CHONGQING UNIVERSITY

IEEE ICASSP 2022

Applying deep learning to known-plaintext attack on chaotic image encryption schemes

Fusen Wang*, Jun Sang*, Chunlin Huang*, Bin Cai*, Hong Xiang* and Nong Sang†

*Key Laboratory of Dependable Service Computing in Cyber Physical Society
of Ministry of Education, Chongqing University, Chongqing, China
†School of Artificial Intelligence and Automation, Huazhong University
of Science and Technology, Wuhan, China

Outline

1. Introduction
2. Traditional Known plaintext attack
3. Proposed Approach
4. Implementation Details
5. Experiment
6. Conclusion

1. Introduction

The known plaintext attack, as one cryptanalysis method, is crucial to evaluate the security of image encryption.

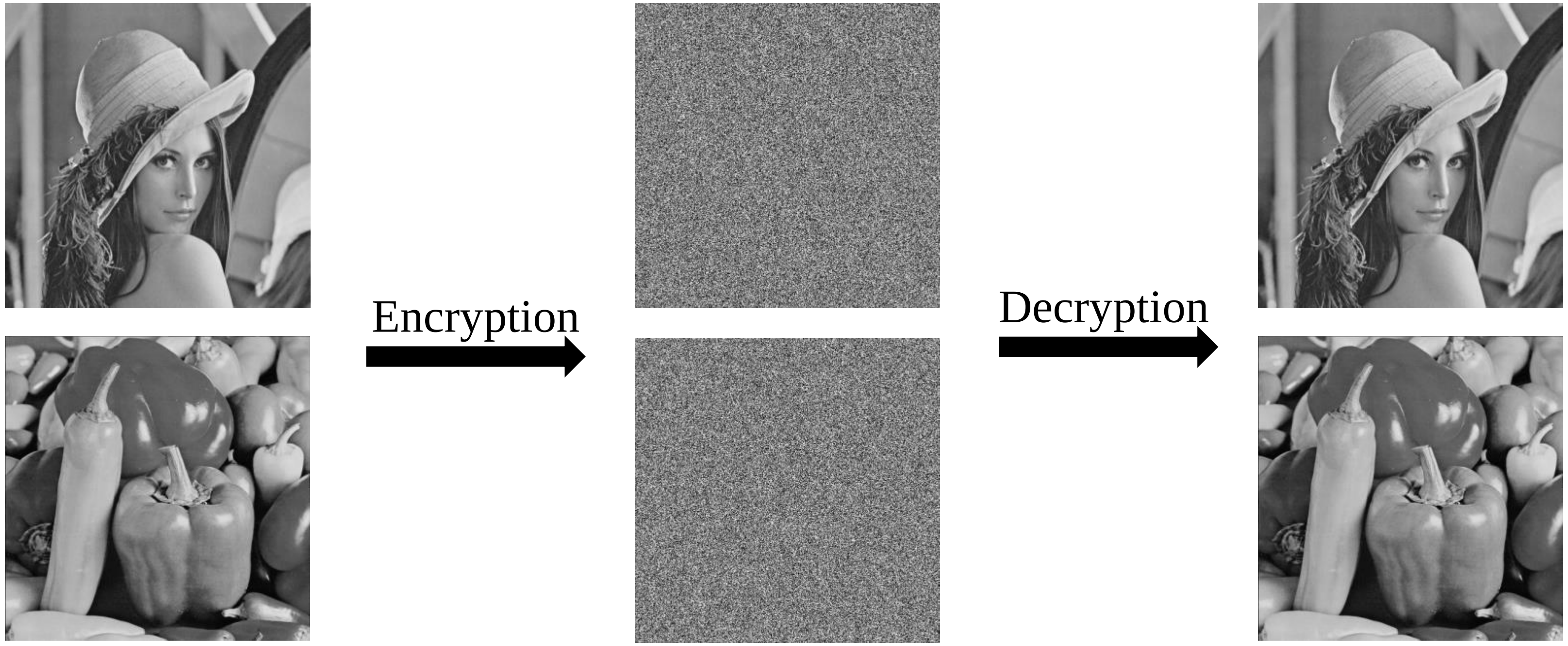


Fig. 1 Some “plaintext-ciphertext” image pairs.

2. Traditional Known plaintext attack

The traditional known plaintext attack works are usually based on some mathematical means, such as differential attack. It has some shortcomings:

- It is complicated to design an attack scheme.
- Usually, one attack method is only designed for a specific chaotic encryption system, which is hard to be applied to other chaotic encryption systems.

3. Proposed Approach

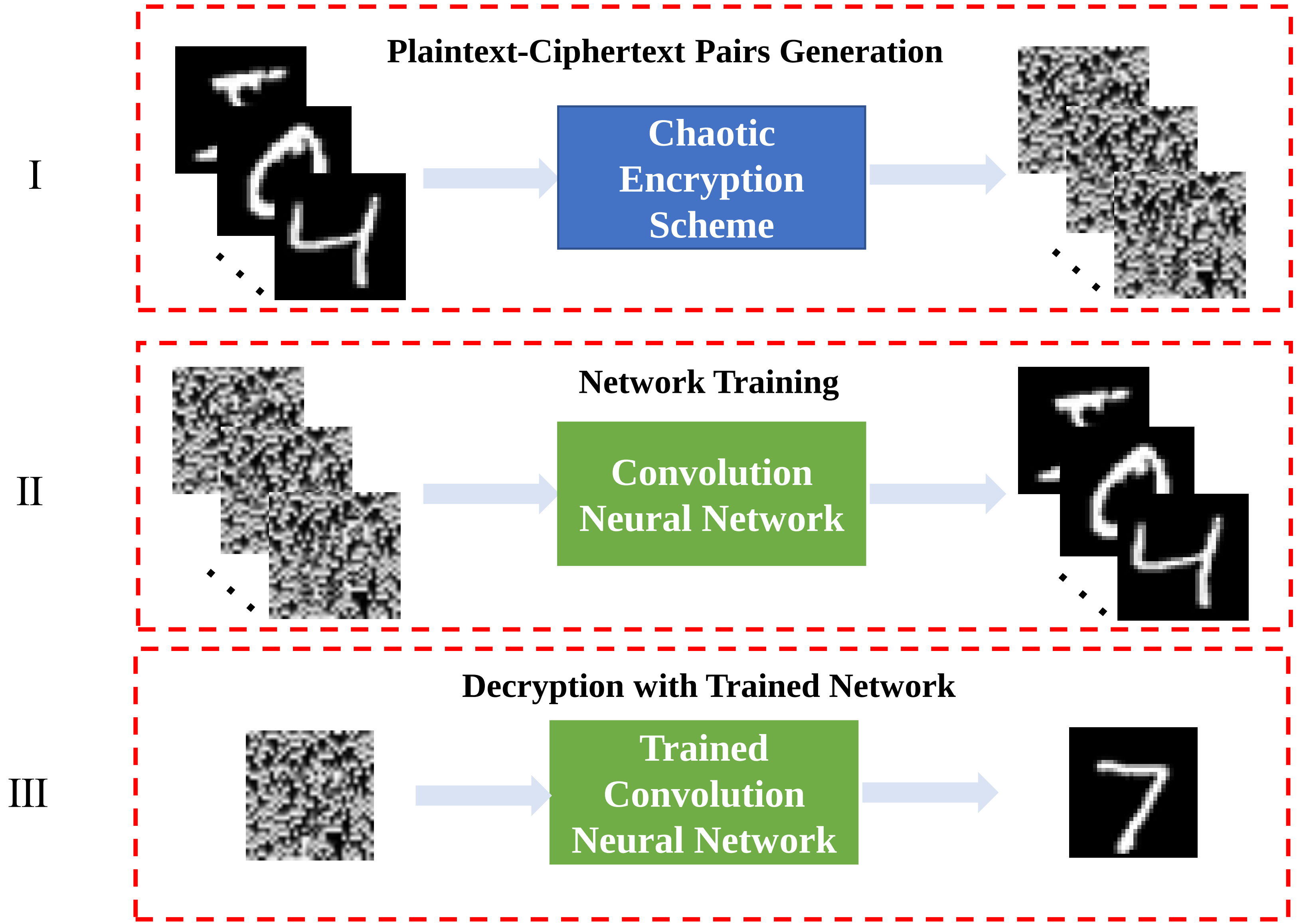


Fig. 2 The overall framework of deep learning-based known-plaintext attack on chaotic cryptosystem.

Advantages

The advantages of the proposed deep learning-based known-plaintext attack method:

- It is easy to design a convolution neural network for the known plaintext attack.
- Different from the traditional known-plaintext attack methods for chaotic cryptosystems, a convolutional neural network can be employed to decrypt different chaotic cryptosystems.

Network architecture

IEEE ICASSP 2022

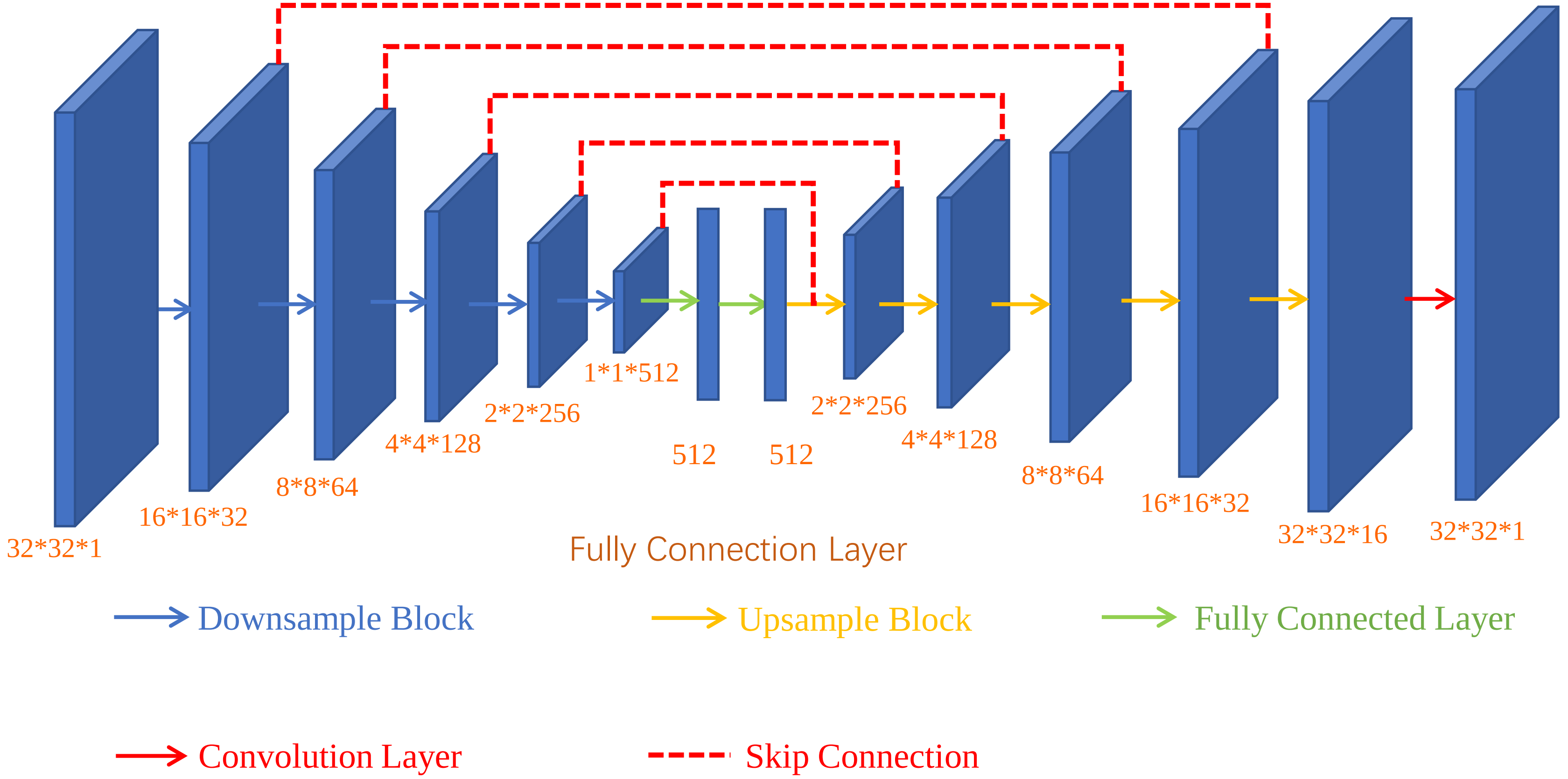


Fig. 3 The architecture of the proposed image decryption encoder-decoder network IDEDNet.

4. Implementation Details

- Loss Function (L1 Loss).

$$\mathcal{L}_1 = \frac{1}{N}\sum_{i=1}^{N} |O(C_i;\theta) - P(C_i)|$$

- Attacked chaotic encryption schemes.

  (1) Song et al. [5]; (2) Pak et al. [10]; (3) H. N. Abdullah et al. [4].

- Evaluation metric (Pearson correlation coefficient).

$$Corr = \frac{(O-\overline{O})(P-\overline{P})}{\sigma(O)\sigma(P)}$$

[5] Y. Song, J. Song, and J. Qu, “A secure image encryption algorithm based on multiple one-dimensional chaotic systems,” in ICCC, 2016.

[10] C. Pak and L. Huang, “A new color image encryption using combination of the 1d chaotic map,” Signal Process, vol. 138, pp. 129–137, 2017.

[4] H. N. Abdullah and H. A. Abdullah, “Image encryption using hybrid chaotic map,” in ICCIT, 2017.

5. Experiment

Table. 1 The ciphertext reconstruction result of known-plaintext attack method based on deep learning on MNIST and MNIST-Fashion datasets.

Network	Encryption Scheme	dataset	Training correlation coefficient	Testing correlation coefficient	Epoch	Time/ Epoch
IDEDNet	Song et al. [5]	MNIST and Fashion	97.6%	94.2%	300	5.8s
	Pak et al. [8]		97.7%	94.5%		5.7s
	H. N. Abdullah et al. [4]		98.6%	96.7%		5.8s

Visualization

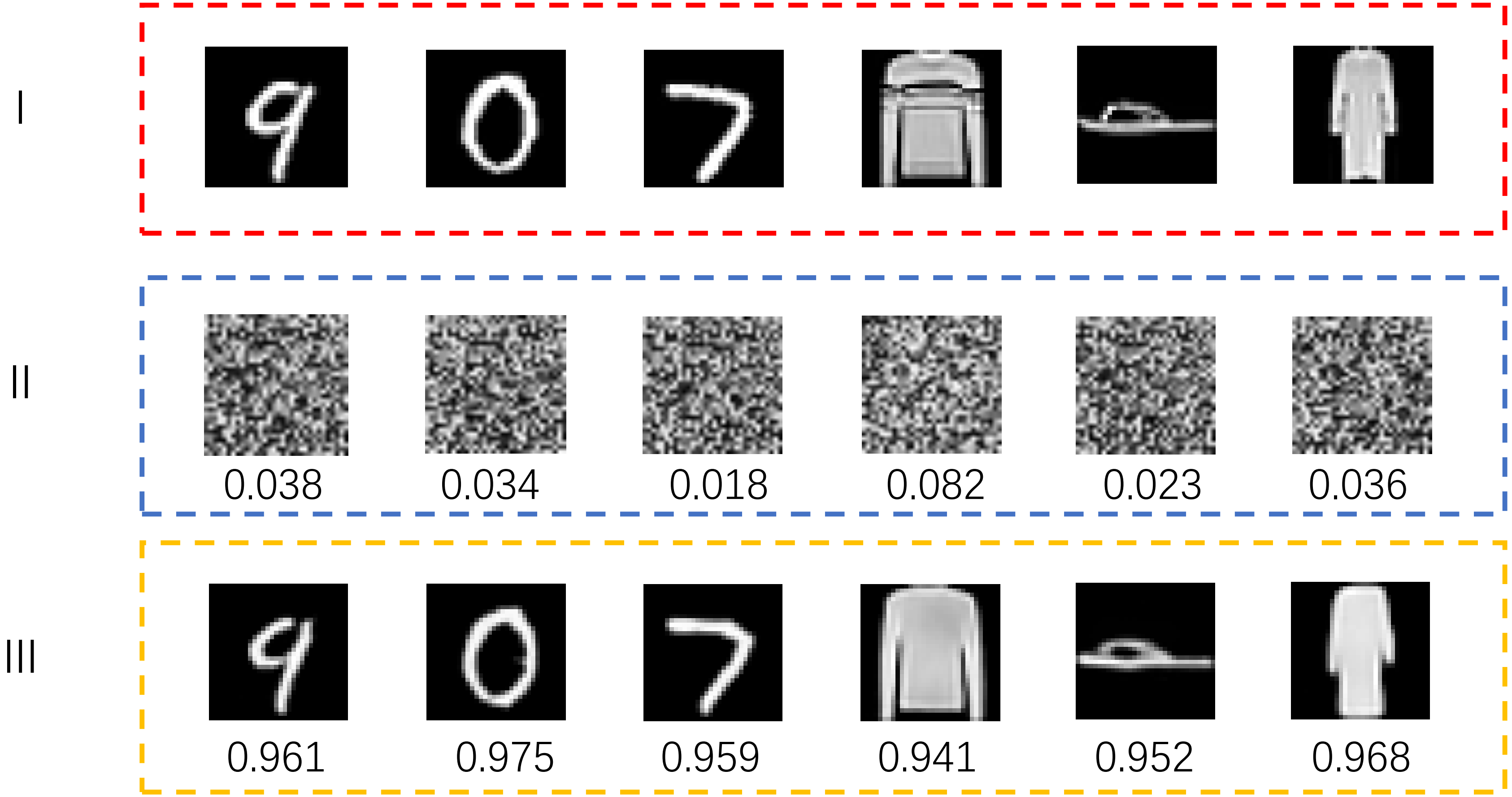
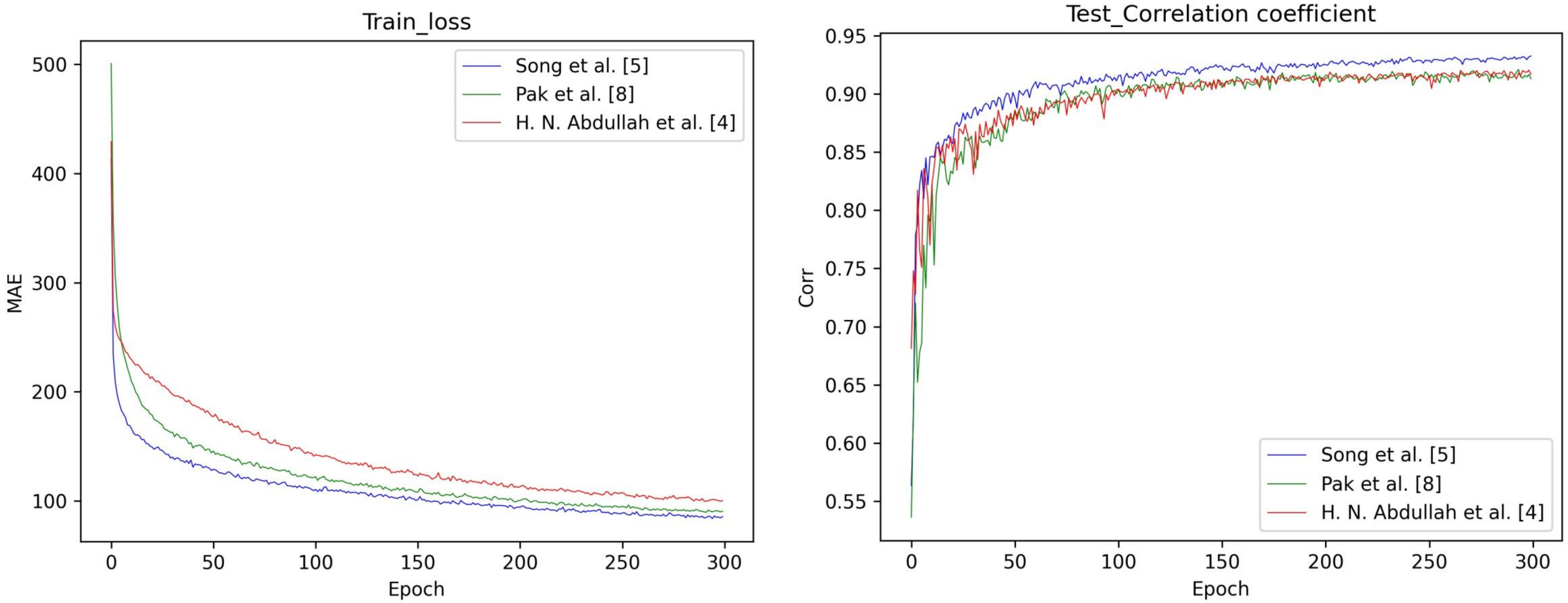


Fig. 4 visualization results on Song et al. [5]. (I) Plaintext image; (II) Ciphertext image; (III) Decrypted image; The number under the image represents the correlation coefficient between the image and the plaintext.

Visualization



(a) (b)

Fig. 5 The change curve of training and testing process on the mixed dataset of MNIST and MNIST-Fashion: (a) Training L1Loss, (b) Testing Correlation Coefficient. The blue, green and red lines represent the chaotic encryption schemes of Song et al. [5], Pak et al. [10], H. N. Abdullah et al. [4].

6. Conclusion

- Compared with the traditional known-plaintext attack methods specific to a certain chaotic cryptosystem, our method is more cost-effective, flexible;
- The chaotic cryptanalysis method based on deep learning can be introduced to multiple chaotic cryptosystems and even to the field of non-chaotic cryptosystems;
- It also proposes a new research direction in the field of multimedia security, i.e., how to prevent cryptography attack methods based on deep learning.

Q&A