

# Author's Accepted Manuscript

Histogram shifting in encrypted images with public Key Cryptosystem for Reversible Data Hiding

Ming Li, Yang Li



PII: S0165-1684(16)30153-0  
DOI: <http://dx.doi.org/10.1016/j.sigpro.2016.07.002>  
Reference: SIGPRO6194

To appear in: *Signal Processing*

Received date: 7 January 2016  
Revised date: 30 June 2016  
Accepted date: 1 July 2016

Cite this article as: Ming Li and Yang Li, Histogram shifting in encrypted images with public Key Cryptosystem for Reversible Data Hiding, *Signal Processing* <http://dx.doi.org/10.1016/j.sigpro.2016.07.002>

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 galley proof before it is published in its final citable 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

# Histogram Shifting in Encrypted Images with Public Key Cryptosystem for Reversible Data Hiding

Ming Li<sup>a,b</sup>, Yang Li<sup>a,\*</sup>

<sup>a</sup> School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China

<sup>b</sup> College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China

**Abstract:** Histogram shifting is an effective reversible data hiding (RDH) approach in processing digital images. When the host image is encrypted for privacy protection in some open environments including the cloud, RDH has to be processed in the encrypted domain accordingly. However, the performance of the existing RDH schemes in encrypted images is generally not satisfactory due to the fact that signal processing in encrypted domain is a challenging problem. In this paper, an effective RDH technique in encrypted images is proposed. Specifically, the histogram of the image is first expanded by applying the homomorphic multiplication in the encrypted domain based on the public key cryptosystem, and the histogram shifting is achieved by using the homomorphic addition in the encrypted domain in order to embed the additional data into the host images. The embedded additional data can be extracted accurately, and the host images can be recovered perfectly. Extensive experiment results are illustrated that the data embedding rate is up to 1 bit per pixel (bpp) or even 1016 bpp regardless of the different pixel distributions of natural images. The performance of the proposed RDH approach is largely improved in encrypted images, which shows the effectiveness of the proposed method.

**Key words:** reversible data hiding, histogram shifting, encrypted image, homomorphic encryption, public key cryptosystem

\* Corresponding author.

E-mail addresses: liming@htu.edu.cn (M. Li), liyang@buaa.edu.cn (Y. Li).

Download English Version:

<https://daneshyari.com/en/article/6958140>

Download Persian Version:

<https://daneshyari.com/article/6958140>

[Daneshyari.com](https://daneshyari.com)