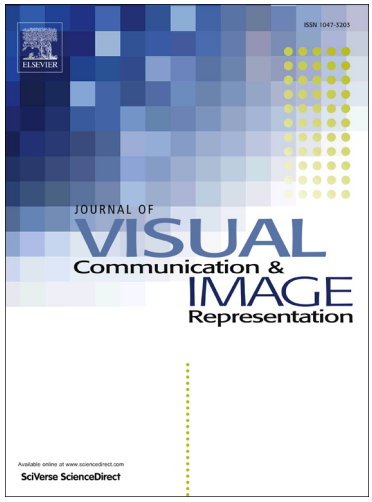
Accepted Manuscript



Improved Joint Reversible Data Hiding in Encrypted Images

Zhenxing Qian, Shu Dai, Fei Jiang, Xinpeng Zhang

PII: S1047-3203(16)30179-1
DOI: http://dx.doi.org/10.1016/j.jvcir.2016.08.020
Reference: YJVCI 1849

To appear in: *J. Vis. Commun. Image R.*

Received Date: 13 April 2016
Revised Date: 5 July 2016
Accepted Date: 23 August 2016

Please cite this article as: Z. Qian, S. Dai, F. Jiang, X. Zhang, Improved Joint Reversible Data Hiding in Encrypted Images, *J. Vis. Commun. Image R.* (2016), doi: http://dx.doi.org/10.1016/j.jvcir.2016.08.020

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Improved Joint Reversible Data Hiding in Encrypted Images

Zhenxing Qian[1,2], Shu Dai[1], Fei Jiang[1], Xinpeng Zhang[1,3]

1. School of Communication and Information Engineering, Shanghai University, Shanghai, China

2. Nanjing University of Information Science Technology (NUIST), Nanjing, China

3. Key Laboratory of Specialty Fiber Optics and Optical Access, Shanghai University, Shanghai, China.

E-mail: zxqian@shu.edu.cn

***Abstract*—This paper proposes an improved method of reversible data hiding in encrypted images (RDH-EI). Three parties constitute the proposed system: the image owner, the remote server and the recipient. To preserve privacy, an image owner encrypts the original image using a stream cipher algorithm and uploads the ciphertext to a remote server. On server side, a data-hider is allowed to embed additional message into the encrypted image using a swapping/shifting based algorithm. After downloading the marked encrypted image from the server and implementing the decryption, a recipient can extract the hidden messages and losslessly recover the original image. Experimental results show that the proposed method achieves a larger payload than the related works. Meanwhile, a limitation in the related works that few bits can be embedded into the encrypted medical images is also eliminated in the proposed method.**

***Index Terms*—Reversible data hiding, image encryption, image recovery**

1. Introduction

Reversible data hiding (RDH) is a technique to embed additional message into a cover media, such as military or medical images, using a reversible manner such that the original cover content can be perfectly restored after the extraction of hidden messages [1][2]. Reversible data hiding in encrypted images (RDH-EI) is a new topic of reversible data hiding [3]. This technique allows a service provider to embed additional messages into encrypted images without accessing the original contents, and guarantees that the original images can be losslessly recovered on the recipient side. RDH-EI technique can be used in many applications [4-12]. For example in medical systems, the medical images can be encrypted before uploading to a server if a patient does not allow his/her privacy to be revealed to outsiders. Meanwhile, for a better management, the database administrator can embed the medical records or the patient's information into the encrypted image. This way, the storage payload can be saved, and the profile management is more convenient. On the other hand, when a doctor downloads the encrypted images containing additional information from the medical server, he/she can extract the patient's information exactly and recover the original medical images for diagnosis without any error.

Some works have been done in the field of RDH-EI. Generally, there are two kinds of RDH-EI approaches: the *joint* RDH-EI and the *separable* RDH-EI. In the former technique, hidden messages are extracted from the marked encrypted image by the user who has the decryption key, which is realized together with image recovery. While in the latter technique, hidden messages can be extracted by the one who has not the decryption key, in which data extraction and image recovery are separated. Compared with *separable* RDH-EI methods, *joint* RDH-EI methods always estimate the spatial correlation of pixels inside the original image. As a result, the marked image should be decrypted before extracting the hidden message and recovering the original contents.

RDH-EI was first proposed in [3], in which a content owner encrypts the original image using a stream cipher algorithm, and a data hider embeds additional message into encrypted blocks by flipping

Download English Version:

https://daneshyari.com/en/article/6938494

Download Persian Version:

https://daneshyari.com/article/6938494

Daneshyari.com