Xuehu YAN, Longlong LI, Jia CHEN, Lei SUN, 2023. Public key based bidirectional shadow image authentication without pixel expansion in image secret sharing. *Frontiers of Information Technology & Electronic Engineering*, 24(1):88-103. https://doi.org/10.1631/FITEE.2200118

Public key based bidirectional shadow image authentication without pixel expansion in image secret sharing

Key words: Image secret sharing; Shadow image authentication; Public key; Pixel expansion; Lossless decoding

Xuehu YAN
E-mail: publictiger@126.com
ORCID: https://orcid.org/0000-0001-6388-1720

Motivation

1. Image secret sharing (ISS) is gaining popularity due to the importance of digital images and its wide application to cloud-based distributed storage and multiparty secure computing. Shadow image authentication generally includes shadow image detection and identification, and plays an important role in ISS.

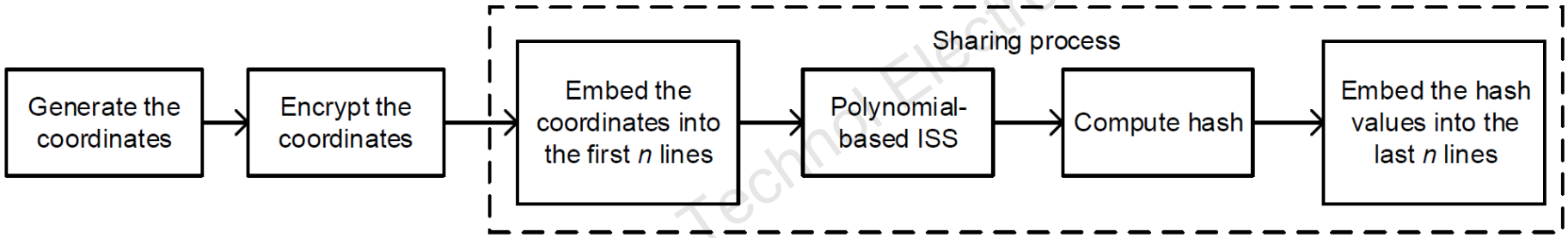
2. However, traditional dealer-participatory methods, which suffer from significant pixel expansion or storing auxiliary information, authenticate the shadow image mainly during the decoding phase, also known as unidirectional authentication. The authentication of the shadow image in the distributing (encoding) phase is also important for the participant.

Main idea

1. We introduce a public key based bidirectional shadow image authentication method in ISS without pixel expansion for a (*k*, *n*) threshold.

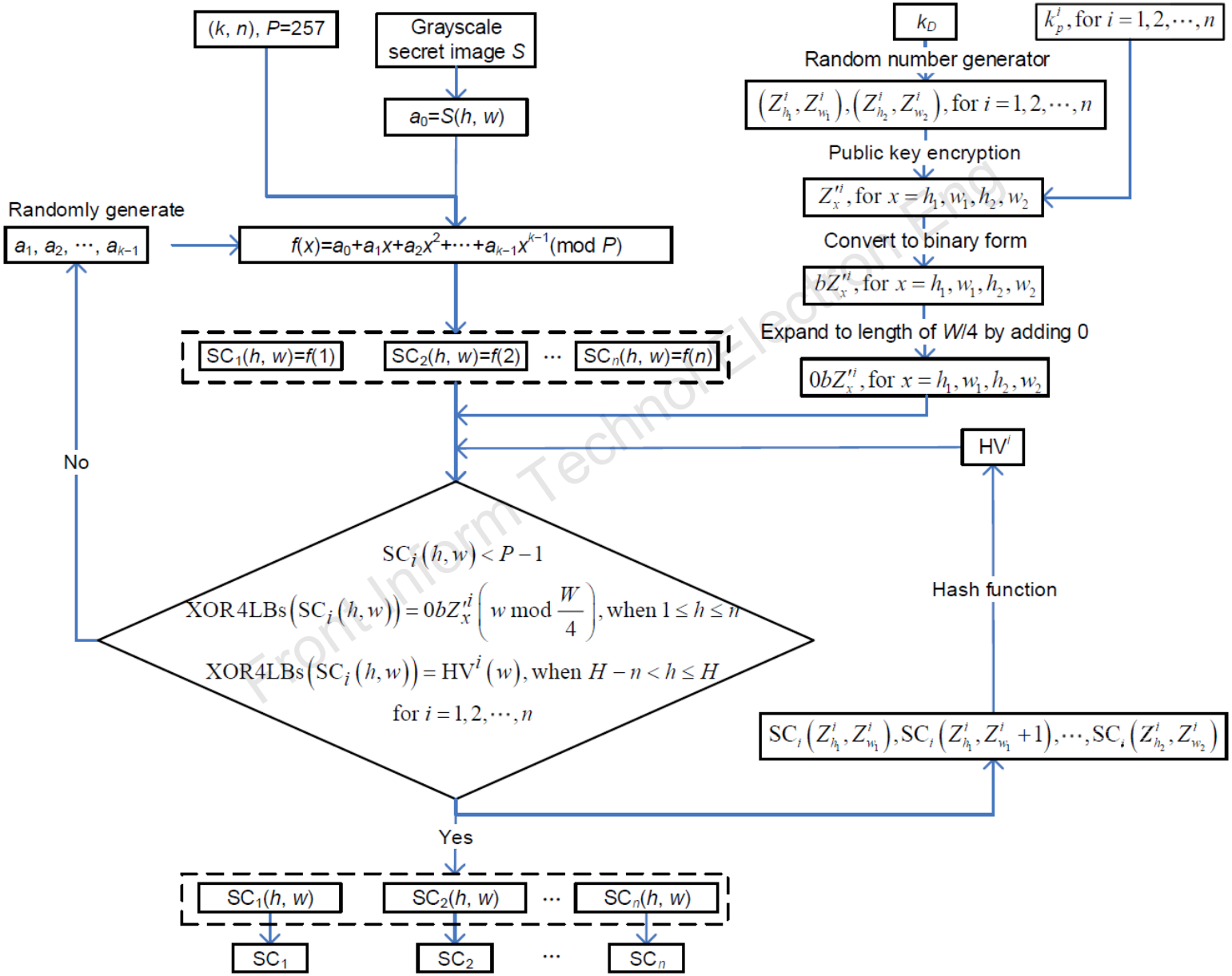
2. When the dealer distributes each shadow image to a corresponding participant, the participant can authenticate the received shadow image with his/her private key. In the decoding phase, the dealer can authenticate each received shadow image with a secret key; in addition, the dealer can losslessly decode the secret image with any *k* or more shadow images.

Framework



Framework of the proposed public key based bidirectional shadow image authentication method

Design concept

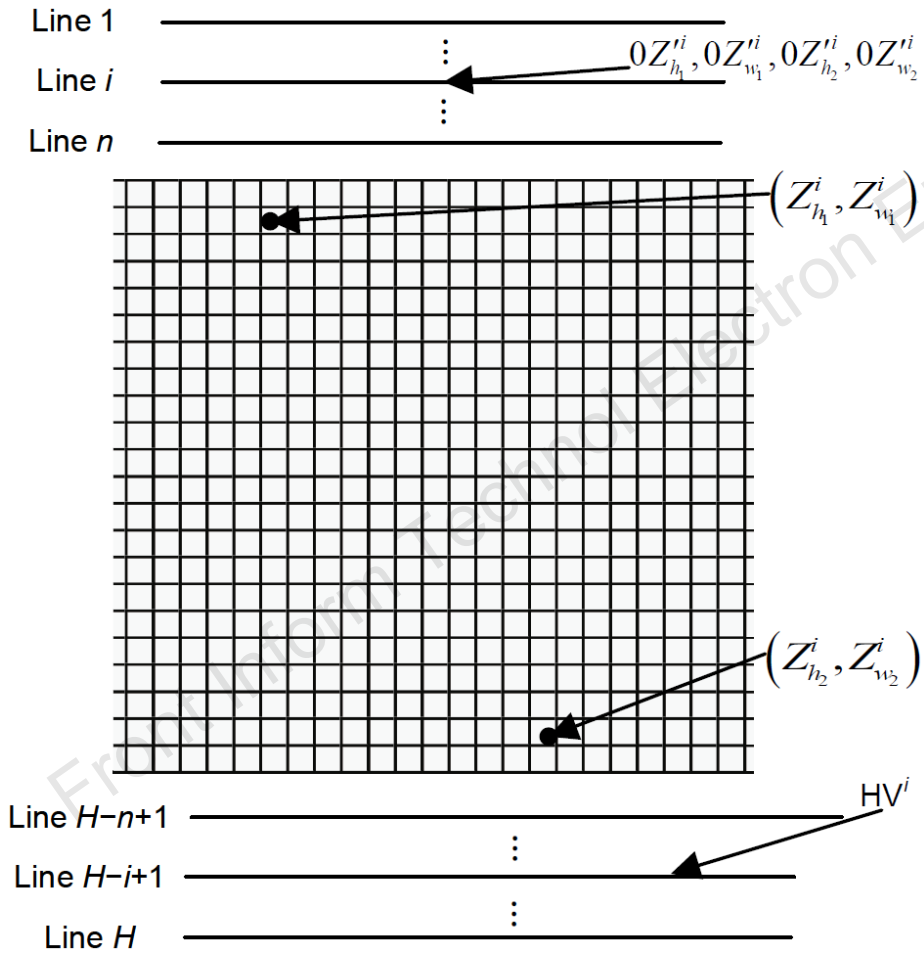


Method

1. The dealer generates the coordinates using his/her secret key, so that he/she knows the concentrated positions to be hashed to authenticate the shadow image when receiving each shadow image during the decoding phase. The dealer encrypts the coordinates using each participant's public key, so that the true participant with the private key can authenticate the shadow image when receiving each shadow image during the shadow image distribution phase.

2. The dealer embeds the encrypted coordinates and hash values into the first *n* and last *n* lines of each shadow image to avoid storing auxiliary information. In this way, no pixel expansion can be achieved.

Method



Information embedding and processing order for the i^{th} shadow image

Major results

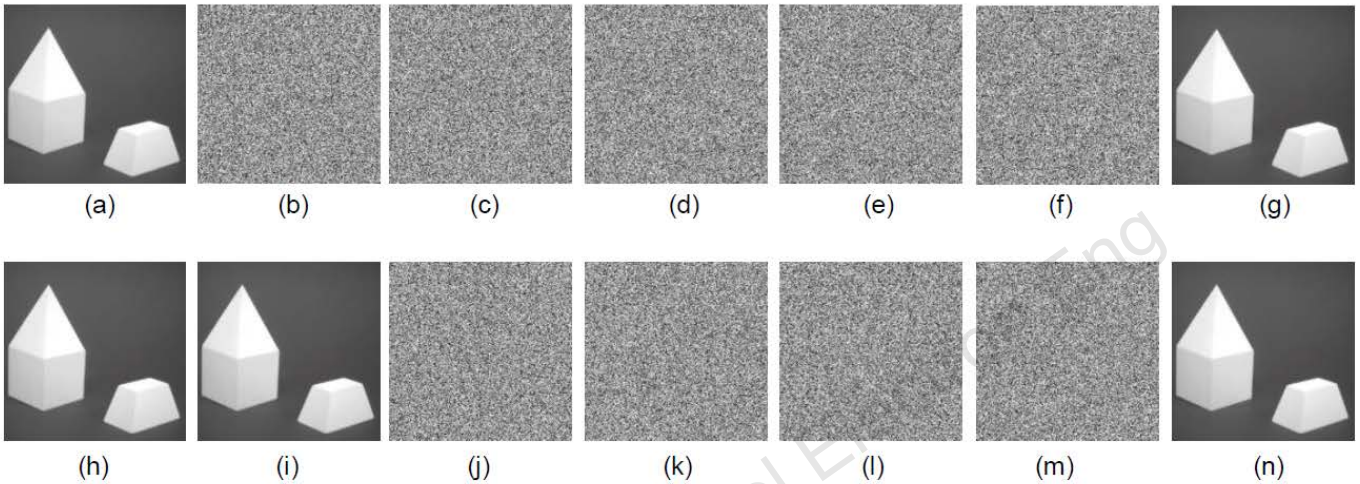


Fig. 9 More experimental results of the proposed (k, n) threshold ISS scheme with bidirectional shadow image authentication without pixel expansion, where $k = 3$ and $n = 4$: (a) grayscale secret image S; (b–e) grayscale shadow images SC_1, SC_2, SC_3, and SC_4; (f–i) grayscale secret image S' decoded with two or more shadow images; (j) fake shadow image SC'_1; (k–n) grayscale secret image S' decoded with SC'_1 and the other one or more shadow images

Table 3 Feature comparisons with related methods

Feature	Description				
	Liu YJ and Chang (2018)	Liu YX et al. (2018b)	Yan et al. (2020a)	Jiang et al. (2020)	Our method
(k, n)-threshold	Yes	Yes	Yes	Yes	Yes
No pixel expansion	No	Yes	Yes	Yes	Yes
Lossless decoding	High quality	High quality	Yes	Yes	Yes
Key idea	Information hiding	Polynomial	ISS	ISS	ISS and hash
Authentication in the distributing phase	No	No	No	No	Yes
Authentication in the decoding phase	Yes	Yes	Yes	Yes	Yes
Authentication ability	Requiring one shadow image	Requiring k shadow images	Requiring one shadow image	Requiring one shadow image	Requiring one shadow image

Conclusions

1. The main contribution of this study is the introduction of an image secret sharing (ISS) scheme with bidirectional shadow image authentication with no pixel expansion, lossless decoding, or auxiliary information. The public key system and hash function were first introduced into ISS to achieve admirable bidirectional shadow image authentication without pixel expansion or additional information, except for the secret key of the dealer and the public/private keys of participants.

2. Theoretical analyses and experimental examples demonstrated the effectiveness of our method. The proposed ISS can losslessly decode secret images with bidirectional shadow image authentication without pixel expansion.