Threshold changeable secret image sharing using bivariate polynomial

CURRENT STATUS: UNDER REVIEW

EURASIP Journal on Image and Video Processing Springer

Yanxiao Liu
XI'AN University of Technology

liuyanxiao@xaut.edu.cn*Corresponding Author*
ORCiD: https://orcid.org/0000-0002-2507-5143

Ping Wu
XI'AN University of Technology

Qindong Sun
XI'AN University of Technology

Zhili Zhou
Nanjing University of Information Science and Technology

DOI:
10.21203/rs.3.rs-16037/v1

SUBJECT AREAS
Nuclear Medicine & Medical Imaging

KEYWORDS
secret image sharing, threshold changeable, bivariate polynomial

Abstract

In secret image sharing (SIS) scheme, a confidential image is en-crypted into multiple shadows, any group of shadows that reaches the thresh-old, otherwise nothing can be reconstructed at all. Most existing SIS schemes have a fixed threshold, however in this work, we consider more complicat-ed cases that the threshold may be adjusted due to the changeable security environment. In this paper, we construct a (k ↔ h, n) threshold changeable SIS (TCSIS) scheme using bivariate polynomial, which has h − k + 1 possible thresholds k, k + 1, ..., h. During image reconstruction, each participant can update the his shadow according to the current threshold T only based on his initial shadow. Comparing with previous TCSIS schemes, the proposed scheme achieves unconditional security, and can overcome the information disclosure problem caused by homomorphism.

Full Text

Due to technical limitations, full-text HTML conversion of this manuscript could not be completed.

However, the manuscript can be downloaded and accessed as a PDF.

Figures

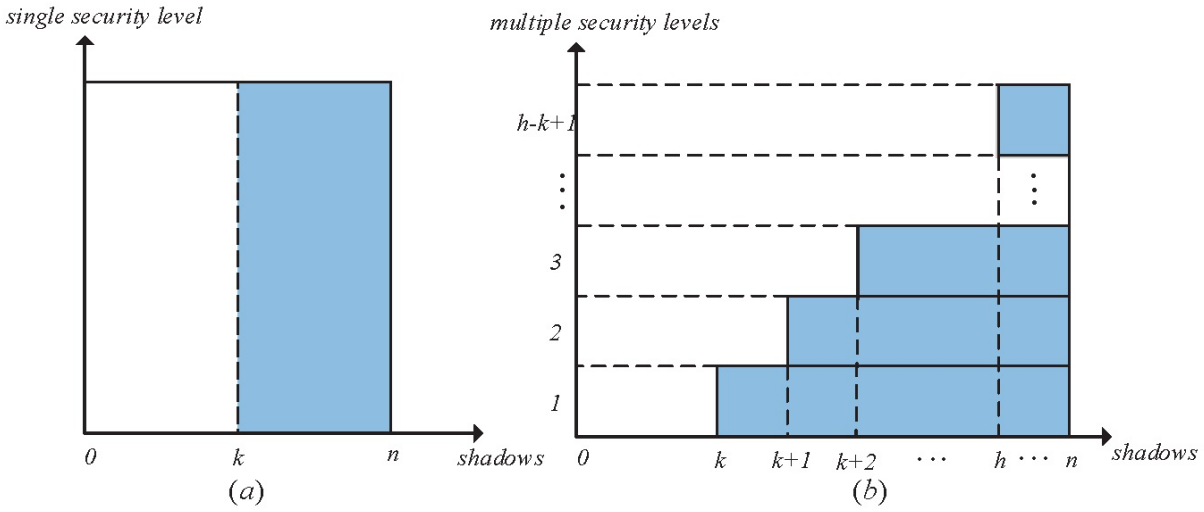

Figure 1

Thresholds for different schemes: (a) (k, n) SIS scheme (b) (k <--> h, n) TCSIS scheme

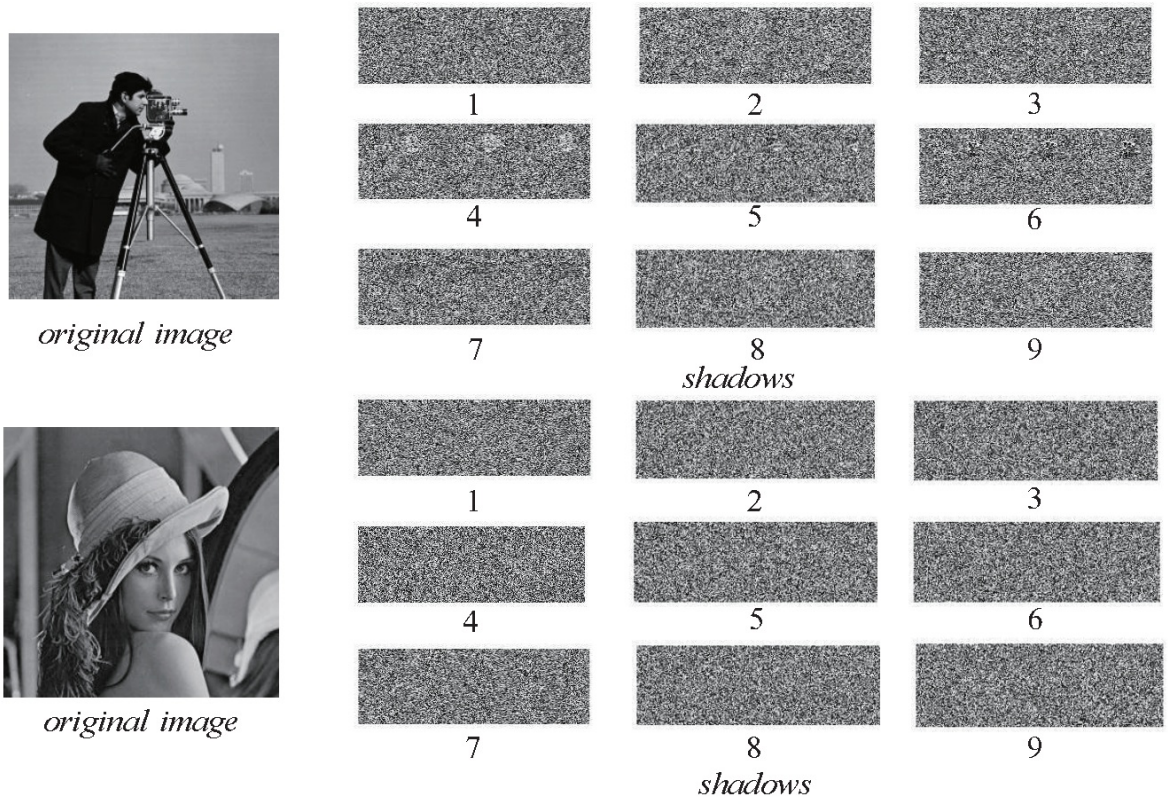

Figure 2

Original images and shadows using proposed scheme

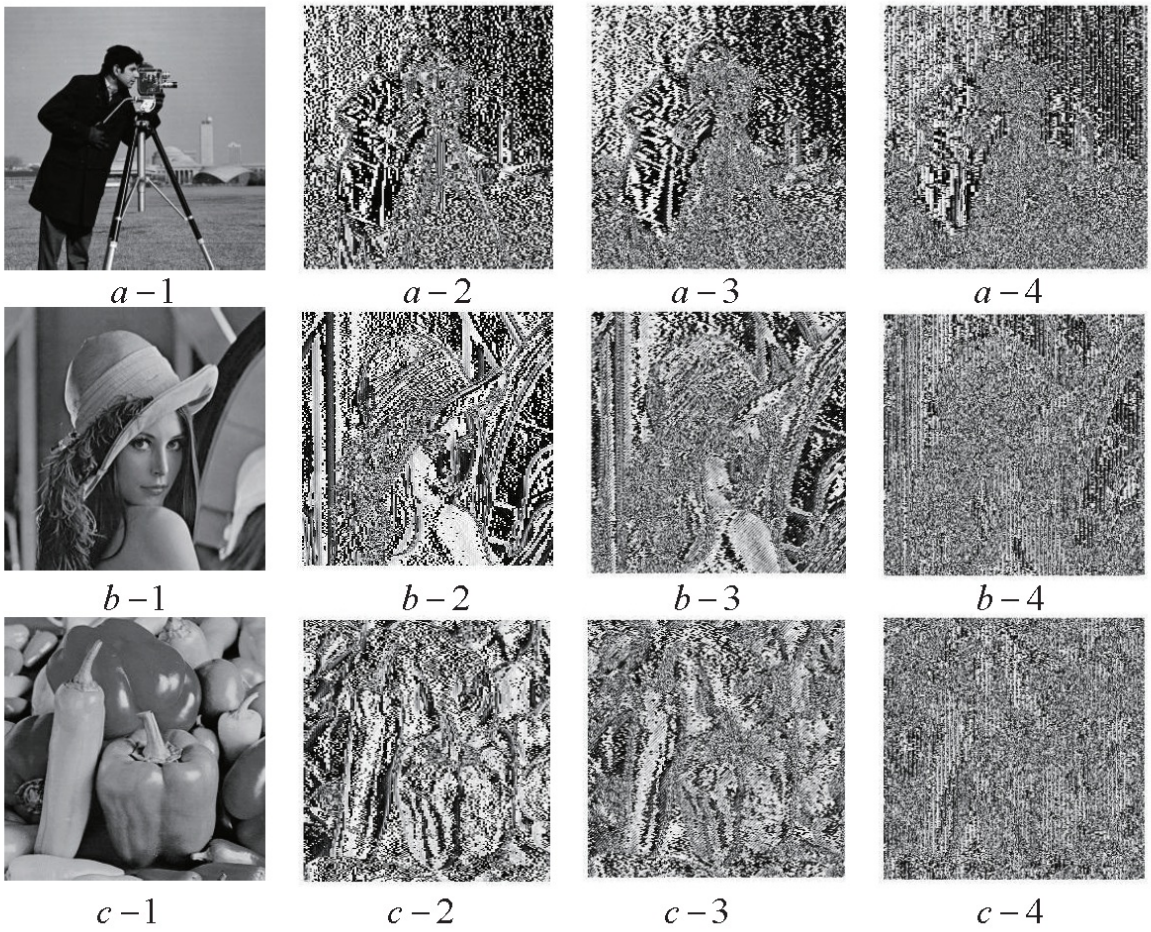

Figure 3

(a-1,b-1,c-1): original images, (a-2,b-2,c-2): quality lossy images with (k′= 2; k = 3), (a-3,b-3,c-3): quality lossy images with (k′= 3; k = 4), (a-4,b-4,c-4): quality lossy images with (k′= 4; k = 5)

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

SI-Liu.tex