scheme for the COVID-19 detection in chest x-ray (CXR) images.

Ⅱ. Methods

a. Perceptual Encryption Method

For a grayscale image $\boldsymbol{I}^{H,W}$, whose dimensions are H rows, and W columns, a block-based PE algorithm consists of the following steps [1]:

Step 1). Divide $\boldsymbol{I}^{H,W}$ into $L \times M$ nonoverlapping blocks with $L = H/N$ and $M = W/N$, and N^2 is a block size.

Step 2). Shuffle block positions through random key $\boldsymbol{K}_1$.

Step 3). Randomly change each block orientation in the shuffled image by using key $\boldsymbol{K}_2$ where its entries represent rotation and flip axis.

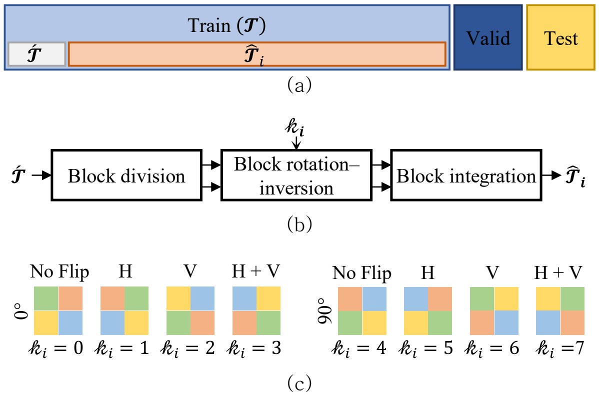

Fig. 1. Proposed augmentation technique that changes block orientations in the encryption domain. (a) is dataset split, the block-based transformation function is in (b) and its rules on a 2×2 block size are in (c). H: horizontal axis and V: vertical axis, $\acute{\boldsymbol{\mathcal{T}}}$: the original training dataset, $\hat{\boldsymbol{\mathcal{T}}}_i$: $\acute{\boldsymbol{\mathcal{T}}}$ transformed with $\mathscr{k}_i$, $\mathscr{k}_i \in \boldsymbol{\mathcal{K}}_a = \{0,1,\ldots,7\}$: is the transformation key with rules specified in (c) and $\boldsymbol{\mathcal{T}} = \{\acute{\boldsymbol{\mathcal{T}}} \cup \hat{\boldsymbol{\mathcal{T}}}_i\}$: is the augmented dataset.

Step 4). Modify each pixel $p_{(s,t)}, \{s,t = 1,2,\ldots,N\}$ value of the i^{th} block randomly chosen by a uniformly distributed key $\boldsymbol{K}_{3(i)}$ as

$$\hat{p}_{(s,t)} = \begin{cases} p_{(s,t)} & \boldsymbol{K}_{3(i)} = 0 \\ 255 - p_{(s,t)} & \boldsymbol{K}_{3(i)} = 1. \end{cases} \qquad (1)$$

b. Proposed Data Augmentation Method

Data augmentation is one of the techniques that has been developed to avoid overfitting in DL models. The traditional techniques perform basic geometric transformations and/or color conversions on the entire image (*image-level methods*) or on specific patches in an image (*patch-level methods*) thus limits the diversity of feature representation [3]. Inspired from PatchMix [3], we proposed to augment each block in the PE cipher image using its rotation-inversion function using $\boldsymbol{\mathcal{K}}_a$ as shown in Fig. 1. For $\boldsymbol{\mathcal{K}}_a = 0$, the original orientation of blocks in the cipher image is preserved.

Ⅲ. Results and Discussion

In our simulations, we have used a publicly available CXR image dataset [4] that have 4,626 images uniformly distributed between two classes: healthy and COVID-19. The dataset was divided into 80% for training, and 10% for each validation and test. Following [2], all the images were preprocessed and resized. In addition, the whole dataset was encrypted with the PE method (8×8) and the training set was augmented as described in Section 2. For comparison, we have benchmarked our proposed augmentation technique against [2] that implements the conventional augmentation technique that transforms the whole image. Specifically, in [2] the training set was augmented using random flip, rotation, zoom, contrast, and translation transformations. In our simulations, we implemented EfficientNetV2-B0 [5] for binary classification with training setup described in [2].

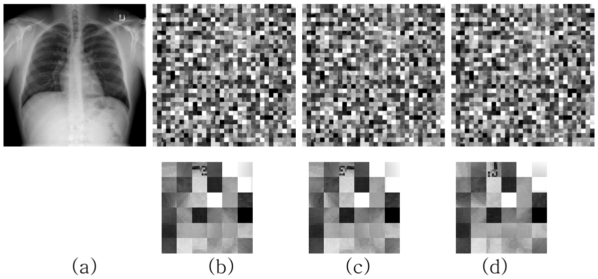

Fig.2. An example image from the dataset. (a) plain image (b) cipher image, and (c) and (d) are the augmented images of (b). The bottom right corner of (b)(c) and (d) are shown below each image.

Table 1 summarizes the performance of our DL model in-terms of binary accuracy. The accuracy score of each method is reported as a mean value of 3 runs on the test set. Overall, the model achieved high performance on the plain images. On the other hand, when PE method is implemented for PPDL with conventional augmentation technique then there is a 3.2% accuracy difference while for proposed augmentation scheme the difference is reduced to 1.78%.

TABLE I. Performance analysis of proposed augmentation technique in-terms of accuracy. The values are reported as mean (black) and standard deviation (gray) for 3 runs.

Plain	[2]	Proposed
98.78±0.31	95.56±0.14	97.0±0.01

IV. Conclusion and Future Work

This study proposed a data augmentation technique specifically designed for PE-based PPDL schemes. The simulation analysis on CXR image dataset showed that our proposed scheme improved their performance.

Tailoring our data augmentation scheme to enable the use of different keys in PE schemes for training and testing could be an interesting future research direction.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government. (MSIT) (RS-2023-00278294).

REFERENCES

[1] K. Kurihara, S. Shiota, and H. Kiya, "An encryption-then-compression system for JPEG standard," in 2015 Picture Coding Symposium (PCS), Cairns, Australia: IEEE, May 2015, pp. 119–123. doi: 10.1109/PCS.2015.7170059.

[2] I. Ahmad and S. Shin, "Perceptual Encryption-based Privacy-Preserving Deep Learning for Medical Image Analysis," in 2023 International Conference on Information Networking (ICOIN), Bangkok, Thailand: IEEE, Jan. 2023, pp. 224–229. doi: 10.1109/ICOIN56518.2023.10048970.

[3] Y. Hong and Y. Chen, "PatchMix: Patch-Level Mixup for Data Augmentation in Convolutional Neural Networks." Nov. 17, 2023. doi: 10.21203/rs.3.rs-3612931/v1.

[4] "COVID19_Pneumonia_Normal_Chest_Xray_PA_Dataset." Accessed: Sep. 22, 2022. [Online]. Available: https://bit.ly/3SpBxTy

[5] M. Tan and Q. V. Le, "EfficientNetV2: Smaller Models and Faster Training," ArXiv210400298 Cs, Jun. 2021, Accessed: May 10, 2022. [Online]. Available: http://arxiv.org/abs/2104.00298