**CHAPTER-2**

**INTRODUCTION**

With the rapid development and popularization of cloud computing, people enjoy various conveniences brought by cloud services, such as storing images on the cloud. However, directly outsourcing images to the public cloud inevitably raises privacy concerns. Once the massive images (e.g., patients’ medical images) containing highly sensitive information have been leaked to unauthorized entities, it will incur serious consequences or unnecessary trouble. In this encrypted image search process, the cloud server is regarded as semi-trusted. Alice stores her images on this cloud server, and entrusts the cloud server to perform similarity search tasks. When Bob comes to query Alice’s images, the cloud server will honestly provide Bob with search service under Alice’s arrangement. The performance of search services, such as search accuracy and efficiency, will profoundly affect Bob’s search experience. Assuming that Bob is a doctor who relies on search results to diagnose a certain patient’s condition, the incorrect search results will lead to a wrong diagnose, which endangers the patient’s health and even life. Besides, the time-consuming search process will prolong the waiting time of the Bob. If Bob is a mobile image user who requires high real-time responses, such a long search time is hard to bear and easily makes search time lose timeliness. Moreover, the above search mechanism still requires Alice to share sk and kie with Bob, which cannot completely protect image privacy. This is because we cannot promise that Bob is fully trusted and does not share sk and kie with other unauthorized image users due to interest incentives in practice

**2.1 LITERATURE SURVEY**

# 1. Title: Reversible cellular automata image encryption for similarity search

**Author**: [YingriSu](https://www.sciencedirect.com/science/article/abs/pii/S0923596518306714" \l "!), [YanWo](https://www.sciencedirect.com/science/article/abs/pii/S0923596518306714#!), [GuoqiangHan](https://www.sciencedirect.com/science/article/abs/pii/S0923596518306714#!)

**ABSTRACT**: The pixels in an image are encrypted in pixel-granularity or pixel-set-granularity to solve utility-security dilemma. And block-based permutation method is used to improve the image security and retrieval accuracy. Experiments on Corel-1000 demonstrate that the proposed method not only offers high image security, but also yields superior retrieval accuracy on encrypted images compared with other image encryption algorithms for similarity search.

# 2.Title: An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing

**Author**: [Jiaohua Qin](https://ieeexplore.ieee.org/author/37669462500); [Hao Li](https://ieeexplore.ieee.org/author/37086524909); [Xuyu Xiang](https://ieeexplore.ieee.org/author/37823140400); [Yun Tan](https://ieeexplore.ieee.org/author/37086699298); [Wenyan Pan](https://ieeexplore.ieee.org/author/37086702252); [Wentao Ma](https://ieeexplore.ieee.org/author/37086526984); [Neal N. Xiong](https://ieeexplore.ieee.org/author/37271732200)

**ABSTRACT**: The encrypted image retrieval in cloud computing is a key technology to realize the massive images of storage and management and images safety. In this paper, a novel feature extraction method for encrypted image retrieval is proposed. First, the improved Harris algorithm is used to extract the image features. Next, the Speeded-Up Robust Features algorithm and the Bag of Words model are applied to generate the feature vectors of each image. Then, Local Sensitive Hash algorithm is applied to construct the searchable index for the feature vectors. The chaotic encryption scheme is utilized to protect images and indexes security. Finally, secure similarity search is executed on the cloud server. The experimental results show that compared with the existing encryption retrieval schemes, the proposed retrieval scheme not only reduces the time consumption but also improves the image retrieval accuracy.

# 3.Title: Efficient Similarity Search over Encrypted Data

# Author: [Mehmet Kuzu](https://ieeexplore.ieee.org/author/38252795500); [Mohammad Saiful Islam](https://ieeexplore.ieee.org/author/37086598411); [Murat Kantarcioglu](https://ieeexplore.ieee.org/author/37279375600)

**ABSTRACT:** In recent years, due to the appealing features of cloud computing, large amount of data has been stored in the cloud. Although cloud-based services offer many advantages, privacy and security of the sensitive data is a big concern. To mitigate the concerns, it is desirable to outsource sensitive data in encrypted form. Encrypted storage protects the data against illegal access, but it complicates some basic, yet important functionality such as the search on the data. To achieve search over encrypted data without compromising the privacy, considerable amount of searchable encryption schemes have been proposed in the literature. However, almost all of them handle exact query matching but not similarity matching, a crucial requirement for real world applications. Although some sophisticated secure multi-party computation based cryptographic techniques are available for similarity tests, they are computationally intensive and do not scale for large data sources. In this paper, we propose an efficient scheme for similarity search over encrypted data. To do so, we utilize a state-of-the-art algorithm for fast near neighbor search in high dimensional spaces called locality sensitive hashing. To ensure the confidentiality of the sensitive data, we provide a rigorous security definition and prove the security of the proposed scheme under the provided definition. In addition, we provide a real world application of the proposed scheme and verify the theoretical results with empirical observations on a real dataset.

# 4.Title: Secure semantic expansion-based search over encrypted cloud data supporting similarity ranking

Author: [Zhihua Xia](https://link.springer.com/article/10.1186/s13677-014-0008-2#auth-Zhihua-Xia),  [Yanling Zhu](https://link.springer.com/article/10.1186/s13677-014-0008-2#auth-Yanling-Zhu), [Xingming Sun](https://link.springer.com/article/10.1186/s13677-014-0008-2#auth-Xingming-Sun) &  [Lihong Chen](https://link.springer.com/article/10.1186/s13677-014-0008-2#auth-Lihong-Chen)

# ABSTRACT: With the advent of cloud computing, more and more information data are outsourced to the public cloud for economic savings and ease of access. However, the privacy information has to be encrypted to guarantee the security. To implement efficient data utilization, search over encrypted cloud data has been a great challenge. The existing solutions depended entirely on the submitted query keyword and didn’t consider the semantics of keyword. Thus the search schemes are not intelligent and also omit some semantically related documents. In view of the deficiency, as an attempt, we propose a semantic expansion based similar search solution over encrypted cloud data. Our solution could return not only the exactly matched files, but also the files including the terms semantically related to the query keyword. In the proposed scheme, a corresponding file metadata is constructed for each file. Then both the encrypted metadata set and file collection are uploaded to the cloud server. With the metadata set, the cloud server builds the inverted index and constructs semantic relationship library (SRL) for the keywords set. After receiving a query request, the cloud server first finds out the keywords that are semantically related to the query keyword according to SRL. Then both the query keyword and the extensional words are used to retrieve the files. The result files are returned in order according to the total relevance score. Eventually, detailed security analysis shows that our solution is privacy-preserving and secure under the previous searchable symmetric encryption (SSE) security definition. Experimental evaluation demonstrates the efficiency and effectives of the scheme.

# 5.Title:  An efficient and privacy-preserving content-based image retrieval scheme in cloud computing

**Author**: [ZhihuaXia](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[a](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[Neal N.Xiong](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[b](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[Athanasios V.Vasilakos](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[c](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[XingmingSun](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)[a](https://www.sciencedirect.com/science/article/abs/pii/S0020025516321971" \l "!)

**ABSTRACT:** The content-based image retrieval (CBIR) has been widely studied along with the increasing importance of images in our daily life. Compared with the text documents, images consume much more storage and thus are very suitable to be stored on the cloud servers. The outsourcing of CBIR to the cloud servers can be a very typical service in cloud computing. For the privacy-preserving purposes, sensitive images, such as medical and personal images, need to be encrypted before being outsourced, which will cause the CBIR technologies in plaintext domain unusable. In this paper, we propose a scheme that supports CBIR over the encrypted images without revealing the [sensitive information](https://www.sciencedirect.com/topics/computer-science/sensitive-informations) to the cloud server. Firstly, the feature vectors are extracted to represent the corresponding images. Then, the pre-filter tables are constructed with the locality-sensitive hashing to increase the search efficiency. Next, the feature vectors are protected by the secure k-nearest neighbor (kNN) algorithm. The security analysis and experiments show the security and efficiency of the proposed scheme.