Chapter 21
Visual Cryptography for Securing Images in Cloud

Punithavathi P.
VIT University, Chennai Campus, India

Geetha Subbiah
VIT University, Chennai Campus, India

ABSTRACT

Images are becoming an inevitable part of knowledge in the modern day society. As data is growing at a rapid rate, costs involved in storing and maintaining data is also raising rapidly. The best alternate solution to reduce the storage cost is outsourcing all the data to the cloud. To ensure confidentiality and integrity of the data, a security technique has to be provided to the data even before it is stored on the cloud using cryptography. An attempt is made to explore the possibility of usage of visual cryptography for providing robust security to the secret image. Visual cryptography proves to be more efficient than other cryptography techniques because it is simple and does not require any key management technique.

INTRODUCTION

Images are becoming an inevitable part of knowledge in the modern day society. As the world changes, the technology is also changing rapidly. Various confidential data such as medical images, biometric images, space and geographical images taken from satellite and commercial important document are transmitted over the Internet and stored in remote locations for future access. The day-to-day needs for computing resources are increasing. As data is growing at a rapid rate, costs involved in storing and maintaining data is also raising rapidly. The best alternate solution to reduce the storage cost is outsourcing all the data to the cloud.

Cloud computing is an emerging technology which provides facilities for storage, computations, database-driven services for various industrial, financial, healthcare, educational and governmental sectors. Cloud model utilizes the computing resources with the capabilities of increasing the resources, providing pay-per-user privilege with a little or no up-front investment costs on the IT infrastructure. This promising model moves the databases to the large data centers. However, the management of the

DOI: 10.4018/978-1-5225-5634-3.ch021

data may not be reliable and the enterprises may not have any control over the data, since the data centers are remote. The common security concerns are:

- Securing data both during transmission and during storage,
- Securing software interfaces,
- User access control, and
- Data separation.

Since, the data in the cloud computing is placed in the hands of trusted third parties, ensuring the data security both during storage and during transmission is of great importance. The data integrity and confidentiality is maintained in the cloud by providing security to the data. This is an important quality of service in cloud computing.

Security of data in cloud is a challenge and is significant as many concerns and faults are yet to be categorized. As data is stored in the cloud, the user is unaware of where it is being stored and who are privileged to access the data. Eventually, the data owners are bothered about the confidentiality and integrity of the data. To ensure this, a security technique has to be provided to the data even before it is stored on the cloud. Such technique should be simple and user-friendly and at the same time should be less complex.

Data encryption techniques can be utilized on a great scale for successfully providing security to the data both during transmission and storage. Cryptography encodes a plain text to a cipher text and decodes the cipher text back to the plain text. There are two types of cryptography algorithms namely symmetric and asymmetric algorithm. The symmetric algorithm uses a single secret key while the asymmetric uses two different keys for encryption and decryption. But both these cases require heavy computation and as well as key management techniques. Moreover, user is required to have some knowledge of cryptography. Hence there is a serious requirement of a simple and less-complex cryptography technique which will be more feasible if there is no encryption/decryption key.

Visual cryptography (VC) is a paradigm in which a secret image is converted into two or more meaningless, non-identical shares, without using any encryption keys. The hidden secret can be revealed only when the shares are stacked together. The magnificence of VC lies in the facts that the hidden secret can never be recovered just by possessing one of the shares, and also that the secret can be revealed without any computer intervention. This allows VC to be used by anyone without any deep understanding of cryptography, and without any hard computations.

VC is different from the usual cryptographic secret sharing. In cryptographic secret sharing technique, each participant is allowed to keep a portion of the secret which could be revealed easily. But this discomfort is overcome by the VC as it uses the idea of hiding secrets into multiple shares which never reveal the secret until stacked together. The secret recovery is as simple as superimposing transparencies containing the shares, which allows the secret to be reconstructed. VC is a desirable scheme as it embodies both the scheme of perfect secrecy and a very simple mechanism for recovering the secret. While considering popular cryptographic schemes which are conditionally secure, VC provides robust security to the secret image. This makes VC suitable for highly sensitive applications like biometric authentication (Ross & Othman, 2010), secure electronic ballots (Chaum, 2004), safe online banking (Roy & Venkateswaran, 2014), digital watermarking (Tai & Chang, 2004), security against DoS attacks in WiMax authentication system (Altaf, Sirhindi, & Ahmed, 2008), etc.