
Ying Zhou, Tingting Guo and Linping Zhou

ABSTRACT

Remotely sensed data sharing services are attracting more and more attention. Advanced cloud computing technologies provide huge storage and efficient support for remotely sensed big data services. Therefore, the security of stored remotely sensed data and usage security in the cloud computing environment have become urgent issues. To address these problems we propose a secure method for remote sensing images (RSIs) in the cloud computing environment. The proposed method not only ensures RSI security without relying on the trustworthiness of cloud servers, but also protects RSI copyrights and extends RSI exploration. Theoretical analysis justifies the security of the proposed scheme. The computation cost of the proposed scheme is acceptable and adjusts to different security levels.

1. INTRODUCTION

With the development of remote sensed acquisition and processing technologies, the use of remotely sensed data (RSD) is becoming more and more widespread. These data collected by platforms such as satellites and airplanes, are used in a wide variety of applications; for example, in agriculture, environmental planning, monitoring, surveillance, weather foresting, and traffic control. At the same time, many diffusion and distribution tools are opening the way towards new services and applications for remotely sensed data. As we have entered the era of "big data", the capability of earth observations has dramatically increased and reached an unprecedented level thanks to widely accessible remotely sensed data [1, 2].
Remotely sensed data storage security is a critical issue when DOs outsource their data to a third party such as cloud computing servers. In this situation, the cloud servers possess the outsourced data; it is possible that a cloud service provider (CSP) can duplicate DO data while claiming that the data are still stored confidentially in the cloud. Thus, DOs need to be convinced that their data is secure and has not been exposed or stolen from the cloud. A feasible solution is data encryption using certain cryptographic primitives, with disclosure of the decryption keys only to authorized users. However, conventional two-party encryption is not suited for three-party data security in cloud computing. Re-encryption as a cryptographic algorithm involving three parties thus becomes a promising approach to maintain data confidentiality in cloud data services [3].

However, although re-encryption can prevent information leakage in the cloud computing, the content owner does not prevent an authorized user’s illegal replication or delivery of the content after the encrypted RSD is legally decrypted [4-5]. Such illegal dealings can seriously harm a content owner’s copyright. Therefore, copyright protection in cloud computing is also a critical issue. Traditional marking techniques can protect ownership rights of the DOs [6-8], but they would cause severe effects on complete remote sensing images (RSIs), such as edges of a RSI [8]. These effects hinder further explorations and RSI applications. Reversible Marking (RM) technique provides a solution to solve the above problem. RM technique is able to erase the distortion introduced by embedding step after cover restoration [9]. Marking information embedded into RSI can be used to protect owner’s copyright. The marked RSI can also satisfy some common applications. Furthermore, to fully satisfy the further exploration of the RSI, the marking information can be fully extracted and the RSI can be recovered.

Therefore, re-encryption technique ensures RSD security in cloud computing. RM techniques protect a RSD copyright and further extend RSD exploration. This paper proposes an encryption and reversible marking method for RSIs in cloud computing that can ensure RSI security, protect an RSI copyright and further extend RSI exploration.

**TABLE I. Syntactic definition of re-encryption.**

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>par</td>
<td>a public parameters</td>
</tr>
<tr>
<td>(sk_u, pk_u)</td>
<td>DU’s secret/public key pair</td>
</tr>
<tr>
<td>(sk_o, pk_o)</td>
<td>DO’s secret/public key pair</td>
</tr>
<tr>
<td>rekey_u</td>
<td>a re-encryption key</td>
</tr>
<tr>
<td>M</td>
<td>a plaintext</td>
</tr>
<tr>
<td>C</td>
<td>a first level ciphertext</td>
</tr>
<tr>
<td>C</td>
<td>a re-encrypted ciphertext</td>
</tr>
<tr>
<td>Rekeygen(par, sk_o, pk_u)</td>
<td>a re-encryption key generator</td>
</tr>
<tr>
<td>E_1(M, pk_o)</td>
<td>an encryption function</td>
</tr>
<tr>
<td>E_2(C, rekey_u)</td>
<td>a re-encryption function</td>
</tr>
<tr>
<td>D(C , sk_o)</td>
<td>a decryption function for re-encrypted ciphertext</td>
</tr>
</tbody>
</table>
The rest of this paper is organized as follows. The scheme of the proposed method is described in Section 2. Experimental results are provided in Section 3. We conclude this paper with a discussion of the results in Section 4.

2. PROPOSED METHOD

In the proposed model, the confidentiality of the DO data is achieved using an asymmetric cryptographic algorithm in the cloud. This is because only the DO has a decryption key for the first layer ciphertext. The CSP can only access the encrypted cloud data. The syntactic definitions of re-encryption are shown in TABLE I. The proposed method is described as following. First, a DO generates secure private-public key pairings using the asymmetric cryptographic algorithm. The DO encrypts his/her own data with the public key and obtains a ciphertext data. Then, the ciphertext data is uploaded to cloud servers. Second, a DU sends a request for the desired RSD derived in several ways such as by searching the encrypted data, to the CSP. The CSP then transmits the request to the DO. Third, after receiving the request, the DO generates a re-encryption key, rekey, with the DO’s private key and access information, then the DO sends the rekey to the CSP. Fourth, after receiving the rekey, the CSP obtains the re-encrypted ciphertext by re-encrypting the ciphertext data with the rekey. Fifth, the DU downloads the re-encrypted ciphertext from the cloud servers. The DU decrypts the re-encrypted ciphertext with DU’s private key.

2.1 Encryption Method based on EIGamal cryptosystem

As a public-key cryptography, the encryption keys $pk_o$, $pk_u$ are to be public known in re-encryption model. To add $m_1$ to another plain-text value $m_2$ in the encryption domain, the following operation can be performed on their encrypted values $E(m_1, pk_o)$ and $E(m_2, pk_o)$ by

$$E(m_1, pk_o) = y^{s_1} \cdot m_1 \mod p$$

(1)

$$E(m_2, pk_o) = y^{s_2} \cdot m_2 \mod p$$

(2)

$$Opt(m_1, m_2) = E(m_1, pk_o) + E(m_2, pk_o) = y^{s_1} \cdot (m_1 + m_2) \mod p$$

(3)

where $Opt$ is an operation between the two encrypted values.

The corresponding plain-text value $m'$ can be obtained by decrypting the cipher value $Opt(m', pk_o)$.
\[ m' = D(\text{Opt}(m_1, m_2), sk_2) = y^s \cdot (m_1 + m_2) \cdot (a^{sk_2})^{-1} \mod p = m_1 + m_2 \]  

where \( m' \) is a decrypted data.

Therefore, in the re-encryption model, the plain-text \( M \) is firstly encrypted. The ciphertext is obtained, \( E_1(M, pk_o) \).

### 2.2 Marking Operation

Given an image encrypted in ElGamal cryptosystem, a portion of the encrypted pixels are reserved to hide the side information such as the amount of bit values to be hidden and the number of encrypted pixel values used for data hiding.

To embed a bit value \( h_i \in \{0,1\} \) into \( E_i(M, pk_o) \), which is the encrypted value of a pixel value \( M_i \), an embedded value \( \text{Opt}(M_i, pk_o) \) is generated by

\[ \text{Opt}(M_i, h_i) = 2 \cdot E_i(M_i, pk_o) + E_i(h_i, pk_o) = y^s \cdot (2M_i + h_i) \mod p \]  

where \( (M_i)_{i=1,2,\ldots,j} = M \), \( l \) denotes the length of embedded bits.

### 2.3 Security Analysis

The security of proposed scheme relies critically on the security of fundamental algorithm (such as re-encryption) used in our construction process, and on the security of the proposed structure itself. In our proposed scheme, the fundamental algorithms are not restricted to specific algorithms. The fundamental algorithm used in our scheme are mature and well-studied techniques and believed to be secure, if properly used. Therefore, the security of the proposed scheme is valid. The analysis supports the proposed scheme as a promising scheme for building the RSD security.

![Figure 1](image_url)

Figure 1. (a) Original Image (b) Encrypted Image and (c) Marked decrypted Image.
3. EXPERIMENTAL RESULTS

For the sake of convenience, the simulation is based on 10 512 × 512 remote sensing images and the results are on average. Standard test image, Square with the size of 512×512, shown in Figure 1(a), is adopted to demonstrate the feasibility of the proposed method. To facilitate the implementation of the proposed scheme, the following simulation experiments are performed in MATLAB. According to above experimental results, the proposed method can support that the original RSI can be full recovered and the embedded bits can be extracted.

4. CONCLUSIONS

Remotely sensed data as a classical big data, its services and applications have been becoming more and more widely. Cloud computing technology provides with a platform for remotely sensed big data services which can support the storage of huge volume of RSD and efficient on-demand access. However, to the best of our knowledge, there has been no report about RSD’s storage and usage security in cloud computing. The re-encryption method ensures RSD security in cloud computing and marking technique protect RSD’s copyright. As for remote sensing image (RSI), current most marking operations would cause a little information loss on the marked RSI. To further extend RSI’s exploration, a reversible marking method for remote sensing imagery is introduced. According to different applications, we can provide two versions: marked RSI and extracted RSI.

REFERENCES