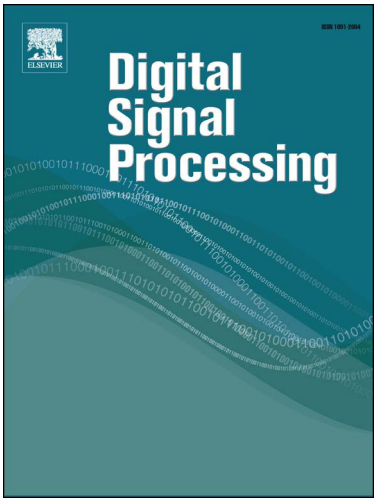
Accepted Manuscript



Chinese remainder theorem-based two-in-one image secret sharing with three decoding options

Xuehu Yan, Yuliang Lu, Lintao Liu, Jingju Liu, Guozheng Yang

PII: S1051-2004(18)30559-1
DOI: https://doi.org/10.1016/j.dsp.2018.07.015
Reference: YDSPR 2379

To appear in: *Digital Signal Processing*

Please cite this article in press as: X. Yan et al., Chinese remainder theorem-based two-in-one image secret sharing with three decoding options, *Digit. Signal Process.* (2018), https://doi.org/10.1016/j.dsp.2018.07.015

Chinese remainder theorem-based two-in-one image secret sharing with three decoding options

Xuehu Yan[a,*], Yuliang Lu[a], Lintao Liu[a], Jingju Liu[a], Guozheng Yang[a]

[a]*National University of Defense Technology, Hefei 230037, China*

Abstract

Two-in-one image secret sharing (ISS) with more decoding options has more applicable scenarios than that with only one decoding option. Conventional two-in-one ISS methods with more decoding options mainly combine visual secret sharing (VSS) and polynomial-based or XOR-based ISS. They have the drawbacks of lossy recovery for (k, n) threshold, only two decoding options, high computation in recovering phase or large pixel expansion. In this article, we design a Chinese remainder theorem (CRT)-based two-in-one ISS with three decoding options: lossless recovery, grayscale stacking recovery and visual previewing capability. In the encoding phase, we encode a binary secret image by random grid (RG)-based VSS (RGVSS). Meanwhile, a grayscale secret image is encoded by CRT in the processing of encoding the binary secret image. In the decoding phase, we can decode the binary secret image with two decoding options: grayscale stacking recovery and visual previewing capability. The grayscale secret image can be losslessly decoded with one decoding option through solving a set of linear congruence equations with only modular operation. Furthermore, the shadow image has no pixel expansion. We show our effectiveness by means of theoretical analyses and experiments.

Keywords:
two-in-one image secret sharing, polynomial-based image secret sharing, visual cryptography, Chinese remainder theorem, multiple decryptions

*Corresponding author: Xuehu Yan.
E-Mail: publictiger@126.com .Tel: 86-551-86402861. Fax: 86-551-86402861-861