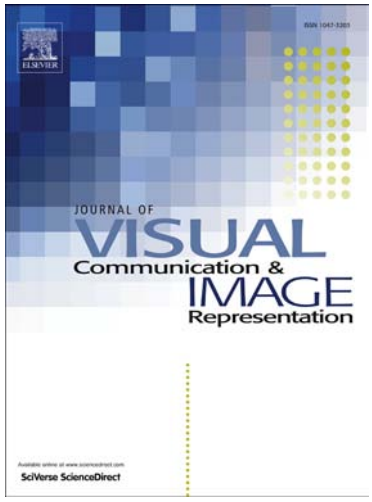

Short communication

JPEG Encryption for Image Rescaling in the Encrypted Domain

Zhenxing Qian, Xinpeng Zhang, Yanli Ren

PII: S1047-3203(14)00167-9
DOI: http://dx.doi.org/10.1016/j.jvcir.2014.10.008
Reference: YJVCI 1433

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

Received Date: 16 February 2014

Please cite this article as: Z. Qian, X. Zhang, Y. Ren, JPEG Encryption for Image Rescaling in the Encrypted Domain, *J. Vis. Commun. Image R.* (2014), doi: http://dx.doi.org/10.1016/j.jvcir.2014.10.008

JPEG Encryption for Image Rescaling in the Encrypted Domain

Zhenxing Qian, Xinpeng Zhang, Yanli Ren

School of Communication and Information Engineering, Shanghai University, Shanghai 200444

E-mail: {zxqian, xzhang, renyanli}@shu.edu.cn

Abstract: This work proposes a novel protocol of encrypting the JPEG image suitable for image rescaling in the encrypted domain. To protect the privacy of original content, the image owner perturbs the texture and randomizes the structure of the JPEG image by enciphering the quantized Discrete Cosine Transform (DCT) coefficients. After receiving the encrypted JPEG image, the service provider generates a rescaled JPEG image by down-sampling the encrypted DCT coefficients. On the recipient side, the encrypted JPEG image rescaled by the service provider can be decrypted to a plaintext image with a lower resolution with the aid of encryption keys. Experimental results show that the proposed method has a good capability of rescaling the privacy-protected JPEG file.

Keywords: signal processing, encrypted domain, image rescaling

1. Introduction

Signal processing in encrypted domain (SPED) has attracted much attention in recent years. The need for SPED technologies originates from a growing social awareness and relevance of security and privacy [1][2]. For example, people are increasingly sharing diversity of personal data on the Internet, or doing many works over cloud computing or delegated calculation. SPED, thus, was proposed to accomplish signal processing at the potentially untrusted sites in a privacy-protected form, without or minimally leaking information [3]. Some works have been done on SPED, such as differential-privacy based sanitizing [3-5], the buyer-seller watermarking protocol [6-9], compression of the encrypted images or videos [10-13], reversible data-hiding in encrypted images [14-18], and so on [19]. While most SPED algorithms are useful for never-compressed images, few SPED methods are suitable for JPEG, which is the most widely used format.

In some applications, the service provider hopes to reduce the data amount during the transmission, or tends to supply the recipient an encrypted image with a lower resolution. For example, in a dealing system, the seller