Accepted Manuscript

Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism

Di Xiao, Yanping Xiang, Hongying Zheng, Yong Wang

PII: S1047-3203(17)30038-X
DOI: http://dx.doi.org/10.1016/j.jvcir.2017.02.001
Reference: YJVCI 1952

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

Received Date: 29 May 2016
Revised Date: 6 January 2017
Accepted Date: 4 February 2017

Please cite this article as: D. Xiao, Y. Xiang, H. Zheng, Y. Wang, Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism, *J. Vis. Commun. Image R.* (2017), doi: http://dx.doi.org/10.1016/j.jvcir.2017.02.001

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.

Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism

Di Xiao [a*], Yanping Xiang [a], Hongying Zheng [a], Yong Wang [b]

[a] Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China

[b] Key Laboratory of Electronic Commerce and Logistics of Chongqing, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: This work proposes a separable reversible data hiding scheme in encrypted images based on pixel value ordering (PVO). After the original image is encrypted using homomorphism encryption by the content owner, the data hider embeds the secret data in encrypted domain. The PVO strategy realizes hiding data in each block. Additive homomorphism guarantees the performance of PVO in encrypted domain is close to that in plain domain. Besides, the homomorphism encryption does not cause data expansion, and the payload can be further improved. With the watermarked encrypted image, if the receiver has only the data hiding key, he can extract the additional data. If the receiver has only the encryption key, he can obtain a decrypted image similar to the original one. If the receiver has both the data hiding key and the encryption key, he can extract the additional data without any error and recover the original image losslessly.

Keyword: Reversible data hiding; encrypted image; pixel value ordering; additive homomorphism; separable

* Corresponding author: Di Xiao

Tel: +86-23-6510-3199; fax: +86-23-6510-4570; E- mail address: xiaodi_cqu@hotmail.com

Download English Version:

https://daneshyari.com/en/article/4969313

Download Persian Version:

https://daneshyari.com/article/4969313

Daneshyari.com