TPEIP: Thumbnail preserving encryption based on sum preserving for image privacy

Cheng-Hsing Yang, Chi-Yao Weng, Yu-Zhen Yang

https://doi.org/10.1016/j.jisa.2022.103352

Abstract

Image privacy technology is a growing important topic in cloud storage services. User can use the cloud services to browse or manage their own images, however, the user will face the problem of image privacy. Accordingly, the traditional image encryption scheme is a way to ensure the safety of images. However, encrypted images will lose their image usable property when users want to search and browse their own images online without downloading and decrypting them. Marohn et al. designed two thumbnail-preserving-encryption (TPE) methods to balance the image privacy and usability. In this paper, a novel TPEIP method based on sum-preserving-encryption (SPE) is proposed for enhancing the image privacy. SPE can avoid the statement of fail encryption using the approximate TPE method. We also applied formulas to present the correctness of the proposed scheme. The combination of thumbnail and encryption approach allows the user to quickly compare encrypted images using thumbnail. Experimental results show that our proposed method not only retained the same thumbnail appearance before and after encryption but also held the image encryption with sufficiently confidential.

Introduction

As network technology continues to develop, the applications in cloud computing have become increasingly important for users. The popularity of smart phones and photographic devices affects people's daily lives, such as using devices to capture and download images and videos. Many people apply the social apps or cloud spaces such as Apple [1], Google, Microsoft, and Dropbox, to share their images and videos generated daily [[2], [3], [4]]. According to a report [5], the number of new photos shared weekly by social app users was over a billion in 2010.

With more and more images being generated and stored in the cloud, users can share and download all images via network in any access devices. However, the context of multimedia protection and security is becoming increasingly important. Image privacy is a good way to prevent unauthorized access. An unauthorized access indicates that the legal user can view and access images or videos uploaded to the cloud, but the illegal user does nothing. Image encryption is a way to allow only authorized access, but an encrypted image contains noise, which cause inconvenience to users. Assume that users will search and view images, they should first decrypt the images from the cloud and then select the decrypted images and download them. However, this access method is not suitable for further management and application because the selected images should be first decrypted before searching and downloading them.

Cloud computing provides many services, such as image sharing or document downloading by users. Users can utilize the cloud space to store files, and reduce file corruption or loss caused by any destruction or misplacement of hardware devices. However, storing data in the cloud is vulnerable to some attacks. Attackers may use illegal tools to steal cloud data [6], and insiders may also illegally access data [7], causing large personal data leakages.

Encrypted data can be used to solve these problems. The data stored and uploaded to the cloud [8,9] are encrypted so that cloud administrators or attackers can only see the encrypted data and cannot directly use the data for other data analyses. However, this solution reduces the convenience of using cloud data. For instance, in the case of images, unencrypted images allow users to quickly search the desired image, as shown in Fig. 1(a). Instead, the encrypted images are indecipherable, and the users cannot directly browse the encrypted images to search for the desired images, as displayed in Fig. 1(b). Traditional image encryption methods can reduce the flexibility of image management.

In 2013, Ra et al. proposed a privacy-preserving image scheme called P3 [11]. Image processed in the P3 method are first divided into secret and public parts, the DC-coefficient is encrypted from the image into the secret part, and the residual coefficient is kept as the public part, marking the image unrecognizable and usable on social networks. This method can enable image privacy with transmission

latency, large storage spaces, occupied bandwidth provided by sharing providers [12]. Additionally, Zhang et al.'s proposed a framework of privacy-preserving outsourced image sharing to protect the image privacy. In their method, they ensure that the cloud service provider can give a secure environment for user who want to outsource images management to share and search their images via mobile device or unauthorised social network. However, in 2016, McPherson et al. indicated that the P3 method is vulnerable to recognize face using deep learning [13].

The thumbnail-preserving encryption (TPE) technology is another method to protect images and manage flexibility. In 2015, Wright et al. proposed a method that allows exchanging pixels within each block to encrypt JPEG images, and the encrypted images will have the effect of thumbnails [12]. The effect of thumbnails means that the image does not show detailed features, only displaying a rough sketch, and such an effect can be used to protect the image. Fig. 1(c) shows an image that is still slightly visible after encryption, allowing it to be easily managed by users. Thumbnails can be applied to search a desired image before decrypting it to the original image. If an encrypted image is stored in the cloud environment, then an attacker or an unauthenticated user cannot decrypt the image. In 2017, Marohn et al. proposed three approximate TPE encryption schemes to achieve image encryption that can be retained by thumbnails [14]. In addition, Tajik et al. (2017) proposed a cryptography method for thumbnail preserving, which balances image privacy and usability [15]. These proposed cryptography methods not only retain the effect of thumbnails but also keep the effect of image features for users to search the desired image, such as histogram [16], blockwise [17], and others [18,19]. This study inspects the TPE technology proposed by Tajiks et al. and methods proposed by other scholars and proposes a novel TPE scheme based on sum-preserving encryption (SPE) to solve the encrypted problem. The method proposed by Marohn et al. fail to completely restore the image. However, the proposed method can fully restore the original image after decryption.

The rest of the paper is organized as follows. The related work is presented in Section 2. The proposed schemes of sum-preserving are introduced detailly in Section 3. The experiment results are demonstrated in Section 4. Finally, the conclusion is draw in Section 5

Section snippets

Related work

In this section, we will review two TPE methods: the approximate TPE method proposed by Marohn et al. in 2017 [14], and the TPE method proposed by Tajik et al. in 2019 [15]. These methods have vulnerability in some situations, which will be aptly described in the following sections.

Our TPEIP based on SPE approach

The new SPE method is proposed in this section. The new SPE method not only improves the method of Tajik et al. but can also avoid the fail encryption problem encountered by the previous method. Assume that we have a pair of pixels (a, b), s is the sum of a and b; and d is 255. Two cases are presented as follows.

Case 1 ($s \le d$): The encrypted result of a must be in the range of [0, s]. Otherwise, the encrypted result of b will not exist, as shown in Fig. 2.

Case 2 ($s > d$): Let , , and

Experimental results

In this section, we analyze the experimental result and the proposed methods. We experimented with two images, named as Peppers and Baboon images, whose the image size is 512 × 512.

Fig. 7(a) is the original image of Peppers, whose thumbnail is shown in Fig. 7(d). Fig. 7(b) and Fig. 7(c) show the use of our thumbnail encryption results for encrypted Lena images, where Fig. 7(b) uses a block size of 16 × 16 and Fig. 7(c) uses a block size of 64 × 64. Fig. 7(e) is the thumbnail generated in Fig. 7

Conclusions

Image privacy for the cloud storage and service provider is addressed in this study. Traditional image encryption schemes can offer image privacy in the cloud storage, but it can lose the property of image privacy. Accordingly, TPE can avoid the issue on image privacy. This

article proposes a novel TPEIP method based on SPE. Our SPE can avoid fail encryption using the approximate TPE method. The experimental results show that the proposed method can achieve the image encryption, where the

CRediT authorship contribution statement

Cheng-Hsing Yang: Supervision, Conceptualization, Methodology. Chi-Yao Weng: Writing the original draft, Investigation. Yu-Zhen Yang: Coding, Simulation.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was partially supported by the National Science and Technology Council of the Republic of China under the Grant No. MOST 108-2221-E-153-006, 108-2221-E-153-004-MY2, MOST 109-2221-E-153-004, 110-2221-E-153-002-MY2, 111-2221-E-153-005 and the Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

References (21)

H. Cheng *et al.*
Encrypted JPEG image retrieval using block-wise feature comparison
J Vis Commun Image Represent (2016)

Y. Su *et al.*
Reversible cellular automata image encryption for similarity search
Signal Process (2019)

H. Liang *et al.*
Huffman-code based retrieval for encrypted JPEG images
J Vis Commun Image Represent (2019)

C. Moss
Integrating cloud computing and mobile applications: a comparative study based on icloud and sanscode
J Cloud Comput (2014)

J. Yu *et al.*
iPrivacy: image privacy protection by identifying sensitive objects via deep multi-task learning
IEEE Transact Inform Forens Secur (2017)

Z. Zhang *et al.*
PIC: enable large-scale privacy preserving context-based image search on cloud
IEEE Transact Parall Distrib Syst (2017)

K. Lida *et al.*
Privacy-preserving content-based image retrieval using compressible encrypted image
IEEE Access (2020)

D. Beaver *et al.*
Finding a needle in Haystack: Facebook's photo storage

K. Gurudatt *et al.*
Mobile cloud computing: security threats

U.H. Rao and U. Nayak, “Access Controls”, In: The infosec handbook, Berkeley, CA, DOI:...

Cited by (16)

A privacy-preserving cross-media retrieval on encrypted data in cloud computing
2023, Journal of Information Security and Applications

> *Citation Excerpt :*
>
> Searchable encryption techniques enhance security while maintaining data searchability. However, existing research on searchable encryption techniques has focused on single-media retrieval such as text [14] and images [15,16], which cannot meet the growing demand for cross-media retrieval. Existing single-media searchable encryption techniques for text and images differ significantly in encryption methods [17], feature selection [18], and index construction [19,20], so single-media encrypted retrieval techniques cannot be directly applied to cross-media encrypted retrieval.

Show abstract

Privacy-Preserving TPE-Based JPEG Image Retrieval in Cloud-Assisted Internet of Things
2024, IEEE Internet of Things Journal

TPE-MM: Thumbnail preserving encryption scheme based on Markov model for JPEG images
2024, Applied Intelligence

TPE-ADE: Thumbnail-Preserving Encryption Based on Adaptive Deviation Embedding for JPEG Images
2024, IEEE Transactions on Multimedia

Chaos-Based Image Encryption: Review, Application, and Challenges
2023, Mathematics

Usability Enhanced Thumbnail-Preserving Encryption Based on Data Hiding for JPEG Images
2023, IEEE Signal Processing Letters