Privacy Preserving Search on Multimedia
Part I

Prof. Ja-Ling Wu
(Cited from Prof. Min Wu’s work)
I. INTRODUCTION

The advancement of information technology has been rapidly integrating the physical world where we live and the online world that we rely on for retrieving, sharing, and managing information. Online services and web applications emerge everyday and benefit our life in almost every aspect: from information retrieval using search engines to sharing user generated content (UGC) through social networks, from personal information management, such as webmail and online photo albums, to online backup services.
With the arrival of the **cloud computing** paradigm, the Internet stores not only information for sharing, but also **sensitive personal data** that should be carefully protected against any unauthorized access. Secure management of personal data stored online is an increasingly important issue that can help achieve the **data confidentiality** and availability requirements of cloud computing. Technologies that can enable secure online data management are going to play a critical role in the future of the internet.
Traditional privacy protection for online personal data focuses on access control and secure data transmission, which ensure that the data can be securely transmitted to the server and no unauthorized people can access the data. However, once the data arrives at the server, the server decrypts the data and operates on plaintext in order to provide services to users, such as categorization, search, and data analysis. This makes the user’s private information vulnerable to untrustworthy service providers and malicious intruders.
For example, most personal emails are stored online as plaintext data and can be viewed by the system administrator. Given the trend that an increasing amount of personal data will be stored at a third-party server, it is both desirable and necessary to develop technologies that can better protect users’ privacy without sacrificing the usability and accessibility of the information. Information retrieval over encrypted databases is a promising technological capability for privacy protection in online information management.
Encryption of the data stored on the server helps protect content privacy against untrustworthy service providers and malicious intruders, but using traditional cryptographic ciphers alone makes it difficult for the server to process the data, and for the user to retrieve information from the encrypted database. The goal of information retrieval over an encrypted database is to provide efficient and accurate search capability over encrypted documents without decrypting them first.
• An example application is that the user stores his/her private data in encrypted form on remote servers and later wants to search and retrieve data similar to a query in a privacy preserving manner, so that the server cannot learn the content of the query and the retrieved images. Due to the widespread use of digital cameras and portable camcorders, multimedia data constitute a significant part of today’s personal data collections. Storing and managing this large volume of multimedia data online is becoming a desirable option for convenient data access anywhere anytime.
Given such a trend of more semantic and multimedia-rich Internet, technologies that can enable content-based retrieval over encrypted multimedia databases will play an important role in helping people manage their multimedia data both effectively and securely. This is the main focus of this talk.
Prior work in the area of information retrieval in the encrypted domain focused on text documents. Song et al. [3], Brinkman et al. [4], and Boneh et al. [5] explored Boolean search to identify whether a query term is present in an encrypted text document. Recent work by Swaminathan et al. [6] proposed a framework for rank-ordered search over encrypted text documents, so that documents can be returned in the order of their relevance to the query term.
Secure text retrieval techniques can also be applied to **keyword based search of multimedia data**. However, keyword search relies on having **accurate text description of the content** already available, and its search scope is confined to the existing keyword set. In contrast, **content-based search** over an encrypted multimedia database provides more **flexibility**, whereby sample images, audios or videos are presented as queries and documents with similar audio-visual content in the database are identified.
An emerging area of work related to secure multimedia retrieval is secure signal processing, which aims at performing signal processing tasks while keeping the signals being processed secret. Erkin et al. [7] provided a review of related cryptographic primitives and some applications of secure signal processing in data analysis and content protection. However, applying cryptographic primitives to content-based multimedia retrieval is not straightforward.
Effective multimedia retrieval typically relies on evaluating the similarity of two documents using the distance between their visual features, such as color histograms, shape descriptors, or salient points [8]. Traditional cryptographic primitives typically do not preserve the distance between feature vectors after encryption. In addition, efficiency and scalability are critical for multimedia retrieval but can be difficult to achieve using cryptographic primitives alone. Another work by Shashank et al. [9] addresses the problem of protecting the privacy of the query image when searching over a public database, where the images in the database are not encrypted.
Recent work in the general area of secure computation for privacy protection addressed different but related problems under various application settings [10]–[14]. Yiu et al. [10] considered privacy preserving range query over geospatial coordinates using a kd-tree. Extending such a technique to multimedia retrieval is difficult because features used for content-based multimedia retrieval are high dimensional vectors and kd-tree is known to be inefficient in high dimensional spaces.
Wong et al. [11] proposed secure k-NN computation that exactly preserves the original dot-product between two vectors. This algorithm identifies the larger of the two distances but keeps the actual distance values secret from the server. Erkin et al. [12] and Sadeghi et al. [13] addressed the problem of privacy preserving face recognition, where one party wants to verify the existence of a given face image in a database hosted on another party’s servers. The two parties want to keep their own data secret from each other. Additive homomorphic encryption schemes are used to allow similarity computation in the encrypted domain.
Similar techniques are also used by Jiang et al. [14] to identify the existence of similar text documents between two parties. As there have been no efficient homomorphic encryption schemes yet that allow both addition and multiplication, multiple rounds of communication between the two parties are required to compute the Euclidean distance between the query and each database entry.

→**Fully Homomorphic Encryption**
The main difference between the scenarios considered in the above mentioned related works [12]–[14] and in this talk is that in the current application, the user stores encrypted multimedia data on a remote server, and the server does not own the data and merely performs computation on the encrypted data on behalf of the user to allow efficient content-based retrieval over a potentially large database. The current high level of computational complexity and communication overhead of schemes being built on homomorphic encryption make them less feasible for the application considered in this talk. Efficient encryption schemes that can enable fast retrieval with little communication overhead are required for private database management over the cloud.
This talk focuses on content-based multimedia retrieval over encrypted databases, where both the query and database documents are encrypted and their privacy is protected, in contrast to the work of Shashank et al. [9] where the database images are publicly known (this approach may be of interest for privacy preserving search over open data). The techniques addressed in this talk enable efficient retrieval directly in the encrypted domain, without multiple rounds of communications between the user and the server, as compared to [12], [13].
We demonstrate the proposed techniques using image databases in this talk, although these techniques are applicable to other multimedia modalities such as video. By analyzing the requirements of secure retrieval scenarios, we propose retrieval techniques from two different viewpoints. The first group of techniques focuses on visual feature protection that allows similarity comparison among encrypted features, while the second group of techniques aim at encrypting the search indexes directly, where the search indexes are typically generated from visual features and carefully designed to enable efficient search over large multimedia databases.
The two groups of techniques are complementary and represent different trade-offs between user-side computational complexity and communication overhead. We jointly exploit cryptography, image processing, and information retrieval techniques to ensure that the encrypted features and indexes preserve search accuracy.
II. PROBLEM FORMULATION

In order to protect data privacy, images need to be encrypted before being transferred to the remote server. Image encryption can be done using state-of-the-art ciphers such as AES or RSA by treating images as ordinary data, or using image specific encryption techniques such as selective and format-compliant encryption [15], [16], [17] to enable post-processing such as transcoding of encrypted images. As these techniques are built upon established cryptographic encryption tools, it is computationally difficult for an adversary to decrypt the encrypted image files.
In modern image retrieval techniques, content similarity is typically evaluated using search indexes or visual features, such as color histograms and salient points, instead of comparing images pixel by pixel. Therefore, encryption of images alone is not sufficient for privacy protection because search indexes or image features in plaintext may reveal information about image content. For example, a color histogram with large values for the blue components would indicate the presence of sky or ocean, and SIFT descriptors [18] may reveal information about distinctive objects in the image.
In order to be able to search through the encrypted database without leaking information from the plaintext search indexes or image features, we devise schemes to generate and appropriately encrypt image features and search indexes on the user side using a secret key and then transfer them to the server, where the encrypted features or indexes are used to evaluate image similarity.
A system model for the secure search scenario is shown in Figure 1, where the left part depicts the database construction stage and the right part depicts the retrieval stage. In the overall system of secure image retrieval, images are encrypted using standard ciphers, and visual features or search indexes extracted from the images are protected by the encryption schemes introduced in this talk.
During retrieval, the search index from the query image is suitably encrypted to allow similarity comparison in the encrypted domain. The block “Build search index” corresponds to encrypting the features in the feature protection schemes or building secure indexes in the secure indexing schemes, which will be described later.
The first approach for **secure image retrieval** is to encrypt the feature vectors of each image and store those encrypted features on the server, as described in Section III-A. The server can use these encrypted features as naïve indexes if the database is small, or the server can build efficient indexes upon the encrypted features for improved search efficiency. Since the similarity of two images is typically measured by computing the distance between features extracted from them [8], the encryption of image features should approximately preserve their distances.
Suppose we represent image features as vectors in $\mathbb{R}^n$, we seek an encryption function $\mathcal{E}(\cdot) : \mathbb{R}^n \rightarrow \mathbb{R}^m$, such that given two feature vectors $f$ and $g$, $d_{\mathcal{E}}(\mathcal{E}(f), \mathcal{E}(g)) \approx c \cdot d(f, g)$, where $d_{\mathcal{E}}(\cdot, \cdot)$ and $d(\cdot, \cdot)$ are some appropriate distance measures on ciphertext and plaintext, respectively, and $c$ is a constant scaling factor. The approximate distance preserving encryption scrambles the visual features for content protection and allows servers to perform similarity comparison in the encrypted domain.
Fig. 1: System model for secure image retrieval
Since **efficiency** and **scalability** are critical aspects for retrieval from a large database and rely on the design of search indexes, the second approach for secure image retrieval **explores the possibility of encrypting the state-of-the-art multimedia search indexes without affecting their search capability.**
The content owner has the flexibility either to provide the server with encrypted features and let the server perform the time-consuming index generation, or to generate the secure index on his/her side to reduce the amount of information that needs to be sent to the server. Therefore, the two kinds of approaches represent different trade-offs between user-side computational complexity and communication overhead.