Perceptual Encryption-Based Image Communication System for Tuberculosis Diagnosis

Subjects: Computer Science, Artificial Intelligence | Computer Science, Information Systems

Contributor: Ijaz Ahmad , Seokjoo Shin

Block-based perceptual encryption (PE) algorithms are becoming popular for multimedia data protection because of their low computational demands and format-compliancy with the JPEG standard. In conventional methods, a colored image as an input is a prerequisite to enable smaller block size for better security. However, in domains such as medical image processing, unavailability of color images makes PE methods inadequate for their secure transmission and storage. A PE method that is applicable for both color and grayscale images is proposed. The EfficientNetV2-based model is implemented for automatic tuberculosis (TB) diagnosis in chest X-ray images.

perceptual encryption JPEG standard EfficientNetV2 deep learning tuberculosis diagnosis

1. Introduction

Cloud services provide a cost-effective solution to meet the Information and Communication Technology (ICT) needs of an organization. The organization can use ICT resources, services and software of a Cloud Services Provider (CSP) via the internet without a necessity of internal infrastructure or hardware on-site installations. With the recent success of Machine Learning (ML) in the field of computer vision, automatic computer aided diagnosis (CAD) systems have emerged in healthcare organizations to assist doctors and practitioners. Particularly, Deep Learning (DL), a subfield of ML, has achieved state-of-the-art performance for image classification [1]. However, DL models are compute-intensive tasks, and their training requires cutting-edge technology and high computational resources. In this regard, healthcare organizations can avail cloud-computing services to access the latest technology in order to speed up the training process and allow DL models to scale efficiently with a lower capital cost [2][3]. In addition, training DL models requires a large volume of sample data, which in some cases such as the medical domain, is expensive and difficult to acquire. To overcome this issue, healthcare organizations can benefit from a community cloud, where services are shared by organizations with common interests. In this case, cloud storage services can be used as a shared central data repository for joint projects and collaboration among the organizations. However, like all communication systems, when data are outsourced for cloud services, there is always a risk of information leakage and a large volume of data requires high bandwidth [4][5][6][7].

Compression and encryption are two processes that satisfy the dual requirements of data transmission over bandwidth constraint and public channels. Image compression gives a compact representation to an image such

that it requires less number of bits. It can be achieved either in lossless or lossy mode. In lossless compression, an image can be recovered with almost the same quality as that of the original image, whereas in lossy mode the image quality degrades. Compared to lossless mode, lossy compression offers better savings; however, resulting quality degradation in lossy mode may not be acceptable in certain domains. For example, medical images contain information crucial for correct diagnosis of diseases; therefore, their compression should be carried out in such a way that the diagnostic information remains intact in them while their sizes are reduced [8][9][10]. One of the popular approaches to achieve this goal is to compress the region-of-interest (ROI) necessary for diagnosis in lossless mode and non-ROI in lossy mode [8][9][10]. Such methods can achieve a significant reduction in the image size while preserving its important details. However, they require segmentation of an image beforehand, which is computationally expensive and is a target task to be performed using cloud-computing resources. Therefore, ROI-based methods are not suitable for efficient image data transmission [2].

Encryption makes image data unintelligible, which can only be recovered by its inverse decryption process. The number theory and chaos theory-based encryption algorithms are proven efficient for securing image data [2]. These conventional encryption algorithms perform stream encryption and/or scrambling of pixel values; however, they are only suitable for encrypting raw images. For example, the JPEG compressed image consists of format markers and any changes in them by an external operation will leave the image uninterpretable. Similarly, re-encoding a cipher image as a JPEG image results in file size increment. Different from other form of data, encryption of image data can be carried out only by disrupting their intrinsic properties. For example, changing pixel correlation and/or redundancy in an image can result in an unintelligible image with a necessary level of security. Based on this observation, a new class of encryption algorithms has been emerged called Perceptual Encryption (PE) algorithms to meet the aforementioned requirements of encrypting compressed images. The main idea is to reverse the conventional order of performing compression prior to encryption. PE performs block-based operations that hides only perceptual information of an image, thereby preserves image intrinsic properties necessary to carry out computations in the encryption domain. For example, refs. [11][12] proposed PE methods for enabling privacy-preserving DL applications. In addition, PE cipher images are JPEG compressible, which makes them suitable for numerous applications, such as cloud photo storage and social networking services [13][14] and image retrieval in the encryption domain [15]. Nonetheless, PE methods are resilient against various attacks, including brute-force and cipher-text-only attacks [16].

Based on an input image representation, PE methods can be grouped as Color-PE and Grayscale-PE methods. The Color-PE represents an input color image as a three-component image and uses same encryption keys for each component [17], whereas their extended versions encrypt each color component independently [12][18]. The latter methods have larger keyspace as they have increased number of blocks. However, this increment is limited by the smallest allowable block size in the JPEG algorithm, for instance, block size no smaller than 16 × 16 should be used for color image compression. This recommended size is necessary to avoid block artifacts resulted from the JPEG chroma-subsampling step [2]. Smaller block size such as 8 × 8, can be utilized in the JPEG algorithm without any adverse effect, for compression of grayscale images. Therefore, to exploit the smaller block size for an expanded keyspace, Grayscale-PE represents color input as a pseudo-grayscale image by combining the color

components along the horizontal or vertical direction [13][14]. Overall, in conventional methods, color image as an input is a prerequisite for better security.

2. Deep Learning-Based Tuberculosis Screening

Grivkov et al. [19] implemented InceptionNetV3 [20] for diagnosis of TB in Shenzhen (SH) and Montgomery (MG) datasets [21] and achieved 86.8% accuracy. Das et al. [22] exploited transfer learning to improve InceptionV3 accuracy to 91.7% on the same datasets. Priya et al. [23] implemented transfer learning on VGG19 [24], ResNet50 [25], DenseNet121 [26] and InceptionV3 models. In their analysis, pre-trained VGG19 has achieved 89% and 95% best accuracies on MG and SH datasets, respectively. Cao et al. [27] implemented DenseNet121, VGG and ResNet152 [25] models and achieved best accuracy of 90.38% classification accuracy with DenseNet121. Raman et al. [28] adopted somewhat different approach than the aforementioned methods. They have used three pre-trained models (ResNet101 [25], VGG19, and DenseNet201 [26]) to extract features from CXR images and use eXtreme Gradient Boosting (XG-Boost) (1.6.1, Tianqi Chen and Carlos Ernesto Guestrin, Seattle, WA, USA) [29] model to classify TB and non-TB in them. In their experiments, DenseNet201 with XG-Boost architecture achieved the highest accuracy of 99.92% as compared to its counterparts. Munadi et al. [30] proposed to enhance CXR quality before feeding them to pre-trained ResNet and EfficientNet [31] models. They have used three different image-enhancing techniques (unsharped masking, high-frequency emphasis filtering, and contrast limited adaptive histogram equalization). In their analysis, EfficientNet with unsharped masking image enhancement achieved 89.92% accuracy on SH dataset. Msnoda et al. [32] implemented ResNet, GoogLeNet [33], and AlexNet [34] with an extra Spatial Pyramid Pooling (SPP) [35] layer. Among the implemented architectures, GoogLeNet achieved the highest classification accuracy of 97%, which was then improved to 98% by using the SPP layer.

The methods discussed so far rely on the architecture of an individual model for classification efficiency. There are methods that combine two or even more models to form an ensemble network to achieve better performance. For example, Rajaraman et al. [36] implemented VGG16, InceptionResNetV2 [37], InceptionV3, XceptionNet [38] and DenseNet121, and then ranked them based on their accuracy. In their experiments, the top-3 models were InceptionV3 (accuracy = 94%), DenseNet121 (accuracy = 92.8%) and InceptionResNetV2 (accuracy = 92.5%). They have evaluated multiple ensemble methods to combine the top-3 models such as majority voting, simple averaging, weighted averaging stacking and blending to make an ensemble network. Their analysis showed that stacking ensemble demonstrated better performance and achieved 94.1% accuracy. Dasanayaka et al. [39] have implemented an ensemble of only two models (VGG16 and InceptionV3), and achieved 97.10% accuracy, which is higher than the ensemble of the three models proposed in [36]. Oloko-Oba et al. [40] have implemented an ensemble of VGG16, ResNet50 and InceptionV3 and achieved best accuracy of 96.14%. In their other study [41], they have explored ensemble of EfficientNets [31] for the diagnosis of TB. In their analysis of individual models, EfficientNet-B4 achieved best accuracy of 94.35% on SH dataset, which was then improved to 97.44% through ensemble learning. The ensemble was built by averaging the performance of three best individual EfficientNets (B2, B3, and B4). Saif et al. [42] proposed to combine the traditional hand-engineered feature with an ensemble of DenseNet169, ResNet50 and InceptionV3 models. Their ensemble model has achieved best accuracy of 99.7% on

SH dataset. Overall, ensemble methods have shown superior performance for TB screening in CXR images than the individual models.

3. Perceptual Encryption Methods

The PE algorithm is block-based and performs four steps: *blocks permutation, rotation and inversion, negative and positive transformation, and color channel shuffling*. Based on these steps, several methods have been proposed in literature. They can be classified as Color-PE and Grayscale-PE methods based on their input image representation. In Color-PE methods, an input color image is represented as a three-component image, whereas Grayscale-PE methods represent an input as pseudo-grayscale image by concatenating its color components along the vertical or horizontal direction. In Grayscale-PE methods, the channel-shuffling step is omitted. This section provides a summary of PE related work.

Kurihara et al. [17] proposed a block-based Color-PE method that performs the encryption steps on each color component by using the same key. Since, the input is a color image, larger block size is used to avoid block artifacts in a decoded image resulted by chroma subsampling of the JPEG algorithm. However, the use of the same key for each color component and larger block size result in a smaller number of blocks, which make the scheme vulnerable to jigsaw puzzle attack. To increase the number of blocks for better security, Imaizumi et al. [43] proposed to perform the first three steps of encryption independently in each color component. As a result, the scheme has a larger key space than that of [17]; however, processing each component individually results in the JPEG compatibility issues. For example, the method is only applicable with the JPEG lossless algorithm only when using RGB colorspace. Ahmad et al. [12][18] proposed a PE method to deal with the compatibility issue of [43]. In their proposed schemes, rotation, inversion and pixel values transformations are performed on each color component independently. The use of a same key for permutation step in each component allows the JPEG algorithm with YCbCr colorspace for better compression savings. The extended PE methods in [12][18][43] have better security than the PE method proposed in [17] as the keyspace is expanded and color distribution is altered significantly. However, the main limitation of extended PE methods is that they cannot exploit the JPEG chroma subsampling.

An alternative approach has been adopted by Chuman et al. [13] that allows the use of a smaller block size. The main idea is to represent an input color image as a pseudo grayscale image by concatenating the color components along the horizontal or vertical direction; therefore, belongs to Grayscale-PE methods. Such representation allows use of a smaller block size without any adverse effect on the decoded image quality and compression savings. In addition to smaller block size, lack of color information improves robustness against jigsaw puzzle solver attack. When chroma subsampling is desirable, Sirichotedumrong et al. [14] proposed to convert input image from RGB to YCbCr colorspace, perform down sampling on the color components and then concatenate them with the luminance component. For example, to combine them horizontally, the color components must be concatenated vertically and vice versa.

Compared to Color-PE methods and their extensions, Grayscale-PE methods provide better security as their use of smaller block size increases the number of blocks and pseudo grayscale representation efficiently disrupts the color information. However, for block-based PE schemes, there is an efficiency tradeoff between compression and encryption because of the block size choice. For example, a block size of no smaller than 16 × 16 and 8 × 8 should be used in Color-PE and Grayscale PE methods, respectively.

References

1. Showkatian, E.; Salehi, M.; Ghaffari, H.; Reiazi, R.; Sadighi, N. Deep Learning-Based Automatic Detection of Tuberculosis Disease in Chest X-ray Images. Pol. J. Radiol. 2022, 87, 118–124.
2. Ahmad, I.; Shin, S. Encryption-Then-Compression System for Cloud-Based Medical Image Services. In Proceedings of the 2022 International Conference on Information Networking (ICOIN), Jeju-si, Korea, 12–15 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 30–33.
3. Awad, A.I.; Fouda, M.M.; Khashaba, M.M.; Mohamed, E.R.; Hosny, K.M. Utilization of Mobile Edge Computing on the Internet of Medical Things: A Survey. ICT Express 2022, in press.
4. Jain, J.; Jain, A. Securing E-Healthcare Images Using an Efficient Image Encryption Model. Sci. Program. 2022, 2022, 1–11.
5. Ahmad, I.; Shin, S. A Novel Hybrid Image Encryption–Compression Scheme by Combining Chaos Theory and Number Theory. Signal Process. Image Commun. 2021, 98, 116418.
6. Siriwardhana, Y.; Gür, G.; Ylianttila, M.; Liyanage, M. The Role of 5G for Digital Healthcare against COVID-19 Pandemic: Opportunities and Challenges. ICT Express 2021, 7, 244–252.
7. Macedo, E.L.C.; de Oliveira, E.A.R.; Silva, F.H.; Mello, R.R.; Franca, F.M.G.; Delicato, F.C.; de Rezende, J.F.; de Moraes, L.F.M. On the Security Aspects of Internet of Things: A Systematic Literature Review. J. Commun. Netw. 2019, 21, 444–457.
8. Ou, Y.; Sur, C.; Rhee, K.H. Region-Based Selective Encryption for Medical Imaging. In Frontiers in Algorithmics; Preparata, F.P., Fang, Q., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4613, pp. 62–73. ISBN 978-3-540-73813-8.
9. Puech, W.; Rodrigues, J.M. Crypto-Compression of Medical Images by Selective Encryption of DCT. In Proceedings of the 13th Eurpoean Signal Processing Conference, Antalya, Turkey, 4–8 September 2005; pp. 1–4.
10. Ahmad, I.; Shin, S. Region-Based Selective Compression and Selective Encryption of Medical Images. In Proceedings of the 9th International Conference on Smart Media and Applications, Jeju-si, Korea, 17 September 2020; pp. 34–38.

11. Kawamura, A.; Kinoshita, Y.; Nakachi, T.; Shiota, S.; Kiya, H. A Privacy-Preserving Machine Learning Scheme Using EtC Images. IEICE Trans. Fundam. 2020, 103, 1571–1578.
12. Ahmad, I.; Kim, E.; Hwang, S.-S.; Shin, S. Privacy-Preserving Surveillance for Smart Cities. In Proceedings of the 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), Barcelona, Spain, 5 July 2022; pp. 301–306.
13. Chuman, T.; Sirichotedumrong, W.; Kiya, H. Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images. IEEE Trans. Inf. Forensics Secur. 2019, 14, 1515–1525.
14. Sirichotedumrong, W.; Kiya, H. Grayscale-Based Block Scrambling Image Encryption Using YCbCr Color Space for Encryption-Then-Compression Systems. APSIPA Trans. Signal Inf. Process. 2019, 8, e7.
15. Iida, K.; Kiya, H. Privacy-Preserving Content-Based Image Retrieval Using Compressible Encrypted Images. IEEE Access 2020, 8, 200038–200050.
16. Chuman, T.; Kurihara, K.; Kiya, H. On the Security of Block Scrambling-Based EtC Systems against Extended Jigsaw Puzzle Solver Attacks. IEICE Trans. Inf. Syst. 2018, 101, 37–44.
17. Kurihara, K.; Shiota, S.; Kiya, H. An Encryption-Then-Compression System for JPEG Standard. In Proceedings of the 2015 Picture Coding Symposium (PCS), Cairns, QLD, Australia, 31 May–3 June 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 119–123.
18. Ahmad, I.; Shin, S. Block-Based Perceptual Encryption Algorithm with Improved Color Components Scrambling. In Proceedings of the Korean Institute of Next Generation Computing, Jeju-si, Korea, 19 May 2022; pp. 155–158.
19. Grivkov, A.V.; Smirnov, A.A. Application of Convolutional Neural Networks for Diagnostics of Tuberculosis; AIP Publishing LLC: Ekaterinburg, Russia, 2020; p. 080011.
20. Szegedy, C.; Vanhoucke, V.; Ioffe, S.; Shlens, J.; Wojna, Z. Rethinking the Inception Architecture for Computer Vision. arXiv 2015, arXiv:1512.00567.
21. Jaeger, S.; Candemir, S.; Antani, S.; Wáng, Y.-X.J.; Lu, P.-X.; Thoma, G. Two Public Chest X-Ray Datasets for Computer-Aided Screening of Pulmonary Diseases. Quant. Imaging Med. Surg. 2014, 4, 475–477.
22. Das, D.; Santosh, K.C.; Pal, U. Inception-Based Deep Learning Architecture for Tuberculosis Screening Using Chest X-Rays. In Proceedings of the 2020 25th International Conference on Pattern Recognition (ICPR), Milan, Italy, 10–15 January 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 3612–3619.
23. Anu Priya, P.; Vimina, E.R. Tuberculosis Detection from CXR: An Approach Using Transfer Learning with Various CNN Architectures. In International Conference on Communication,

Computing and Electronics Systems; Bindhu, V., Tavares, J.M.R.S., Boulogeorgos, A.-A.A., Vuppalapati, C., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2021; Volume 733, pp. 407–418. ISBN 978-981-334-908-7.

24. Simonyan, K.; Zisserman, A. Very Deep Convolutional Networks for Large-Scale Image Recognition. arXiv 2015, arXiv:1409.1556.
25. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. arXiv 2015, arXiv:1512.03385.
26. Huang, G.; Liu, Z.; van der Maaten, L.; Weinberger, K.Q. Densely Connected Convolutional Networks. arXiv 2018, arXiv:1608.06993.
27. Cao, K.; Zhang, J.; Huang, M.; Deng, T. X-Ray Classification of Tuberculosis Based on Convolutional Networks. In Proceedings of the 2021 IEEE International Conference on Artificial Intelligence and Industrial Design (AIID), Guangzhou, China, 28–30 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 125–129.
28. Rahman, M.; Cao, Y.; Sun, X.; Li, B.; Hao, Y. Deep Pre-Trained Networks as a Feature Extractor with XGBoost to Detect Tuberculosis from Chest X-ray. Comput. Electr. Eng. 2021, 93, 107252.
29. Chen, T.; Guestrin, C. XGBoost: A Scalable Tree Boosting System. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, 13–17 August 2016; pp. 785–794.
30. Munadi, K.; Muchtar, K.; Maulina, N.; Pradhan, B. Image Enhancement for Tuberculosis Detection Using Deep Learning. IEEE Access 2020, 8, 217897–217907.
31. Tan, M.; Le, Q.V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. arXiv 2020, arXiv:1905.11946.
32. Msonda, P.; Uymaz, S.A.; Karaağaç, S.S. Spatial Pyramid Pooling in Deep Convolutional Networks for Automatic Tuberculosis Diagnosis. Trait. Du Signal 2020, 37, 1075–1084.
33. Szegedy, C.; Wei, L.; Yangqing, J.; Sermanet, P.; Reed, S.; Anguelov, D.; Erhan, D.; Vanhoucke, V.; Rabinovich, A. Going Deeper with Convolutions. In Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 7–12 June 2015; pp. 1–9.
34. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. ImageNet Classification with Deep Convolutional Neural Networks. Commun. ACM 2017, 60, 84–90.
35. He, K.; Zhang, X.; Ren, S.; Sun, J. Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition. IEEE Trans. Pattern Anal. Mach. Intell. 2014, 8691, 346–361.
36. Rajaraman, S.; Antani, S.K. Modality-Specific Deep Learning Model Ensembles Toward Improving TB Detection in Chest Radiographs. IEEE Access 2020, 8, 27318–27326.

37. Szegedy, C.; Ioffe, S.; Vanhoucke, V.; Alemi, A. Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. arXiv 2016, arXiv:1602.07261.
38. Chollet, F. Xception: Deep Learning with Depthwise Separable Convolutions. arXiv 2017, arXiv:1610.02357.
39. Dasanayaka, C.; Dissanayake, M.B. Deep Learning Methods for Screening Pulmonary Tuberculosis Using Chest X-Rays. Comput. Methods Biomech. Biomed. Eng. Imaging Vis. 2021, 9, 39–49.
40. Oloko-Oba, M.; Viriri, S. Ensemble of Convolution Neural Networks for Automatic Tuberculosis Classification. In Computational Collective Intelligence; Nguyen, N.T., Iliadis, L., Maglogiannis, I., Trawiński, B., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2021; Volume 12876, pp. 549–559. ISBN 978-3-030-88080-4.
41. Oloko-Oba, M.; Viriri, S. Ensemble of EfficientNets for the Diagnosis of Tuberculosis. Comput. Intell. Neurosci. 2021, 2021, 1–12.
42. Saif, A.F.M.; Imtiaz, T.; Shahnaz, C.; Zhu, W.-P.; Ahmad, M.O. Exploiting Cascaded Ensemble of Features for the Detection of Tuberculosis Using Chest Radiographs. IEEE Access 2021, 9, 112388–112399.
43. Imaizumi, S.; Kiya, H. A Block-Permutation-Based Encryption Scheme with Independent Processing of RGB Components. IEICE Trans. Inf. Syst. 2018, 101, 3150–3157.