Ziyi ZHOU, Chengyue WANG, Kexun YAN, Hui SHI, Xin PANG, 2024. Reversible data hiding in encrypted images based on additive secret sharing and additive joint coding using an intelligent predictor. *Frontiers of Information Technology & Electronic Engineering*, 25(9):1250-1265. https://doi.org/10.1631/FITEE.2300750

Reversible data hiding in encrypted images based on additive secret sharing and additive joint coding using an intelligent predictor

Front Inform Technol Electron Eng

Key words: Reversible data hiding in encrypted images (RDHEI); Additive secret sharing; Adaptive joint coding; Intelligent predictor

Corresponding author: Hui SHI
E-mail: shihui_jiayou@lnnu.edu.cn
ORCID: https://orcid.org/0000- 0001-5029-7461

Motivation

To bolster security without significant computational cost, we propose to combine additive secret sharing encryption with pixel prediction and compression techniques. Our method integrates an intelligent predictor based on a ResNet architecture, enhancing embedding capacity by improving the accuracy. Leveraging neural network capabilities allows for precise pixel correlation anticipation, reducing prediction errors and optimizing embedding space utilization. Additionally, three-dimensional (3D) chaotic mapping and multi-layer randomness strengthen additive secret sharing, enhancing security and resilience against advanced attacks. Our adaptive joint encoding improves embedding rates and mitigates risks associated with pixel modifications at specified coordinates.

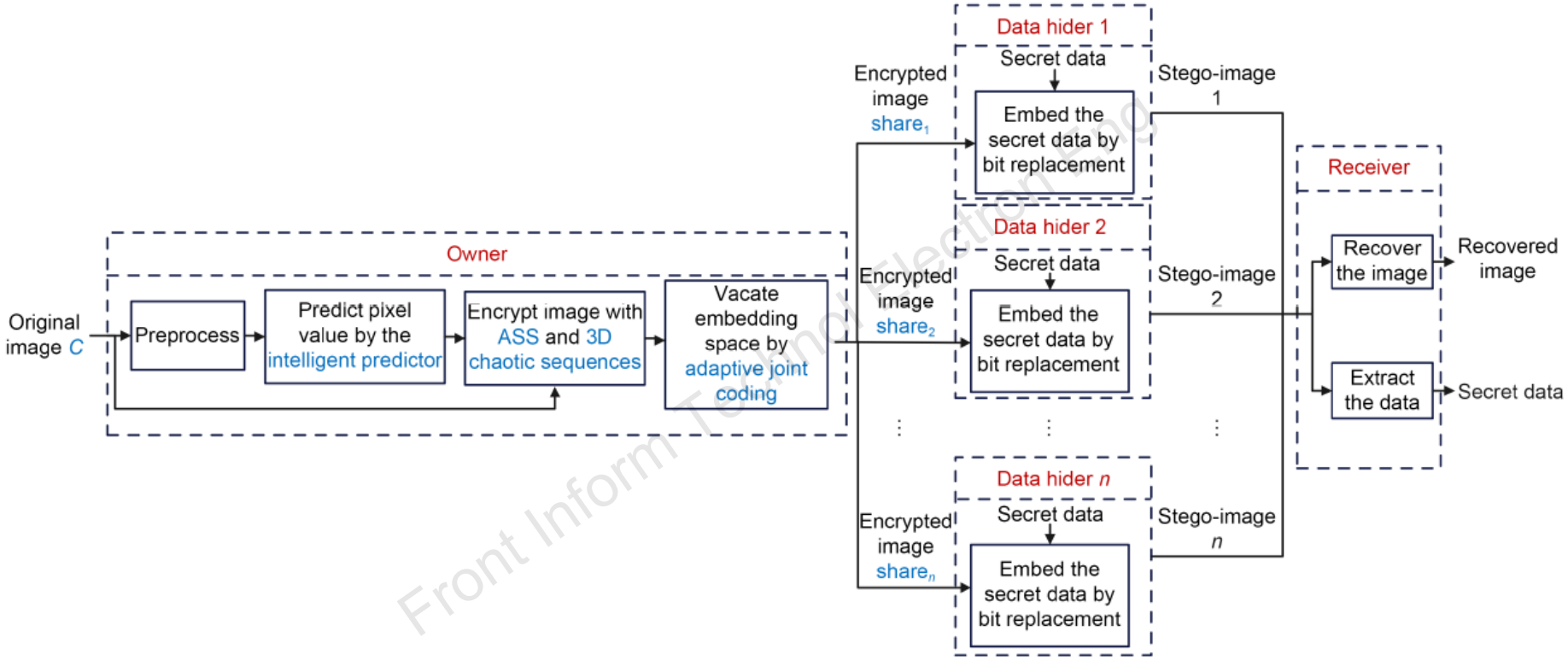
Front Inform Technol Electron Eng

Main idea

We propose an intelligent pixel predictor based on a residual group block and a spatial attention module, showing superior pixel prediction performance compared to existing predictors. Additionally, we introduce an adaptive joint coding method that leverages bit-plane characteristics and intra-block pixel correlations to maximize embedding space, outperforming single coding approaches. The image owner employs the presented intelligent predictor to forecast the original image, followed by encryption through additive secret sharing before conveying the encrypted image to data hiders. Subsequently, data hiders encrypt secret data and embed them within the encrypted image before transmitting the image to the receiver. The receiver can extract secret data and recover the original image losslessly, with the processes of data extraction and image recovery being separable. Our innovative approach combines an intelligent predictor with additive secret sharing, achieving reversible data embedding and extraction while ensuring security and lossless recovery. Experimental results demonstrate that the predictor performs well and has a substantial embedding capacity. For the Lena image, the number of prediction errors within the range of [−5, 5] is as high as 242 500 and our predictor achieves an embedding capacity of 4.39 bpp.

Front Inform Technol Electron Eng

Framework



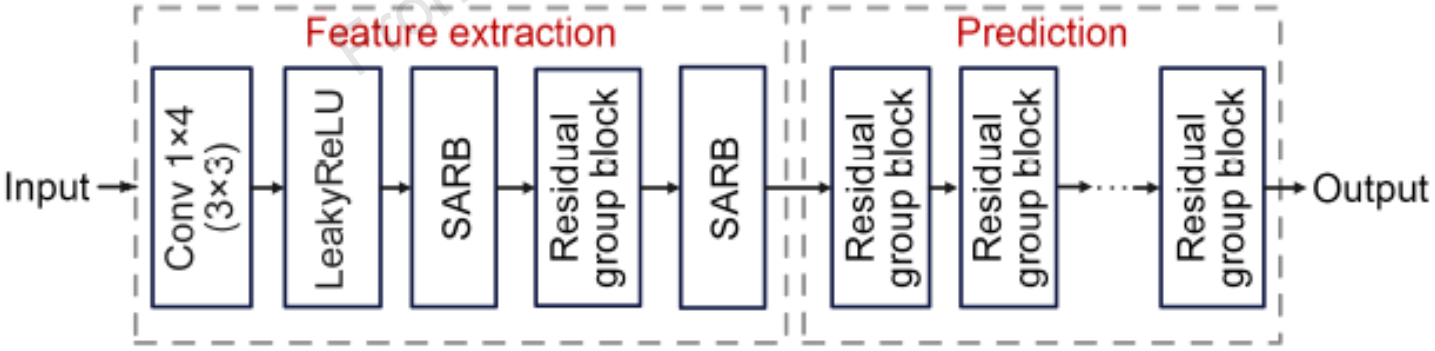
An overview of the proposed reversible data hiding in encrypted images

Method

To predict pixel values, we construct an intelligent predictor based on a residual group block and a spatial attention module (SAM). The formula for the proposed intelligent predictor is $P_r=F(C_\eta, \psi)$.

The architecture of the proposed intelligent predictor is depicted. The predictor consists of 53 convolutional layers and four modules: input module, feature extraction module, prediction module, and output module.

Front Inform Technol Electron Eng



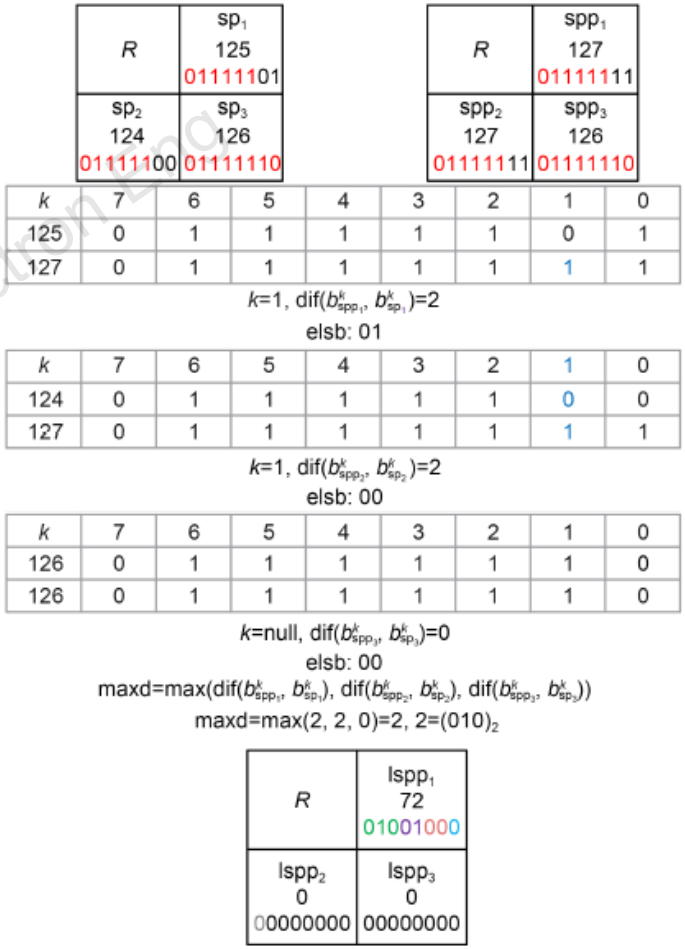
Method

For compressing the cover image to vacate embedding space, we propose an adaptive joint coding method. When maxe$\leqslant\tau$&&(3+3$\times$maxd)>T, the encoding method based on the prediction error is used, where maxe represents the maximum prediction error within a block, τ represents the threshold for pixel values, maxd represents the highest differing bit in bit-plane comparison, and T represents the threshold for the prediction error. When (maxe$\leqslant\tau$&&(3+3$\times$maxd)$\leqslant T$)|| (maxd$\leqslant\tau$&&maxe>τ), the encoding method based on bit-plane comparison is used.

Front Inform Technol Electron Eng

Method

Maxd is represented using a three-bit binary value, and the least significant bit-planes (LSBs) of sp_1, sp_2, sp_3 and the error bit-planes “elsb” are extracted. The three-bit binary representation of maxd and the maxd LSBs of sp_1, sp_2, sp_3 are sequentially replaced by sp_1, sp_2, sp_3. Let sp_1, sp_2, sp_3 be 125, 124, 126, and spp_1, spp_2, spp_3 be 127, 127, 126, respectively. maxd=max(2, 2, 0)=2, and then maxd is converted to its three-bit binary representation as “010,” which serves as the first three bits of the label. LSBs of the original pixel values sp_1, sp_2, sp_3 are recorded as “elsb,” resulting in 01, 00, 00, respectively. The label and elsb are stored, while the remaining bit-planes are set to 0. Thus, the compressed pixel values using bit-plane comparison based coding are $lspp_1$ 72, $lspp_2$ 0, and $lspp_3$ 0.



Front Inform Technol Electron Eng

Method

Prediction error based encoding represents prediction errors using four-bit binary codes. Illustrates an example using numerical values, where sp_1, sp_2, sp_3 are taken as 126, 129, 128, and spp_1, spp_2, spp_3 are taken as 127, 127, 127, respectively. $e_1=127-126=1$, $e_2=127-129=-2$, $e_3=127-128=-1$. These values $|\ e_\varphi\ |$ are converted into a three-bit binary representation, resulting in 001, 010, and 001. When combined with the sign codes, we obtain 0001, 1010, and 1001. The four LSBs of each pixel are then set to 0, creating space. The compressed pixel values based on the prediction error encoding are thus obtained as $pspp_1$ 16, $pspp_2$ 160, $pspp_3$ 144.

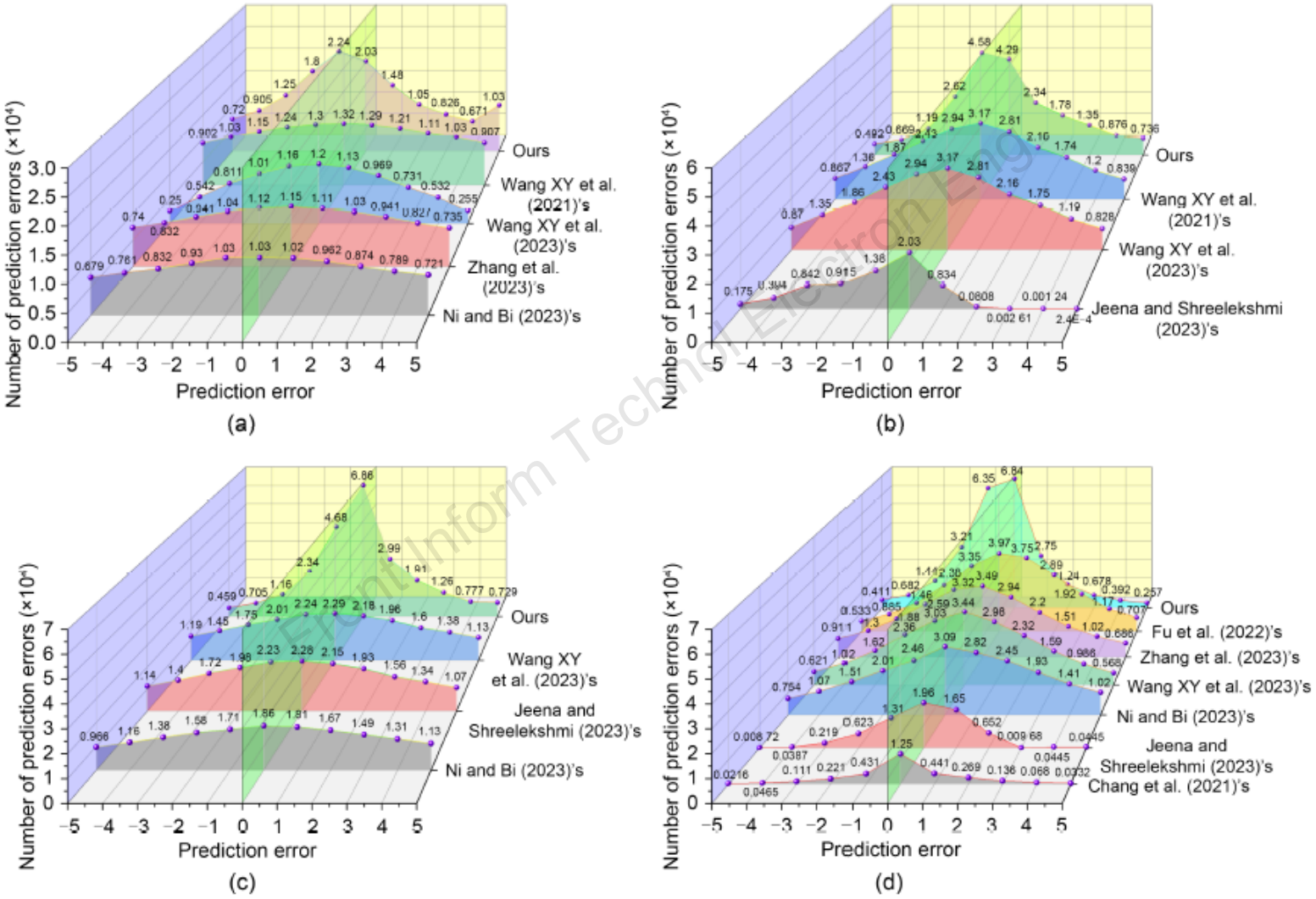
R	sp_1 126 01111110	R	spp_1 127 01111111
sp_2 129 10000001	sp_3 128 10000000	spp_2 127 01111111	spp_3 127 01111111

sp_φ	126	129	128
spp_φ	127	127	127
$e_\varphi=spp_\varphi-sp_\varphi$	1	−2	−1
Codeword	0001	1010	1001

R	$pspp_1$ 16 00010000
$pspp_2$ 160 10100000	$pspp_3$ 144 10010000

Front Inform Technol Electron Eng

Results



Front Inform Technol Electron Eng

Fig. 13 Comparison of the number of prediction errors within the range of [−5, 5] with advanced methods: (a) Baboon; (b) Barbara; (c) Boat; (d) Lena

Results

Table 1 Comparison of the number of zero prediction errors between the model without SARB and the proposed intelligent predictor

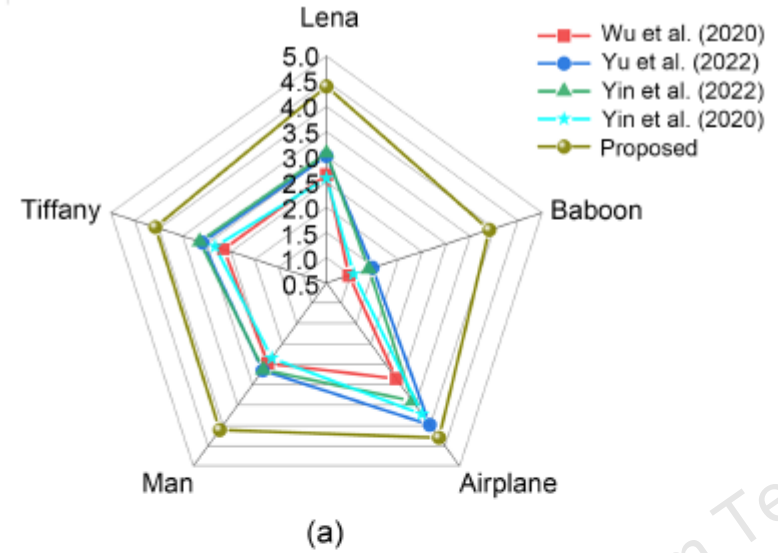
Image	Number of zero prediction errors	
	The predictor without SARB	The proposed intelligent predictor
Airplane	33 585	38 437
Baboon	13 863	20 259
Barbara	29 471	42 941
Boat	33 296	68 561
Jetplane	17 955	21 760
Lena	33 283	68 416
Pepper	34 929	53 339
Man	15 317	26 139
Tiffany	21 576	25 216

Table 3 Embedding capacity (EC) and embedding rate (ER) of the proposed method on nine test images

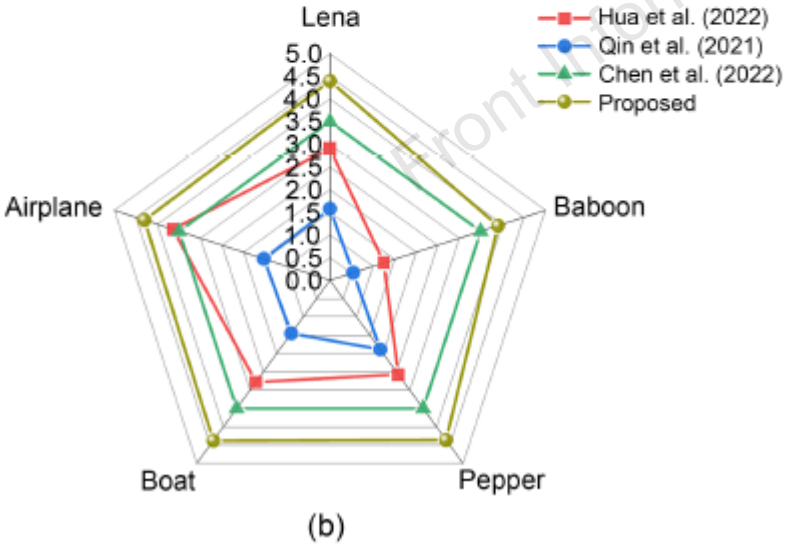
Image	ER (bpp)	EC (bit)
Airplane	4.2895	1 124 478
Baboon	3.9018	1 022 855
Barbara	4.2113	1 103 989
Boat	4.3770	1 147 408
Jetplane	4.3025	1 127 899
Lena	4.3966	1 152 545
Pepper	4.3601	1 142 979
Man	4.1089	1 077 132
Tiffany	4.0743	1 068 063

Front Inform Technol Electron Eng

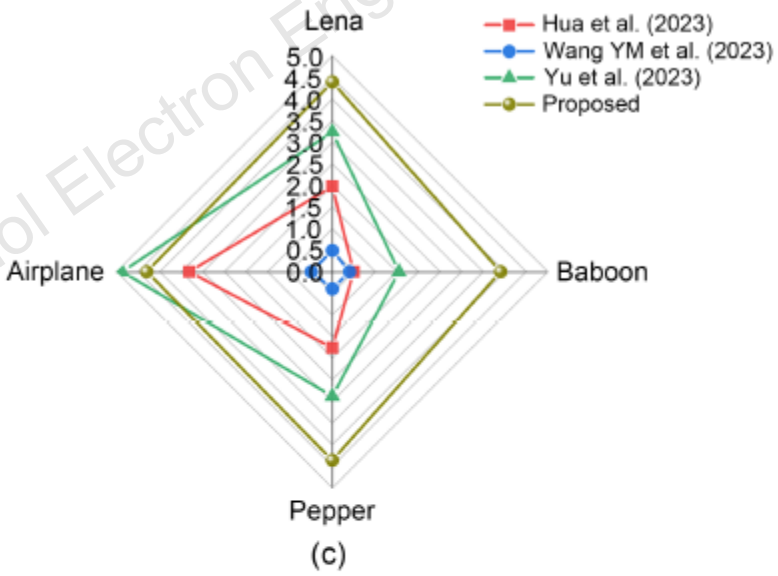
Results



(a)



(b)



(c)

Front Inform Technol Electron Eng

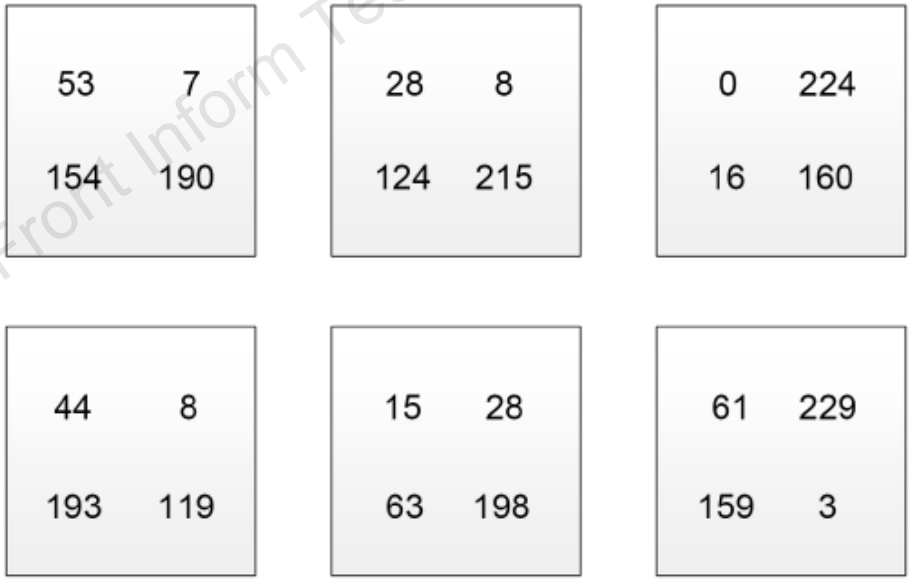
Fig. 14 Comparison of capacity with similar schemes: (a) comparison with methods (Wu et al., 2020; Yin et al., 2020, 2022; Yu et al., 2022) on Lena, Baboon, Airplane, Man, and Tiffany; (b) comparison with methods (Qin et al., 2021; Chen et al., 2022; Hua et al., 2022) on Lena, Baboon, Pepper, Boat, and Airplane; (c) comparison with methods (Hua et al., 2023; Wang YM et al., 2023; Yu et al., 2023) on Lena, Baboon, Pepper, and Airplane

Results

In the experimental results, we encrypted Lena twice using two sets of random keys. By examining the pixel values at the same position in these two sets of encrypted images, we can observe significant differences.

It is evident that the pixel values at the same position obtained from two encrypted images are entirely different. This encryption system, characterized by uncertainty and randomness, is capable of effectively resisting numerous potential attacks.

Front Inform Technol Electron Eng



Conclusions

We introduce a novel approach for reversible data hiding in encrypted data, combining intelligent prediction and additive secret sharing. Our method comprises key components: training an intelligent predictor, encrypted predictions, additive encryption, and joint encoding for embedding. It offers efficient hiding, adaptive encoding, and lossless recovery. The method possesses several notable advantages: first, it significantly enhances the efficiency of information concealment by employing an intelligent predictor; second, the utilization of additive secret sharing mechanism ensures robust encryption, achieving a good balance between security and efficiency; third, the application of adaptive joint encoding technology maximizes the capacity of hidden information; last, thanks to accurate prediction mechanisms, the method ensures lossless recovery of the original information even in the case of lost shares. Our method represents a significant advancement in reversible data hiding in encrypted data. Future enhancements aim to refine and extend its capabilities, ensuring relevance and impact in the field.

Front Inform Technol Electron Eng

Ziyi ZHOU holds a master's degree from Liaoning Normal University. Her research interests include cryptography and information security.

Hui SHI received her PhD degree from Dalian University of Technology and is currently an associate professor at Liaoning Normal University. Her research interests include artificial intelligence security and cryptography.

Front Inform Technol Electron Eng

Xin PANG is a teacher at Liaoning Normal University. His research interests include artificial intelligence security and cryptography.