Xiuli CHAI, Xiuhui CHEN, Yakun MA, Fang ZUO, Zhihua GAN, Yushu ZHANG, 2023. TPE-H2MWD: an exact thumbnail preserving encryption scheme with hidden Markov model and weighted diffusion. *Frontiers of Information Technology & Electronic Engineering,* 24(8):1169-1180.
https://doi.org/10.1631/FITEE.2200498

TPE-H2MWD: an exact thumbnail preserving encryption scheme with hidden Markov model and weighted diffusion

Key words: Hidden Markov model; Weighted diffusion; Balance between usability and privacy; Image encryption

Corresponding authors: Fang ZUO; Zhihua GAN
E-mail: zuofang@henu.edu.cn; gzh@henu.edu.cn
ORCID: https://orcid.org/0000-0001-5673-8870;
https://orcid.org/0000-0002-2372-2853

Motivation

1. With the substantial increase in image transmission, the demand for image security is increasing. Noise-like images can be obtained by conventional encryption schemes, and although the security of the images can be guaranteed, the noise-like images cannot be directly previewed and retrieved.

2. Based on the rank-then-encipher method, some researchers have designed a three-pixel exact thumbnail preserving encryption (TPE2) scheme, which can be applied to balance the security and availability of images, but this scheme has low encryption efficiency.

Main idea

1. The TPE-H2MWD encryption process takes the entire block as a unit while changing the position and value of the pixels and keeping the sum of the pixels constant.

2. In the scrambling phase, the zigzag models are applied in the lower four bit planes, and the hidden Markov model is used in the higher four bit planes.

3. In the diffusion phase, the sum of the pixel values is kept constant by using weighted diffusion.

Method

1. A new exact TPE-H2MWD is presented. Bit-level permutation and diffusion methods are used to realize the exact TPE directly, which improves the encryption efficiency.

2. A bit-level permutation method based on the hidden Markov model is presented, improving the security of the encryption scheme.

3. A weighted diffusion method is introduced under the condition that the sum of pixels is unchanged, which prevents the leakage of bit statistical information.

Major results

1. Analysis of the encryption effect

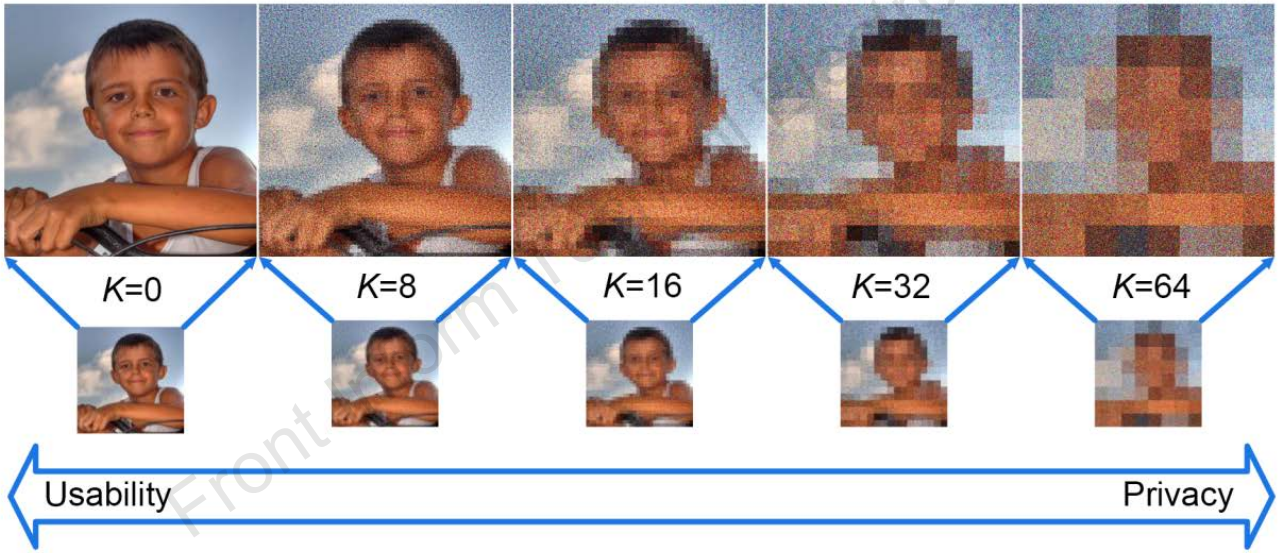


Fig. 7 TPE-H2MWD encrypted images with different block sizes (original, 8×8, 16×16, 32×32, and 64×64) and corresponding preserved thumbnails

Major results

2. Ciphertext image perception quality

Table 1 Peak signal-to-noise ratio (PSNR) values between 500 plaintext and encrypted image thumbnails

Algorithm	PSNR (dB)		
	8×8	16×16	32×32
TPE-LSB (1-bit) (Marohn et al., 2017)	20.045	20.532	21.347
TPE-LSB (2-bit)	29.545	30.393	31.889
TPE-LSB (3-bit)	39.145	40.675	43.327
TPE2 (Zhao et al., 2021)	+∞	+∞	+∞
TPE-H2MWD	+∞	+∞	+∞

Major results

3. Adjacent pixel correlation analysis

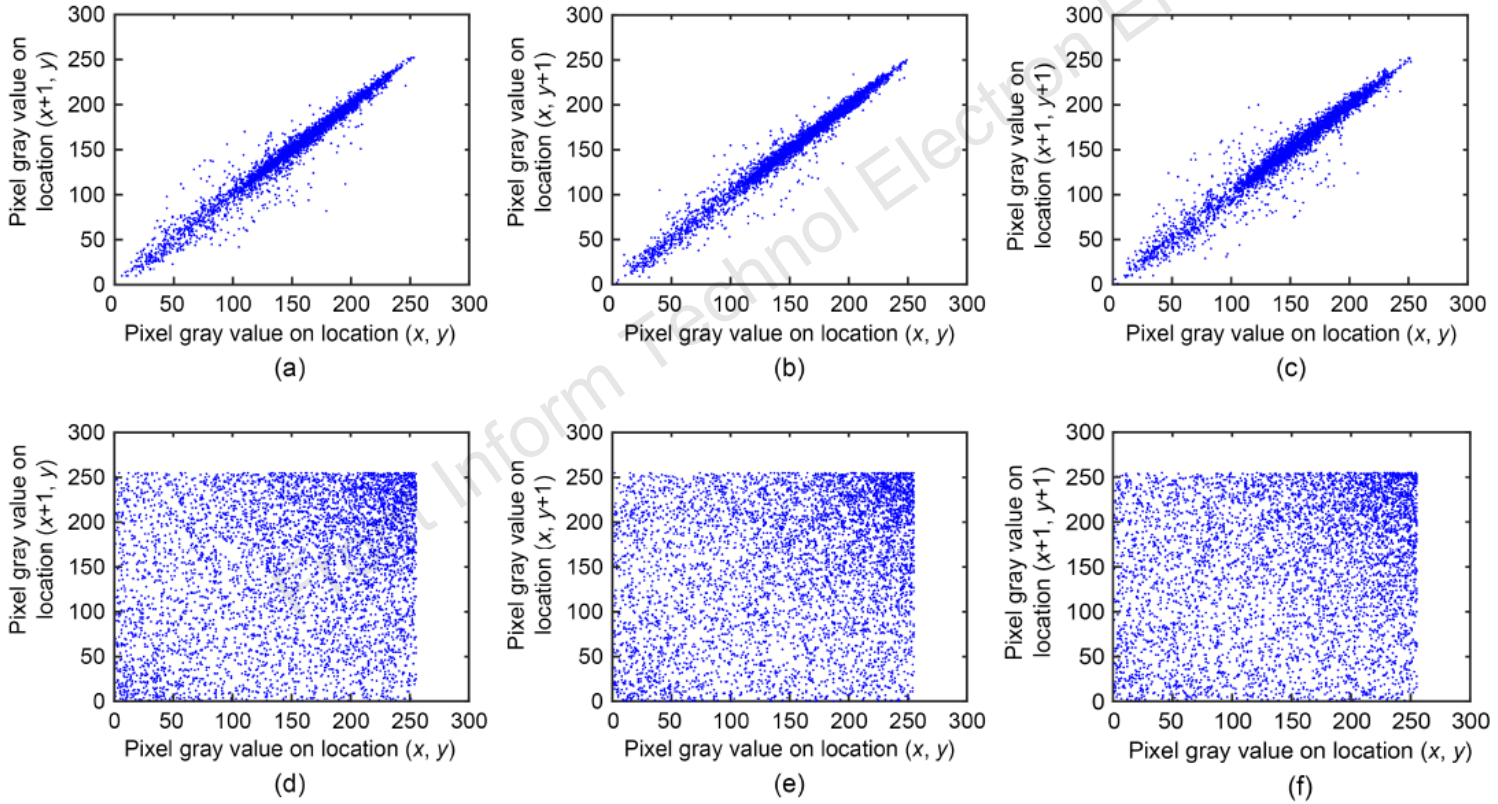


Fig. 9 Correlation analysis of the R channel in the image: (a)–(c) are the results of correlation of plaintext image in the horizontal, vertical, and diagonal directions, respectively; (d)–(f) are the results of correlation of encrypted image with K= 32 in the horizontal, vertical, and diagonal directions, respectively

Major results

4. Size expansion rate

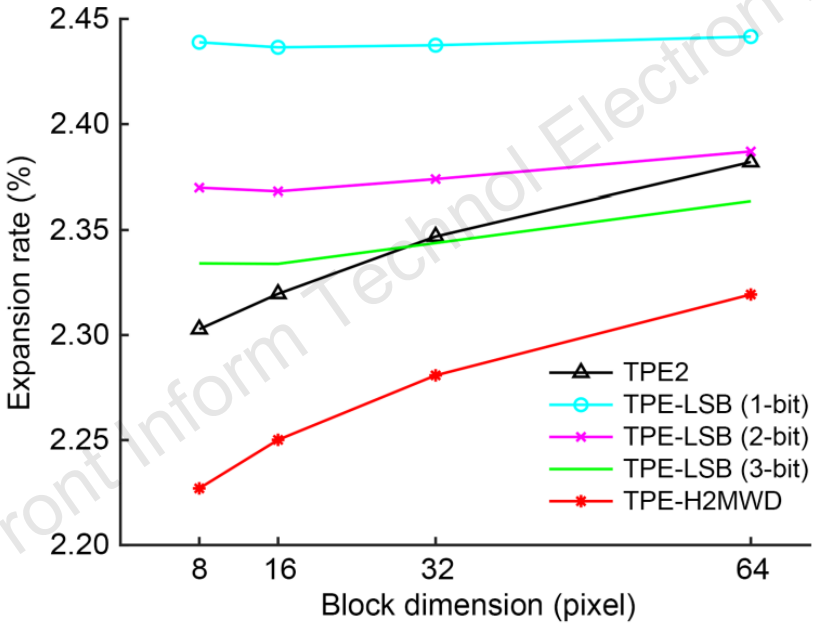


Fig. 11 Average size expansion rate of encrypted images

Conclusions

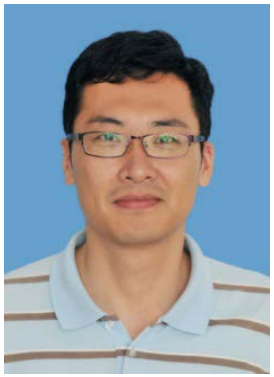
1. In this paper, an exact TPE is implemented with hidden Markov model and weighted diffusion, and the specific encryption process and simulation results are given.

2. TPE-H2MWD can effectively balance the security and availability of images, where illegal users cannot obtain detailed information about the plaintext images from the encrypted images, while image owners can achieve image usability based on the relevant information about the plaintext images retained in the encrypted images.

Xiuli CHAI received her PhD degree from the South China University of Technology, Guangzhou, China, in 2008. She is currently a professor with the School of Artificial Intelligence, Henan University, Zhengzhou, China. Her research interests include information security, multimedia security, and cryptography aspects of chaos.

Xiuhui CHEN received her BE degree from the School of Software Engineering, Anyang Normal University, China, in 2020. She is currently pursuing her ME degree at the School of Artificial Intelligence, Henan University. Her research interests are image encryption and thumbnail preserving encryption.

Yakun MA received his BE degree from the College of Electronics and Information Engineering, Shanghai University of Electric Power, Shanghai, China, in 2019. He is currently pursuing his ME degree with the School of Artificial Intelligence, Henan University.



Fang ZUO received his BS degree in computer science and his MS degree in applied mathematics both from Henan University, Kaifeng, China, and his PhD degree in computer application technology from East China Normal University, Shanghai, China. He is now an associate professor at the School of Software, Henan University. His research interests include P2P networks, distributed multimedia systems, algorithmic game theory, and mathematical optimization theory.

Zhihua GAN received his PhD degree from the School of Computer Science & Technology, Beijing Institute of Technology, Beijing, China, in 2017. He is currently an associate professor with the School of Software, Henan University, Kaifeng, China. His research interests include multimedia security and image processing.

Yushu ZHANG received his PhD degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2014. He is currently a professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include multimedia security, artificial intelligence security, and blockchain.