**INTRODUCTION**

THE world has witnessed a rapid development of imaging devices, such as digital cameras, medical imaging equipments, smart phones, and so on. Accordingly, the number of digital images increases dramatically. In order to retrieve similar images quickly from large amount of images, many practical Content-based Image Retrieval (CBIR) techniques have been developed. However, typical image database is simply too large, including millions of images and each may be larger than 40 megabytes [1]. Thus, CBIR service generally requires heavy storage and computation. Such demands make it attractive to outsource CBIR services to the cloud server. In this way, the image owner needs not to store the image database locally, and can efficiently retrieve the desired images from the cloud server [2].

Apart from the enormous benefits of CBIR outsourcing, the privacy of images becomes the biggest concern to the image owner. Both the image database and the query image should be protected properly.

**Contribution.** In this paper, we propose an outsourced CBIR scheme where the image content is properly protected.

The main contributions are summarized as follows:

1) A BOEW model is proposed for CBIR outsourcing. We propose to encrypt images by blocks and make sure that the secure and useful local features can be directly extracted from the encrypted blocks. *k*-means clustering algorithm is deployed to generate the encrypted visual words. The final feature vectors, also the encrypted ones, are then constructed with the visual words. The similarity between the feature vectors can be directly measured by Euclidean or Manhattan distance. The proposed BOEW could be a valuable model in encrypted image processing.

2) As a case study, we propose to encrypt image by color value substitution, block permutation, and intra-block pixel permutation. With the specially-designed encryption method, secure local histograms can be directly extracted from the encrypted images on cloud server side. The index construction can also be finished by cloud server. Compared with the scheme using secure global histogram [3], [4], our method achieves a much better retrieval accuracy. The rest of this paper is organized as follows. Section 2 introduces the related works. Section 3 presents the technical overview. Section 4 addresses the proposed scheme design. Section 5 gives the security analysis. Experiments and results are presented in Section 6. Finally, conclusion is made in Section 7.