International Journal of Digital Crime and Forensics
Volume 10 • Issue 1 • January-March 2018

Random Grid and Reversible Watermarking-Based On Verifiable Secret Sharing for Outsourcing Images in Cloud

Hang Gao, College of Computer and Control Engineering, Nankai University, Tianjin, China
Mengting Hu, College of Computer and Control Engineering, Nankai University, Tianjin, China
Tiegang Gao, College of Software, Nankai University, Tianjin, China
Renhong Cheng, College of Computer and Control Engineering, Nankai University, Tianjin, China

ABSTRACT

A novel random grid and reversible watermarking based verifiable secret sharing scheme for outsourcing image in cloud is proposed in the paper. In the proposed scheme, data owner firstly embeds the hash value of the secret image into the secret image itself using reversible watermarking algorithm; then, watermarked image is divided into n sub image. Secondly, the hash of n sub image is calculated, and then the hash value is transformed into the initial value of hyper-chaos, thus n random grids are generated by different hyper-chaos. Lastly, after expanding the sub-image to the same size with the original secret image, it is performer XOR operation with the corresponding random grid, this will accordingly produce n sharing secret. In order to securely outsource the image in the cloud, the generated shares are issued to the n different cloud server. For authorized user, (s)he can get shares from different cloud server, and then can recover the original secret image through a series of decryption operations and extraction of reversible watermarking. The proposed scheme can losslessly restore the original secret image, and have the double verification ability, that is to say, it can verify whether the anyone of the sharing is modified, and it can also verify whether the original secret image is completely reconstructed. Some analysis and comparisons are given to show the security and effectiveness of proposed scheme.

KEYWORDS

Data Outsourcing, Hyper-Chaos, Random Grid, Reversible Watermarking, Visual Secret Sharing

1. INTRODUCTION

Cloud computing, one of the most important computing paradigms emerged in recent years, has become a good means for users to manage data efficiently. By outsourcing the data files into the cloud, the large enterprises as well as individual users can dynamically increase their storage space when required without buying any storage devices, and this also can reduce the costs for purchasing hardware equipment, managing enterprise data and maintaining the system. However, a major issue for cloud computing is the privacy of outsourced data, when data owner outsources the data to the cloud, (s)he may only allow the authorized user to visit the data, though cloud can provide some basic security mechanisms such as firewalls, it is thought untrusted, so privacy-preserving of data owner

DOI: 10.4018/IJDCF.2018010103

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

in the cloud environment is a challenging task, especially on data privacy, security and reliability issues (Song, Wagner, & Perrig, 2000; Ziegeldorf, Morchon, & Wehrle, 2014; Henze et al., 2013).

At present, encryption of sensitive data is the most extensively used methods to fulfill data security in the cloud. That is, data owners place the encrypted data in the cloud, and only the authorized users can decrypt the data and visit them. Up to now, people have proposed many schemes to guarantee the security of data in the cloud using asymmetric or symmetric algorithm (Zhu et al., 2016; Zou et al., 2016; Shaozhang, Shanshan, & Huang, 2015; Li & Ma, 2014; Hadavi & Jalili, 2010). Among them, Hui Zhu et al. (2016) proposed an efficient privacy-preserving location-based services query scheme in outsourced cloud by using symmetric encryption algorithm; in the scheme, the location provider's data is encrypted and issued to the cloud, and the registered user can get accurate location query results from the cloud server. Qin Zou et al. gave a content-based image retrieval of cloud using comparable encryption algorithm (2016). In asymmetric encryption, Niu Shaozhang et al. presented a security access control for the data in the cloud efficiently by using asymmetric encryption system (2015); Keying Li and Hua Ma proposed an improved multi-authority attribute-based encryption for outsourced data by means of asymmetric and symmetric encryption (2014).

However, complexity of asymmetric or symmetric encryption/decryption operations is extremely high, so they are not efficient facing with the explosive growth in the amount of outsourced data in the number of access. Thus, as an emerging approach for the encryption of outsourced data, secret sharing has attracted much attention for its low computational complexity in recent years (Hadavi & Jalili, 2010; Agrawal et al., 2011; Dautrich & Ravishankar, 2012; Liu & Chang, 2016; Liu, Wu, & Chang, 2014; Hadavi et al., 2015; Hong, Kim, & Chang, 2016). For example, in the schemes proposed by Agrawal (2011), a data file is divided into n sections shared among n cloud storage servers; who has the knowledge of any t or more pieces can recover the file. The developers of these schemes have claimed that they are secure, but Dautrich pointed out the scheme is vulnerable to the collusion attack in which any t colluding servers can recover all files outsourced in the cloud (2012), Recently, Liu et al. proposed a secure secret sharing mechanism based on Shamir's secret sharing method, the scheme can allow an authorized data user to recover all data files in a specified subset (2014). Mohammad et al. studied the security and search-ability in secret sharing-based data outsourcing, and proposed multiple partitioning methods that enable clients to efficiently search among shared secrets (2015).

In this paper, a novel and verifiable random grid-based image security scheme for outsourcing the image to the cloud is proposed. In the scheme, data owner firstly embeds the hash value of the image into the image itself using reversible algorithm; then, watermarked image is divided into n sections. Secondly, the hash of n sub image is calculated, and then the hash value is transformed into the initial value of hyper-chaos, thus n random grids are generated by using hyper-chaos. Lastly, after expanding the sub image to the same size with the original image, it is performer XOR operation with the corresponding random grid, this will accordingly produce n sharing secret. In order to outsource the image in the cloud, we only need to put the n sharing secret in the different cloud server, this will guarantee the security of the outsourced image.

The proposed scheme can make user losslessly restore the original secret image, and have the double verification ability for sharing secret and the restored secret image. The above advantages make it especially suitable for secret sharing of important images such as medical and military images. Large numbers of experiments show the effectiveness of proposed scheme and the authorized users can access and restore the original image in a secure manner, and some comparisons and analysis are also given to explain the highlights of the proposed scheme.

2. PRELIMINARIES

In this section, some knowledge and technology related to the scheme, including hash function, RG-based VSS, reversible watermarking and the hyper-chaotic system based encryption algorithm are firstly introduced.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/random-grid-and-reversible-watermarking-based-on-verifiable-secret-sharing-for-outsourcing-images-in-cloud/193018

Related Content

Dynamic Structural Statistical Model Based Online Signature Verification
Yan Chen, Xiaoqing Dingand Patrick S.P. Wang (2011). *New Technologies for Digital Crime and Forensics: Devices, Applications, and Software (pp. 239-256).*
www.irma-international.org/chapter/dynamic-structural-statistical-model-based/52857

Ethical Hacking, Threats, and Vulnerabilities in Cybersecurity
Nabie Y. Conteh (2021). *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 1-18).*
www.irma-international.org/chapter/ethical-hacking-threats-and-vulnerabilities-in-cybersecurity/282221

Medical Images Authentication through Repetitive Index Modulation Based Watermarking
Chang-Tsun Liand Yue Li (2009). *International Journal of Digital Crime and Forensics (pp. 32-39).*
www.irma-international.org/article/medical-images-authentication-through-repetitive/37423

Behavioural Evidence Analysis: A Paradigm Shift in Digital Forensics
Barkha Shreeand Parneeta Dhaliwal (2021). *International Journal of Digital Crime and Forensics (pp. 20-42).*
www.irma-international.org/article/behavioural-evidence-analysis/283125

A Model of Cloud Forensic Application With Assurance of Cloud Log
More Swami Das, A. Govardhanand Vijaya Lakshmi Doddapaneni (2021). *International Journal of Digital Crime and Forensics (pp. 114-129).*
www.irma-international.org/article/a-model-of-cloud-forensic-application-with-assurance-of-cloud-log/283130