Information Sciences 422 (2018) 77–97

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Reversible data hiding based on Shamir's secret sharing for color images over cloud

Priyanka Singh[a,*], Balasubramanian Raman[b]

[a] Department of Computer Science, University at Albany, State University of New York, USA
[b] Department of Computer Science and Engineering, Indian Institute of Technology at Roorkee, Uttarakhand, INDIA

ARTICLE INFO

Article history:
Received 17 March 2017
Revised 18 August 2017
Accepted 23 August 2017
Available online 1 September 2017

Keywords:
Shamir's secret sharing
Encrypted domain
Rightful ownership

ABSTRACT

To reduce the vulnerability of the multimedia content against the wide attacking surface of the cloud-based paradigm, obscuring the information before dissemination becomes a necessary step. In this paper, a reversible data hiding scheme based on Shamir's secret sharing for rightful ownership verification in encrypted domain has been proposed. It obscures the cover information via distributing it into multiple random looking shares and embeds a secret information specific to the owner into some of these encrypted shares based on a secret key prior to outsourcing the media information to cloud servers. The shares reveal no information at the cloud servers and even if they get attacked at these cloud servers, the owner information can be extracted to provide the rightful ownership of the media. The scheme facilitates extraction of secret information either directly from the cloud servers or after recovery of the original media at the authentic entity end possessing the secret keys. The robustness of the scheme has been validated by considering different attack scenarios in the encrypted domain itself. The visual quality of the recovered media and the extracted secret information evaluated via peak signal to noise ratio (PSNR), normalized cross correlation metric (NCC) and structural similarity index (SSIM) prove the efficacy of the proposed scheme.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

The explosive growth in the amount of multimedia content is pushing people to switch to cloud-based architecture that provides immense functionalities of enormous storage space and high end computational resources. For utilization of such resources, one only needs to transmit multimedia data to the cloud servers for processing. After completion of the process, the data can be retrieved back by the user [2]. However, the wide attacking surface of cloud-based architecture poses a high chance of security breaches to the residing content [1,5]. To address this alarming issue, secure signal processing is pacing as a very active research area where efforts are being made to provide the same functionalities as those provided in the plain domain to keep the data secured in the encrypted domain. Encryption for preserving privacy of content can be attained by the traditional encryption techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), etc.

[*] Corresponding author.
E-mail address: psingh9@albany.edu (P. Singh).

http://dx.doi.org/10.1016/j.ins.2017.08.077
0020-0255/© 2017 Elsevier Inc. All rights reserved.

However, processing on such encrypted data is a real challenge and may not be possible with these encryption schemes. Only partial or fully homomorphic encryption schemes can make the processing feasible in the encrypted domain as they preserve the relationship of the plaintext domain in the encrypted domain also [20,23]. The real challenge of processing while keeping the data encrypted varies from application to application and needs to be resolved specifically while solving the problem.

Watermarking has served for decades as a very successful technique to secure the content in the plaintext domain but its potential in the encrypted domain has been explored to a lesser extent [13,18,21,22,24]. Guo et al. proposed a robust watermarking scheme in the encrypted domain via integrating discrete wavelet transform with discrete cosine transform [10]. They used the partial homomorphic pallier cryptosystem towards attaining this goal and provided a secure technique against attacks in encrypted domain. Maintaining the privacy of the buyer seller protocol by devising a watermarking scheme by embedding encrypted fingerprint information of the buyer into publicly available encrypted information of seller was proposed in [17]. The scheme proved quite secure as seller could not fetch information of the watermarked version of the buyer and the buyer could not get hold of the original image information as well. Another encrypted domain robust watermarking scheme addressing traitorship issue while distribution of media in a multi level network was proposed in [25]. The watermark was embedded in JPEG2000 compressed and encrypted content.

Zhang has proposed a scheme for separable reversible data hiding in encrypted images by compressing the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate additional data [30]. In [11], the encrypted image was partitioned into blocks and data extraction along with image recovery was performed by examining the smoothness of the block. It used the side match scheme to decrease the error rate of extracted bits. Yuan has investigated secret sharing scheme with steganography in which two secret sharing methods for natural images based on multi-cover adaptive steganography have been proposed [29]. In [16], a threshold based secret sharing scheme with capabilities of steganography and authentication has been proposed. It divides the image into n shares that are hidden in camouflage image in which fragile watermark signals are embedded for authentication to form stego-image. However, it suffered from the drawback that dishonest participants could easily manipulate the stego-image. This issue has been considered in [28] which improves upon the method proposed in [16] and prevents dishonest participants from cheating. Scheme presented in [6] further improves the schemes proposed in [16,28] by employing Chinese Remainder Theorem (CRT) for enhancement of visual quality of the stego-images. A detailed cryptanalysis of image encryption schemes based on CRT has been done in [14]. In [27], instead of directly replacing the LSBs of cover images with secret data and authentication code, optimal pixel adjustment process has been applied to enhance image quality. A tunable visual image quality based on genetic algorithm has been proposed in [12]. It models the steganography problem as a search and optimization problem. In [26], a data hiding method based on secret sharing scheme with DNA exclusive or (DNA-XOR) operator for color images has been proposed.

For protection of medical images, a joint encryption and watermarking system based on stream cipher and block cipher has also been presented in [3]. It facilitates the extraction of watermark and decryption as independent tasks at the verification stage though it was combined at the protection stage. In [9], a reversible data hiding for medical images has been proposed. The scheme achieves contrast enhancement of region of interest (ROI) and tamper localization against attacks on the ROI via segmentation of ROI and background of medical image using Otsus automatic optimal thresholding method. Separability of information extraction is quite encouraged as data embedders may not always be the data owners. One such data hiding scheme that encrypted the content and compressed the least significant bits of encrypted data for hiding additional information was presented [31]. Depending on the keys possessed by the entity, the corresponding data could be extracted whether it is the secret information or the recovery of the original media. It eradicated the problems existing in a pipeline system where one must be followed by the other. Another variant of the scheme came further that included the recovery information of the content and proposed a visible watermarking framework [32]. Partial encryption based scheme embedding secret information into plaintext domain though reduced computational complexity and data expansion problems of homomorphic schemes, but still the security of the plaintext regions remained vulnerable [4,15].

A privacy preserving watermarking scheme for outsourcing multimedia content over cloud and rightful ownership verification in encrypted domain has been proposed in this article. The scheme secures the information by distributing it into multiple random looking information theoretically secure shares. These shares are obtained based on the Shamir's secret sharing and their homomorphic properties are exploited to embed an owner specific secret information in some of these random looking shares based on a secret key. The owner specific information can be extracted on the receiver end either directly from the cloud data centers or after recovery of the watermarked media at the authentic entity end possessing the secret keys. A comparative study of the proposed scheme with the state-of-the-art approaches has been presented in Table 1. Thus, the scheme addresses the aforementioned challenges of processing in encrypted domain as follows:

- Information theoretic security: The shares outsourced at the cloud data centers are information theoretically secure i.e. no matter how much computation power an adversary has, no information can be retrieved from them.
- Facilitates separability of secret information extraction from recovery of media: Depending on the secret keys, either the owner specific information can be extracted directly from the cloud centers or can be extracted after the recovery of the cover media at the authentic entity end.

Download English Version:

https://daneshyari.com/en/article/4944110

Download Persian Version:

https://daneshyari.com/article/4944110

Daneshyari.com