An Efficient System for impulsive Data Screening in Encrypted images

[1]Vanitha C
chanvani2009@gmail.com
Assistant Professor

[2]Giribabu V
vemulagiribabu@gmail.com

[3] Jagan P
jaganpadmanaban@gmail.com

[4] Karthikeyan D
karthikn1241@gmail.com

[2][3][4]UG students
Department of Computer Science and Engineering
T.J.S. Engineering College

Abstract

As in Cloud Environment, it is vital to protect the privacy of data and enable the cloud server to easily manage the data at the same time. , we propose a novel framework for IDS-EI (Impulsive Data Screening-Encrypted Images) based on reversible image transformation (IIT). Different from all previous encryption based frameworks, in which the ciphertexts may attract the notation of the curious cloud, IIT-based framework allows the user to transform the content of original image into the content of another target image with the same size. The transformed image, that looks like the target image, is used as the "encrypted image", and is outsourced to the cloud. Therefore, the cloud server can easily embed data into the "encrypted image" by any IDS methods for plaintext images. Two IDS methods, including traditional IDS scheme and unified embedding and scrambling scheme, are adopted to embed watermark in the encrypted image, which can satisfy different needs on image quality and large embedding capacity respectively.

Index Terms – impulsive data screening , image encryption, impulsive image transformation, privacy protection

1. Introduction

Now a days outsourced storage by cloud becomes a more and more popular service, especially for multimedia files, such as images or videos, which need large storage space. To manage the outsourced images, the cloud server may embed some additional data into the images, such as image category and notation information, and use such data to identify the ownership [1] or verify the integrity of images. Obviously, the cloud service provider has no right to introduce permanent distortion during data embedding into the outsourced images. Therefore, impulsive data Screening (IDS) technology is needed, by which the original image can be losslessly recovered after the embedded message is extracted. This technique is also Widely used in medical imagery [2], military imagery and law forensics, where no distortion of the original cover is allowed.

So far, many IDS methods on images have been proposed. In essence, all these methods can be viewed as a process of semantic lossless compression [3], [4], in which some space is saved for embedding extra data by losslessly compressing the image. Herein, "semantic compression" means that the compressed image should be close to the original image, and thus one can get a marked image with good visual quality. Because the residual part of images, e.g., the prediction errors (PE), has small entropy and can be easily compressed, almost all recent IDS methods first generate PEs as the host sequence [5]–[7], and then reversibly embed the message into the host sequence by modifying its histogram with methods like histogram shifting (HS) [8] or difference expansion (DE) [9]. Proposed the optimal histogram modification Algorithm [4], [10] for IDS by estimating the optimal modification probability [11], [12].

On the other hand, cloud service for outsourced storage makes it challenging to protect the privacy of image contents. For instance, recently many private photos of Hollywood actress leaked from iCloud [13]. Although IDS is helpful for managing the outsourced images, it cannot protect the image content. Encryption is the most popular technique for protecting privacy. So it is interesting to implement IDS in encrypted images (IDS – EI), by which the cloud server can reversibly embed data into the image but cannot get any knowledge about the image contents. Inspired by the needs of privacy protection, many methods have been presented to extend IDS methods to encryption domain. From the viewpoint of compression, these methods on IDS-EI belong to the next two frameworks [14]: Framework I "vacating room after encryption (VRAE)" and Framework II "reserving room before encryption (RRBE) ".

2. Framework Comparison

The differences between the the novel frame-work and previous frameworks, which shows that, by frame-works VRAE and RRBE, the user's images are stored in the form of ciphertext in the cloud account, while by the the IIT-based framework, the image is stored in a form of plaintext.

In the framework VRAE shown in Fig.1(a), such as schemes in [17] and [18], the image owner (the sender) encrypts the image I into E(I) with a key K. The cloud server embeds data by compressing the encrypted image E(I) and generates $E_w(I)$ that is stored in the cloud. When getting a retrieval request, the cloud server returns $E_w'(I)$ to the recevier, maybe an authorized third party, who generates I through a process of joint decompression and decryption with the key K. Herein, $E_w'(I)$ may be just $E_w(I)$ or a modified version obtained by removing the embedded data. Note that the cloud server cannot restore E(I) from $E_w(I)$, since decompression should be joined with decryption with the help of K. In this framework, the complexity is taken on by the receiver who must join the process of decompression and decryption to get the original image. In other words, the compression-based IDS method used by the cloud server should be specified together with the receiver, i.e., the IDS method is receiver-related.

In the framework RRBE shown in Fig.1(b), such as schemes in [14], [22], the image owner (the sender) reserves room from the image I and encrypts it into E(I) with a key K, and then sends it to the cloud server who embeds data into the reserved room and generates $E_w(I)$. $E_w(I)$ is stored in the cloud, from which the cloud server can extract the data that is used for management. When an authorized user (the receiver) wants to retrieve the image, the cloud server can restore E(I) from $E_w(I)$ and send E(I) to the user who can decrypt E(I) and get I with the key K. In the framework RRBE, the complexity is borne by the sender who should reserve room for IDS by exploiting the redundancy within the image and thus the IDS method used by the cloud should be specified with the sender, that is, the IDS method used by cloud is sender-related.

- The idea of IIT is exploited for IDS-EI, by which the user can outsource the encrypted image to the cloud in a form of plaintext and thus it will avoid the attention of the curious cloud.
- In the IIT based framework, the cloud server can easily embed data into the "encrypted image" by arbitrarily selecting IDS methods for plaintext images such as those in [4], [6], [7], [10]. In other words, the IDS used by the cloud is irrelevant with both the sender and receiver, which is called a client-free IDS-EI scheme by us. "Client free" is important for the scenarios of public clouds, in which it is hard for the cloud server to ask the clients how to encrypt or decrypt their data, because the cloud is thought to be only semi-honest [24].

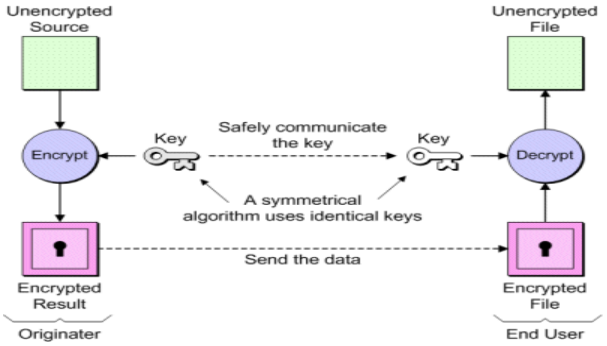
3. Literature Review

Many different approaches have been proposed. In Tailored Reversible Watermarking Schemes for Authentication of Electronic Clinical Atlas [1] It is accepted that digital watermarking is quiterelevant in medical imagingHowever, due to the special nature of clinical practice, it is often required that watermarking do not introduce irreversible distortions to medical imagesElectronic clinical atlas has such a need of "lossless" watermarking.We present two tailored reversible watermarking schemes forclinical atlas by exploiting its inherent characteristics Recursive Histogram Modification: Establishing Equivalency Between Reversible Data Hiding and Lossless Data Compression [2 State-of-the-art schemes for reversible data hiding (IDS) usually consist of two steps: first construct a host sequence with a sharp histogram via prediction errors, and then embed messages by modifying the histogram with methods, such as difference expansion and histogram shift Reversible Watermarking Algorithm Using Sorting and Prediction [3], This paper presents a reversible or lossless watermarking Algorithm for images without using a location map in most cases.This Algorithm employs prediction errors to embed data into an image. A sorting technique is used to record the prediction errors based on magnitude of its local variance. Using sorted prediction errors and, if needed, though rarely, a reduced size location map allows us to embed more data into the image with less distortion.The performance of the proposed reversible watermarking scheme is evaluated using different images and compared with four methods.But the strengthening of initial seed set is difficult. It also finds the multiple memberships of the individual users. Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding [4 In prediction-error expansion (PEE) based reversible data hiding, better exploiting image redundancy usually leads to a superior performance. However, the correlations among prediction-errors are not considered and utilized in current PEE based methods. Local-Prediction-Based Difference Expansion Reversible Watermarking [5], This paper investigates the use of local prediction in difference expansion reversible watermarking. For each pixel, a least square predictor is computed on a square block centered on the pixel and the corresponding prediction error is expanded. The same predictor is recovered at detection without any additional information

4. Existing System

In Existing concept user content by relying on content matching has processed. Most images are not encrypted but texts are encrypted correctly. Encryption

is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended, is encrypted using an encryption Algorithm, generating cipher text that can only decrypted.



The content of another target image is not get correctly. Privacy is not sure are the main disadvantages.

5. Proposed System

5.1 AN EXAMPLE ON IMPULSIVE IMAGE TRANSFORMATION

In this section, we propose a method of IIT to encrypt spatial images, which is inspired by the technique of image transformation proposed by Lee et al. [26]. Lee et al.'s method can transform the original image to a freely-selected target image with the same size, yielding a secret-fragment-visible mosaic image defined in [25]. But the original image cannot be restored in a lossless way. It is not reversible, so it is not suitable for the scenario of IDS-EI. We will modify Lee et al.'s method to be reversible and obtain an encrypted image which looks like the target image.

For color images, we transform the color channel R, G, and B respectively in the same manner. So we just take gray images (one channel) as an example to describe the method. For an original image I, we randomly select a target image J having the same size with I from an image database.

Firstly, we divide the original image I and the target image J into N non-overlapping blocks respectively, and then pair the blocks of I and J as a sequence such that $(B_1, T_1), \ldots, (B_N, T_N)$, where B_i is an original block of I and T_i is the corresponding target block of J, $1 \le i \le N$. We will transform B_i toward T_i and generate a T_i' similar to T_i. After that, we replace each T_i with T_i' in the target image J to get the transformed image J′. Finally we embed some accessorial information into J′ with an IDS method

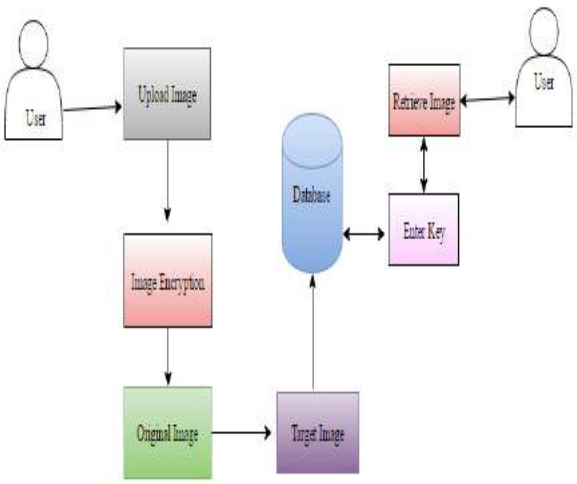


Fig 5:System Architecture

Algorithm 1 Procedure of Transformation

Input: An original image I and a secret key K. **Output:** The encrypted image E(I).

1) Select a target image J having the same size as I from an image database.
2) Divide both I and J into several non-overlapping 4×4 blocks. Assuming that each image consists of N blocks, calculate the mean and SD of each block.
3) Classify the blocks with %α quantile of SDs and gen-erate CITs for I and J respectively. Pair up blocks of I with blocks of J according the CITs as described in subsection III-A.
4) For each block pair (B_i, T_i) $(1 \le i \le N)$, compute the mean difference u_i. Add u_i to each pixel of B_i and then rotate the block into the optimal direction θ_i ($\theta_i \in \{0^o, 90^o, 180^o\ 270^o\}$, which yields a transformed block T_i'.
5) In the target image J, replace each block T_i with the corresponding transformed block T_i' for $1 \le i \le N$ and generate the transformed image J′.
6) Collect u_i's and θ_i's for all block pairs, and compress them together with the CIT of I. Encrypt the compressed sequence and the parameter α by a standard encryption scheme such as AES with the key K.
7) Take the encrypted sequence as accessorial information (AI), and embed AI into the transformed image J′ with an IDS method such as the one in [7], and output the encrypted image E(I).

Algorithm 2 Procedure of Anti-transformation

Input: The encrypted image E(I) and the key K. **Output:** The original image I.

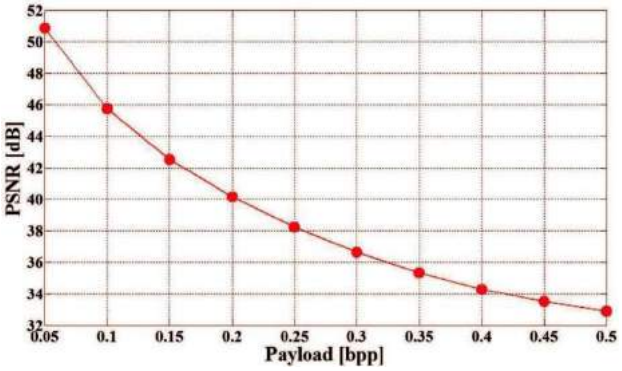
1) Extract AI and restore the transformed image J' from E(I) with the IDS scheme in [7].
2) Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I, u_i, θ_i ($1 \le i \le N$) and α.
3) Divide J' into non-overlapping N blocks with size of 4×4. Calculate the SDs of blocks, and then generate the CIT of J' according to the $\%\alpha$ quantile of SDs.
4) According to the CITs of J' and I, rearrange the blocks of J' as described in Subsection III-A.
5) For each block T_i' of J' for $1 \le i \le N$, rotate T_i' in the anti-direction of θ_i, and then subtract u_i from each pixel of T_i', and finally output the original image I.

5.2 IDS IN ENCRYPTED IMAGE

IIT generates an encrypted image E(I), which has the advantage of keeping a meaningful form of the image com-pared to traditional encryption methods. Therefore, it is free for the cloud server to employ any classical RDS on the encrypted image. Selecting what kind of RDS method depends on whether to keep the image quality or not. In this section we simply adopt two RDS methods, one is a traditional RDS that keeps the quality of images and the other is a unified data embedding and scrambling method that may greatly degrades image structures for embedding large payload.

A. Traditional RDS on the encrypted image

It should be noted that any one of classical RDS method for plaintext image can be implemented to embed and extract watermark in the encrypted image E(I) in the IIT based scheme. As an example, we select the method proposed by Dragoi et al. [7] to embed watermark into the encrypted image. Dragoi et al.'s method is a typical PEE (predicted error expansion) based RDS method, in which a new local least square (LLS) predictor with high prediction accuracy is predicted. Obviously the smaller the PE is, the higher the quality of marked image will be. The scheme of Dragoi et al. is briefly described as follows. For each pixel, a least square predictor is computed on a square block centered on the pixel, which can adaptively make use of every neighbor pixel's distinction in a local region. The most interesting aspect of the approach is the fact that the same predictor can be realized at the receiver side, avoiding the need of embedding a large amount of additional information. Having predicted the current pixel, the predicted error (PE) will be shifted for vacating room or be expanded for embedding one message bit. For more details please refer to [7].



We depicted the average PSNR results of 100 test images between the marked image and the encrypted image given

6. Conclusion

We realize an IIT based method by improving the image transformation technique is to be reversible. By IIT, we can transform the original image arbitrary selected target image with the same size, and restore the original image from the encrypted image in a lossless way. Two IDS methods including PEE-based IDS and UES are adopted to embed watermark in the encrypted image to satisfy different needs on image quality and embedding capacity. Several interesting problems can be considered in the future, including how to improve the quality of the encrypted image and how to extend idea of IIT to audio and video.

9. References

[1] F. Bao, R. H. Deng, B. C. Ooi, et al., "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," IEEE Trans. On Information Technology in Biomedicine, vol. 9, no. 4, pp. 554-563,

[2] W. Zhang, X. Hu, N. Yu, et al. "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. on Image Processing, vol. 22, no. 7, pp.2775-2785, Jul. 2013.

[3] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. On Circuits and Systems for Video Technology

[4] B.ou, X. Li, Y. Zhao, R. Ni, Y. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," IEEE Trans. on Image Processing [5] Ioan-Catalin Dragoi, Dinu Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014.