

**CHENNAI – PONDICHERRY**

**Privacy-preserving Image Processing in the Cloud**

**Abstract:**

Millions of private images are generated in various digital devices every day. The consequent massive computational workload makes people turn to cloud computing platforms for their economical computation resources. Meanwhile, the privacy concerns over the sensitive information contained in outsourced image data arise in public. In fact, once uploaded to cloud, the security and privacy of the image content can only presume upon the reliability of the cloud service providers. Lack of assuring security and privacy guarantees becomes the main barrier to further deployment of cloud-based image processing systems. This paper studies the design targets and technical challenges lie in constructing cloud-based privacy-preserving image processing system. We explore various image processing tasks, including image feature detection, digital watermarking, content-based image search. The state-of-the-art techniques, including secure multiparty computation, and homomorphic encryption are investigated. A detailed taxonomy of the problem statement and the corresponding solutions is provided.

**Exisitng System:**

The participation of a third-party cloud computing platform also increases the vulnerability of private data, e.g., potential data breach and lost. Under current cloud architecture, the content of outsourced image data will inevitably be leaked to CSPs. In this case, the leaked content might be sensitive information like data owner’s personal identity, home address, or even financial records. Moreover, even we assume CSPs are completely honest and could be trusted to have data owners’ private information, such privacy leakage still happens. In fact, cloud server is usually considered as a low-qualified locker rather than a strong bank deposit box. Comparing with traditional network server, the cloud computing platform suffers from more security threats. For instance, a severe vulnerability in cloud server is the sharing of computing resources: flaws in System Virtual Machine (SVM) software are frequently discovered and exploited to attack cloud servers in recent years.

**Proposed System:**

**The proposed system consists of two main phases as follows:**

*Data Preprocessing*: In Data Preprocessing phase, for image *I*, a user prepares ciphertext *C* through encoding process *Encode*(*I*) and sends *C* to the CCP, where computation tasks over the encrypted image *C*. Such encoding algorithm should be lightweight and support as many image processing algorithms as possible. Hence, user only needs to encode its image data once, and the majority of computation workload is taken by CCP.

*Encrypted Image Evaluation*: After receiving the encrypted image data, CCP performs image processing algorithms over the ciphertext domain to get the corresponding encrypted results. Meanwhile, the private information of uploaded image data should be protected against CCP. (After that, the user can decrypt and get image processing results in plaintext.)