Xiao-ling HUANG, You-xia DONG, Kai-xin JIAO, Guo-dong YE, 2020. Asymmetric pixel confusion algorithm for images based on RSA and Arnold transform. *Frontiers of Information Technology & Electronic Engineering*, 21(12):1783-1794. https://doi.org/10.1631/FITEE.2000241

Asymmetric pixel confusion algorithm for images based on RSA and Arnold transform

Key words: Rivest-Shamir-Adleman (RSA); Arnold map; Pixel confusion; Asymmetric algorithm; Image confusion

Corresponding author: Guo-dong YE
E-mail: guodongye@hotmail.com
ORCID: https://orcid.org/0000-0003-4222-1824

Motivation

1. Digital images are increasingly integrated into people's lives and play an increasingly important role in communication.

2. Because of the advantages of high security and easy digital signature and verification implementations, asymmetric cryptography algorithms have been extensively researched.

3. The Arnold map cycle can be effectively prolonged by local (sub-block) and global (whole block) confusion.

Main idea

1. Texture features of ultrasound images are critical information, and are often used for computing tasks of kidney ultrasound images.

2. A feature fusion model is designed, which integrates deep features and domain texture features as multi-level description.

3. Transfer learning is used to train the model to reduce the risk of overfitting.

4. The proposed model is assessed by five-fold cross validation.

Method

1. An asymmetric pixel confusion algorithm for images is based on the Rivest-Shamir-Adleman (RSA) public-key cryptosystem and Arnold map.

2. RSA asymmetric algorithm is used to generate two groups of Arnold transform parameters to address the problem of symmetrical distribution of Arnold map parameters.

3. The first group of parameters is used to perform Arnold confusion on each sub-block, while the second group of parameters is used to perform Arnold confusion on the entire image.

Major results

Asymmetric image confusion algorithm

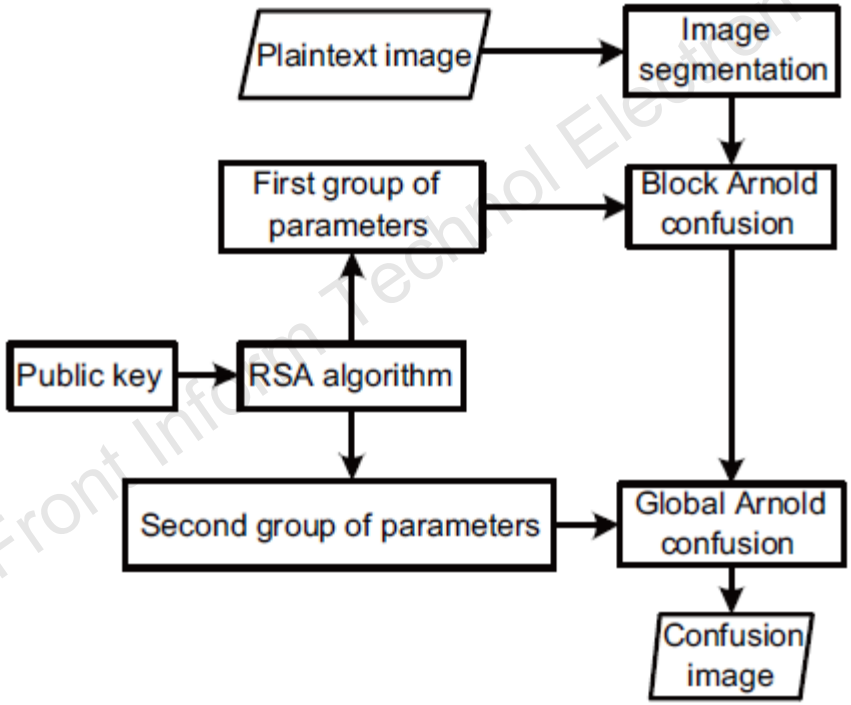

Fig. 2 Asymmetric image confusion algorithm

Major results

Test results of our algorithm

Table 3 Correlation coefficients of different images

Image		Correlation coefficient		
		Horizontal	Vertical	Diagonal
Plaintext image	Boat	0.9372	0.9240	0.8790
	Man	0.9638	0.9336	0.9137
	Baboon	0.9135	0.9323	0.8746
	Peppers	0.9517	0.9447	0.9168
Confusion image	Boat	0.0141	−0.1020	0.0363
	Man	0.0629	0.0191	0.0347
	Baboon	−0.0483	−0.0338	−0.0613
	Peppers	−0.0131	−0.0147	−0.0039

Major results

Test results of our method and the traditional method

Table 5 Transformation period comparison between our method and the traditional method

N	T	
	Our method	Ttraditional method
4	9	3
6	4	12
8	18	6
10	300	30
12	144	12
16	72	12
32	288	24
50	6000	150
64	1152	48
128	4608	96
256	18 432	192
512	73 728	384

Conclusions

The public-key algorithm separates the encryption and decryption keys, reduces the number of keys required for multi-user communication, saves system resources, and facilitates key management. Image confusion is a means to hide information. Considering the security of the confusion algorithm, a new asymmetric image pixel confusion algorithm was proposed based on RSA and the Arnold map. Public and private keys were generated using the RSA algorithm, and then the image's pixels were confused. The Arnold confusion method was used on the image blocks first, and then the entire image was confused to enhance the confusion effect. The experimental results showed that the proposed algorithm is simple to implement and has high confusion degree with test values near to one.

Guo-dong YE, corresponding author of this paper, is a professor at Guangdong Ocean University of China. He received his PhD degree from City University of Hong Kong in 2015. From 2016 to 2018, he was a post-doctor at Zhejiang University. From June 2012 to August 2012, he was a Senior Research Associate at the City University of Hong Kong. His research interests include image encryption, nonlinear dynamics, and image data hiding.

Xiao-ling HUANG is an associate professor at Guangdong Ocean University of China. She received her MS degree from Shantou University in 2008. Her research interests include image encryption and mathematics with its application.