## CONCLUSION

In this paper, a novel privacy-preserving CBIR scheme is proposed. A novel bag-of-encrypted-words (BOEW) model is designed to achieve a good retrieval accuracy. As a case study, we protect the image content by color value substitu tion , block permutation, and intra-block pixel permutation. Local histograms are calculated as local features. *k*-means algorithm is utilized to generate encrypted visual words. The histogram of the visual words is calculated to represent the image. The similarity between images can be directly measured by the Manhattan distance between feature vectors on the cloud server side. Besides the search operation, the index construction in our scheme can be also outsourced to the cloud server. The proposed scheme can be further improved. Firstly, it could be a meaningful future work to design better local descriptors under our BOEW model. Secondly, how to protect the image content under CPA model needs further studies. Finally, it could be interesting to apply the BOEW model to JPEG images.