

**CHENNAI – PONDICHERRY**

**Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories**

**Abstract**

Storage requirements for visual data have been increasing in recent years, following the emergence of many highly interactive multimedia services and applications for mobile devices in both personal and corporate scenarios. This has been a key driving factor for the adoption of cloud-based data outsourcing solutions. However, outsourcing data storage to the Cloud also leads to new security challenges that must be carefully addressed, especially regarding privacy. In this paper we propose a secure framework for outsourced privacy-preserving storage and retrieval in large shared image repositories. Our proposal is based on IES-CBIR, a novel Image Encryption Scheme that exhibits Content-Based Image Retrieval properties. The framework enables both encrypted storage and searching using Content-Based Image Retrieval queries while preserving privacy against honest-but-curious cloud administrators. We have built a prototype of the proposed framework, formally analyzed and proven its security properties, and experimentally evaluated its performance and retrieval precision. Our results show that IES-CBIR is provably secure, allows more efficient operations than existing proposals, both in terms of time and space complexity, and paves the way for new practical application scenarios.