# A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps

**Ahmad Pourjabbar Kari** ( a.pourjabar@gmail.com )
Islamic Azad University Tehran North Branch https://orcid.org/0000-0001-5303-3453
**Ahmad Habibizad Navin**
Islamic Azad University Tabriz Branch
**Amir Massoud Bidgoli**
Islamic Azad University Tehran North Branch
**Mirkamal Mirnia**
Tabriz University: University of Tabriz

**Original Research Paper**

**Keywords:** Multimedia security, Image encryption, Information entropy, Noise attack, Chaotic maps, Henon map

**Posted Date:** February 3rd, 2021

**DOI:** https://doi.org/10.21203/rs.3.rs-164388/v1



**Version of Record:** A version of this preprint was published at Multimedia Systems on March 13th, 2021. See the published version at https://doi.org/10.1007/s00530-021-00772-y.

# Abstract

This paper introduces a new multi-image cryptosystem based on modified Henon map and nonlinear combination of chaotic seed maps. Based on the degree of correlation between the adjacent pixels of the plain image, a unique weight is assigned to the plain image. First, the coordinates of plain images are disrupted by modified Henon map as confusion phase. In the first step of diffusion phase, the pixels content of images are changed separately by XOR operation between confused images and matrices with suitable nonlinear combination of seed maps sequences. These combination of seed maps are selected depending on the weight of plain images as well as bifurcation properties of mentioned chaotic maps. After concatenating the matrices obtained from the first step of diffusion phase, the bitwise XOR operation is applied between newly developed matrix and the other produced matrix from the chaotic sequences of the Logistic-Tent-Sine hybrid system, as second step of diffusion phase. The encrypted image is obtained after applying shift and exchange operations. The results of the implementation using graphs and histograms show that the proposed scheme, compared to some existing methods, can effectively resist common attacks and can be used as a secure method for encrypting digital images.


# Full Text

This preprint is available for download as a PDF.

# Figures

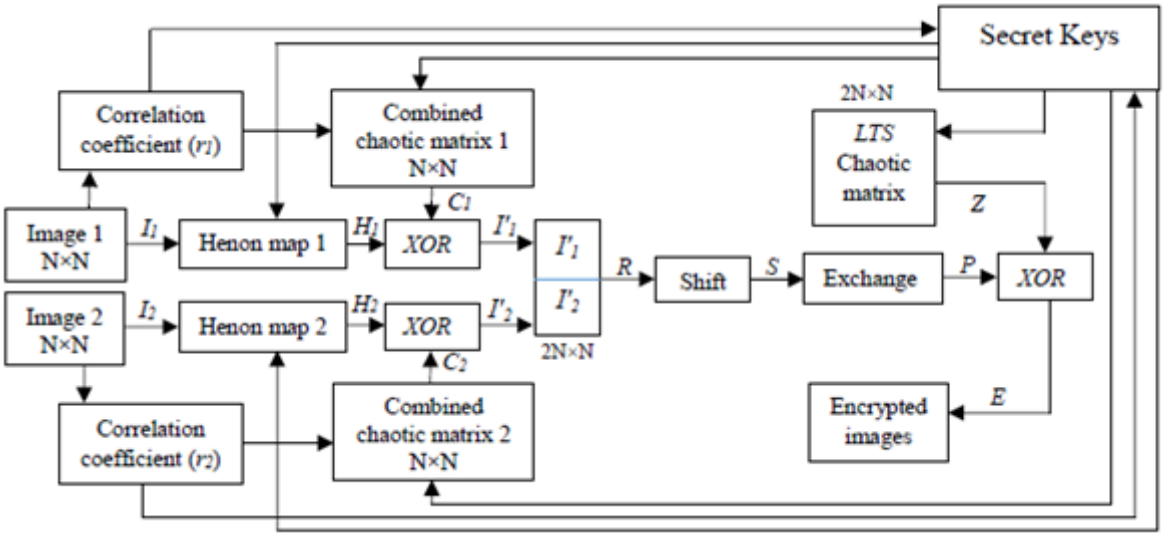
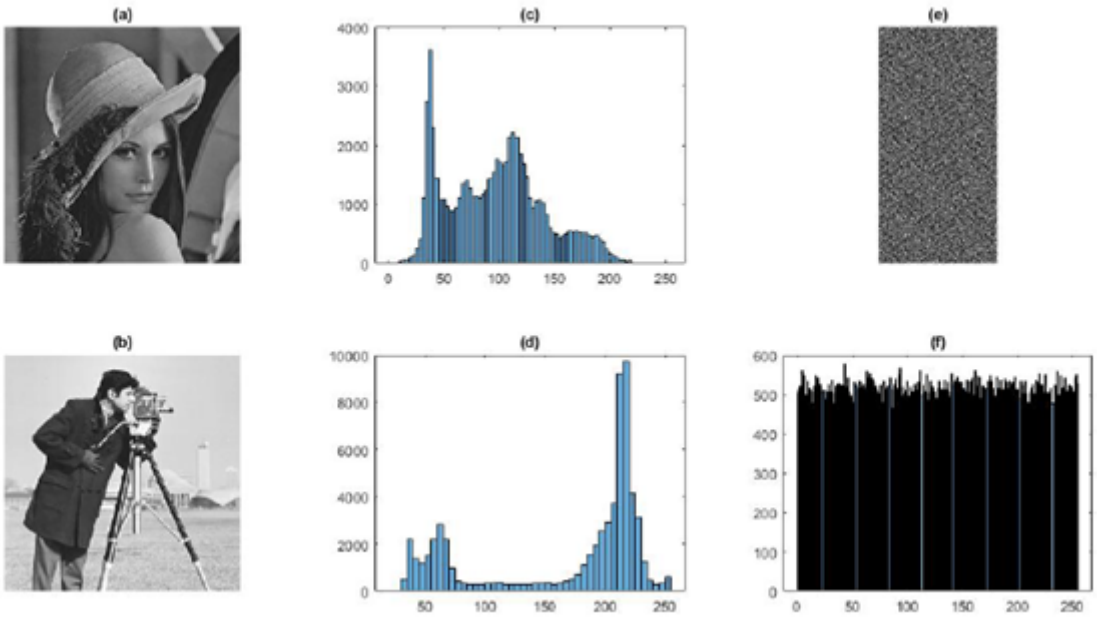


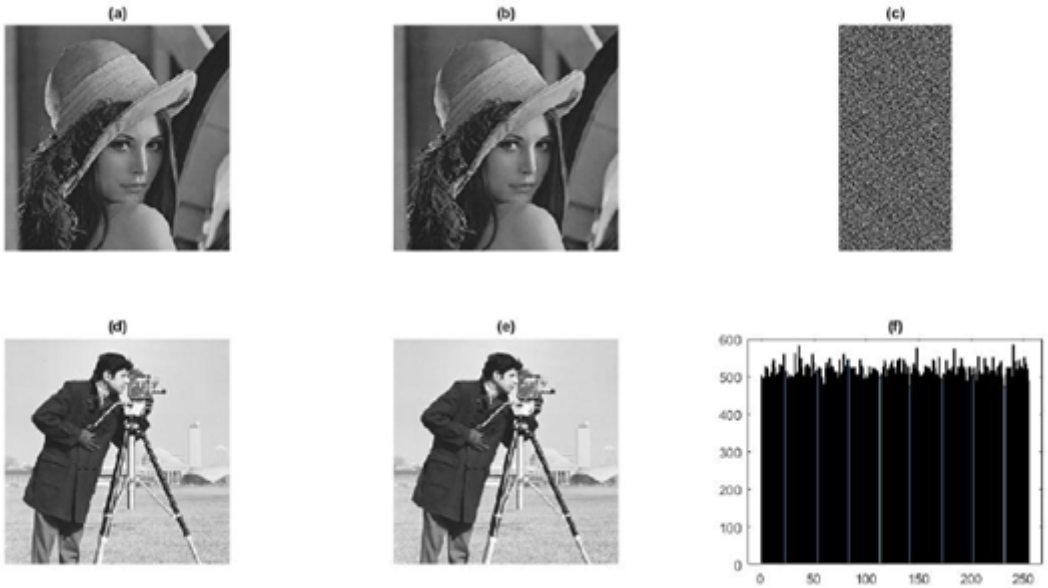

**Figure 1**

Block diagram of the proposed method



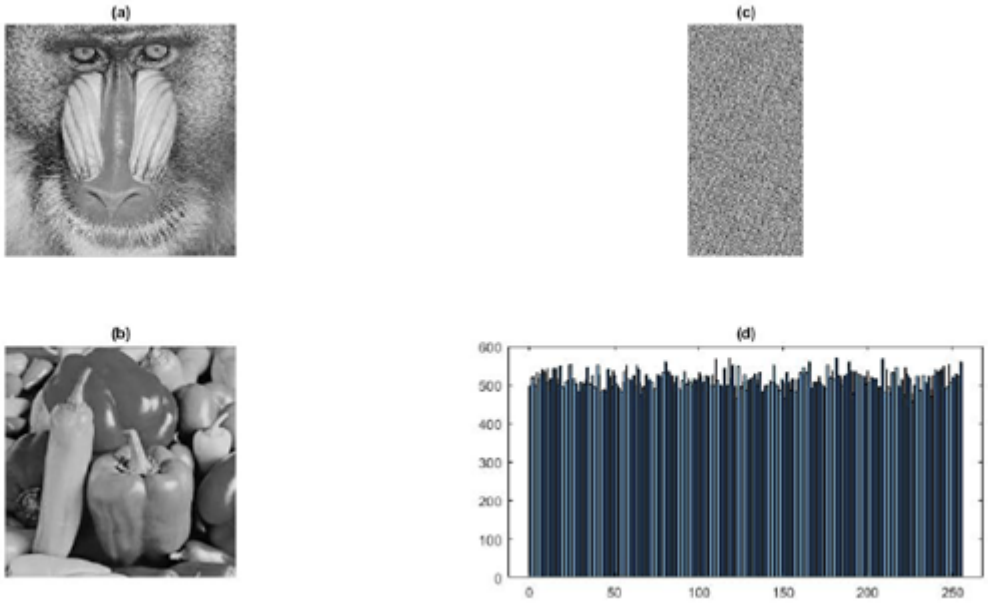

## Figure 2

(a) standard 256×256 "Lena" plain image, (b) standard 256×256 "Camera man" plain image, second column (c), (d) are plain images with non-uniform histograms respectively, (e) is the 512×256 two plain image single encrypted image, (f) is the uniform histogram of double encrypted images



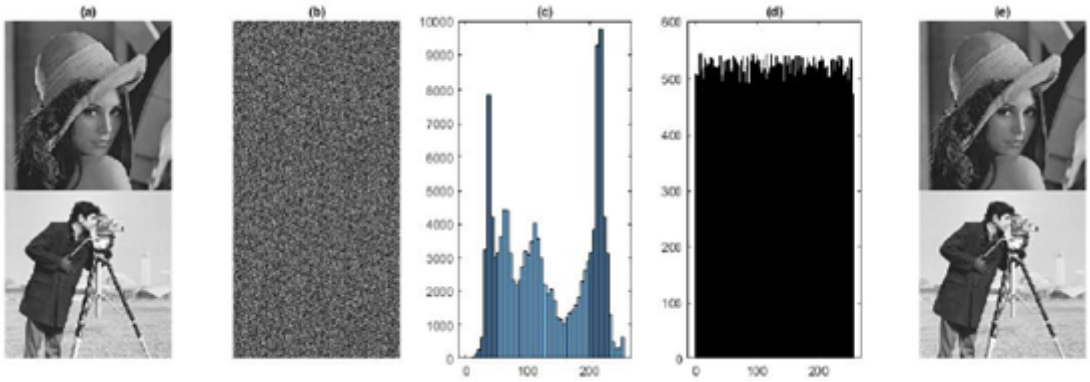

## Figure 3

First column (a), (d) are two 256×256 plain images, second column (b), (e) are decrypted images respectively, (c) is the 512×256 two plain image single encrypted image, (f) is the uniform histogram of double encrypted images



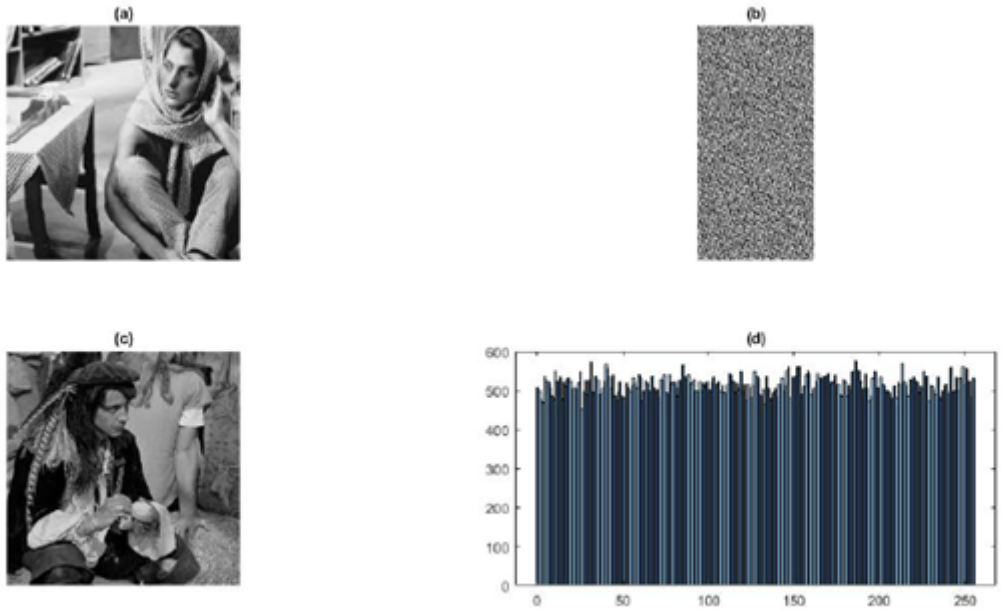

## Figure 4

(a) standard 256×256 "Baboon" plain image, (b) standard 256×256 "Peppers" plain image, (c) is the 512×256 two plain image single encrypted image, (d) is the uniform histogram of encrypted images



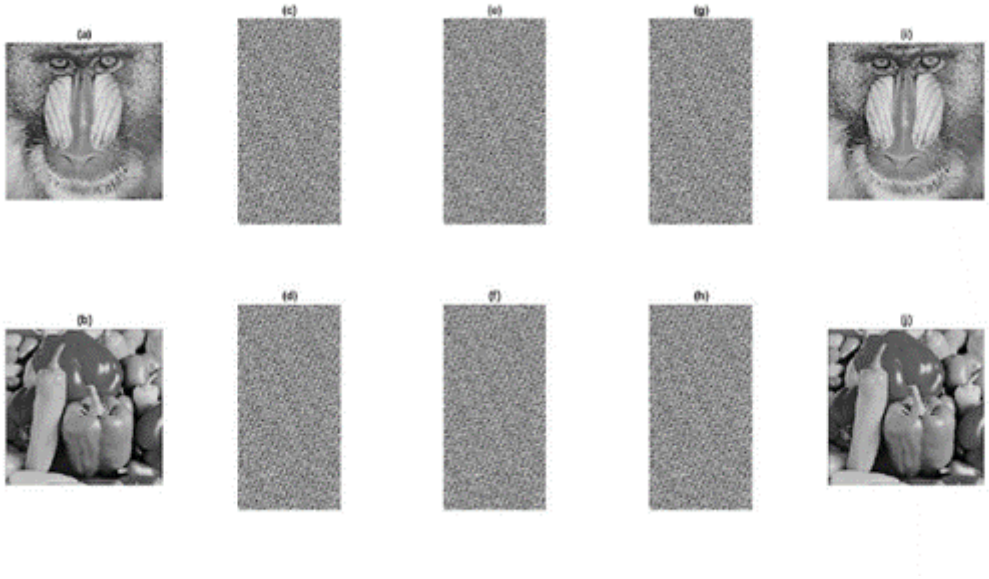

## Figure 5

(a) is 512×256 merged two 256×256 plain images, (b) is the 512×256 two plain image single encrypted image, (c) is the histogram of two concatenated plain images, (d) is the uniform histogram of encrypted images, (e) is the decrypted image




## Figure 6

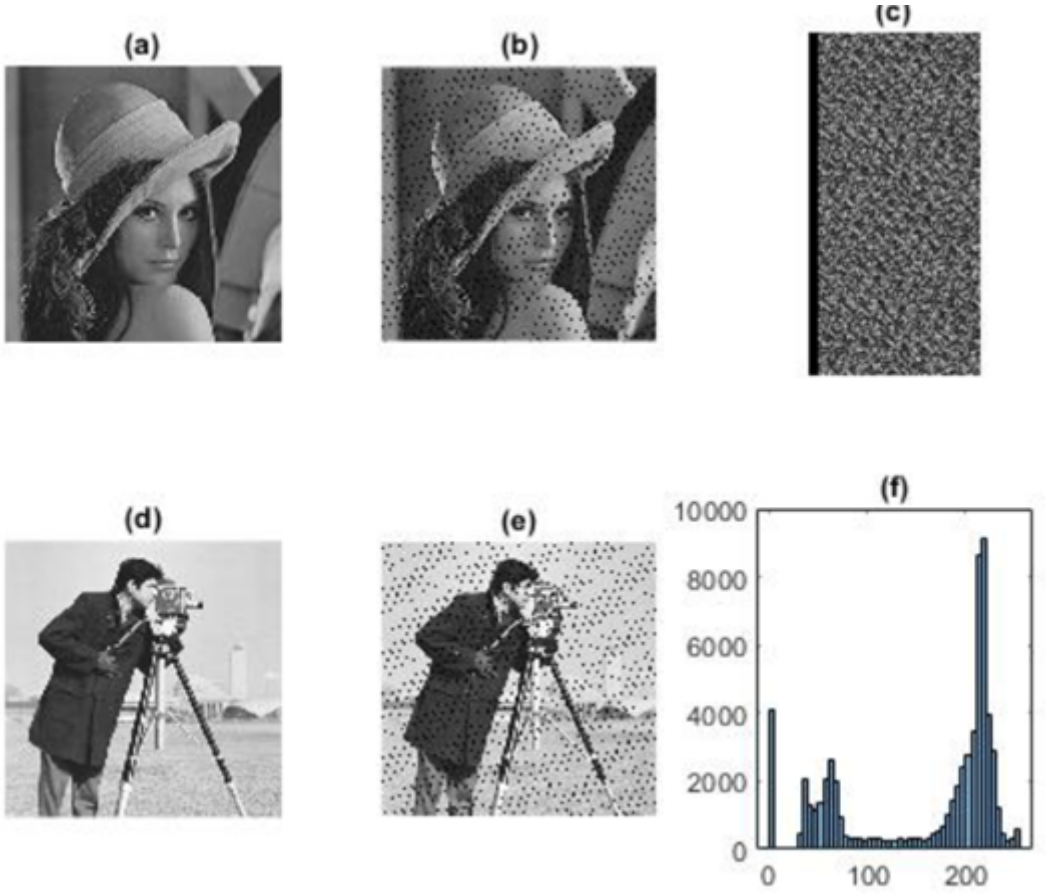
(a) standard 256×256 "Female" plain image, (c) standard "Male" 256×256 plain image, (b) is the 512×256 two plain image single encrypted image, (d) is the uniform histogram of encrypted images



## Figure 7

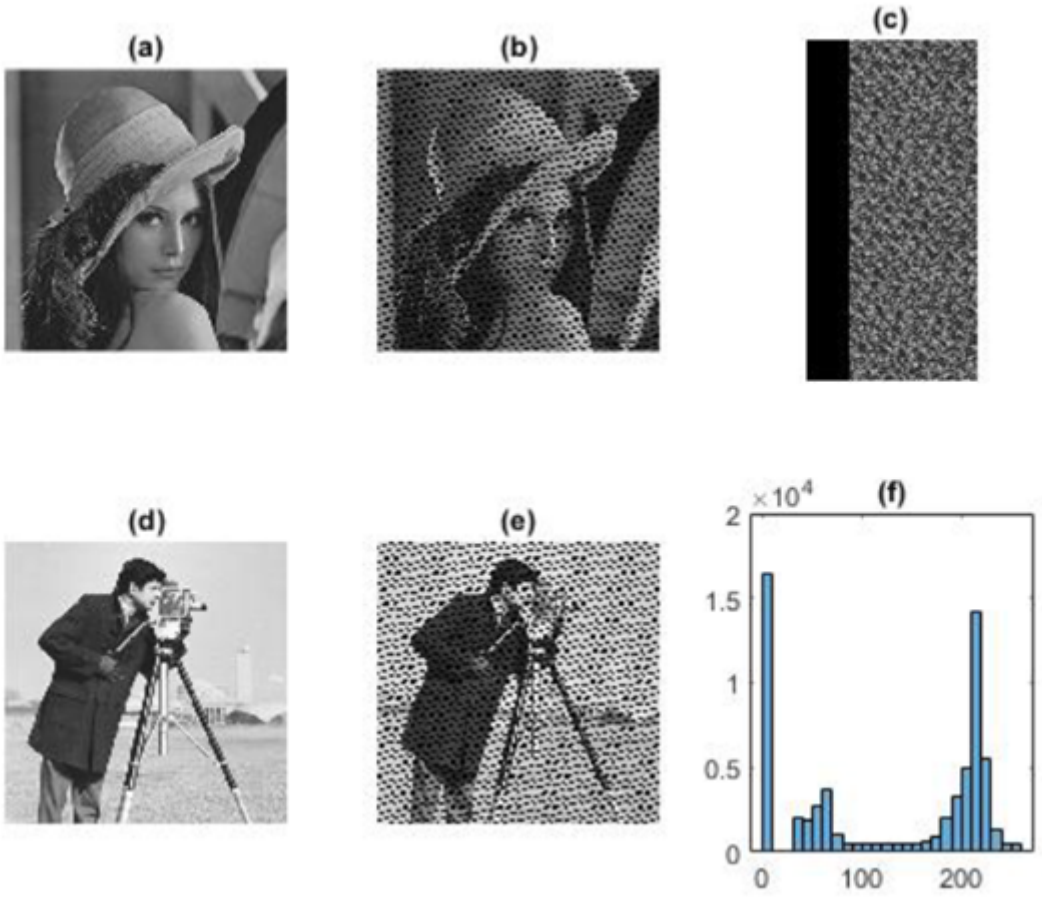
(a) and (b) are 256×256 plain images, (c) is the 512×256 encrypted image of two plain images with secret key Ke1=0.78, (d) is the 512×256 encrypted image of two plain images with secret key Ke2=0.83, (e) is the 512×256 decrypted image of two plain images with secret key Ke3=0.78+10-14, (f) is the 512×256 decrypted image of two plain images with secret key Ke4=0.83+10-14, (g) is the 512×256 decrypted image of two plain images with secret key Ke5=0.93, (h) is the 512×256 decrypted image of

two plain images with secret key Ke4=0.63, (i) is the decrypted image of plain image (a) with correct secret key Ke1=0.78, (j) is the decrypted image of plain image (b) with correct secret key Ke2=0.83



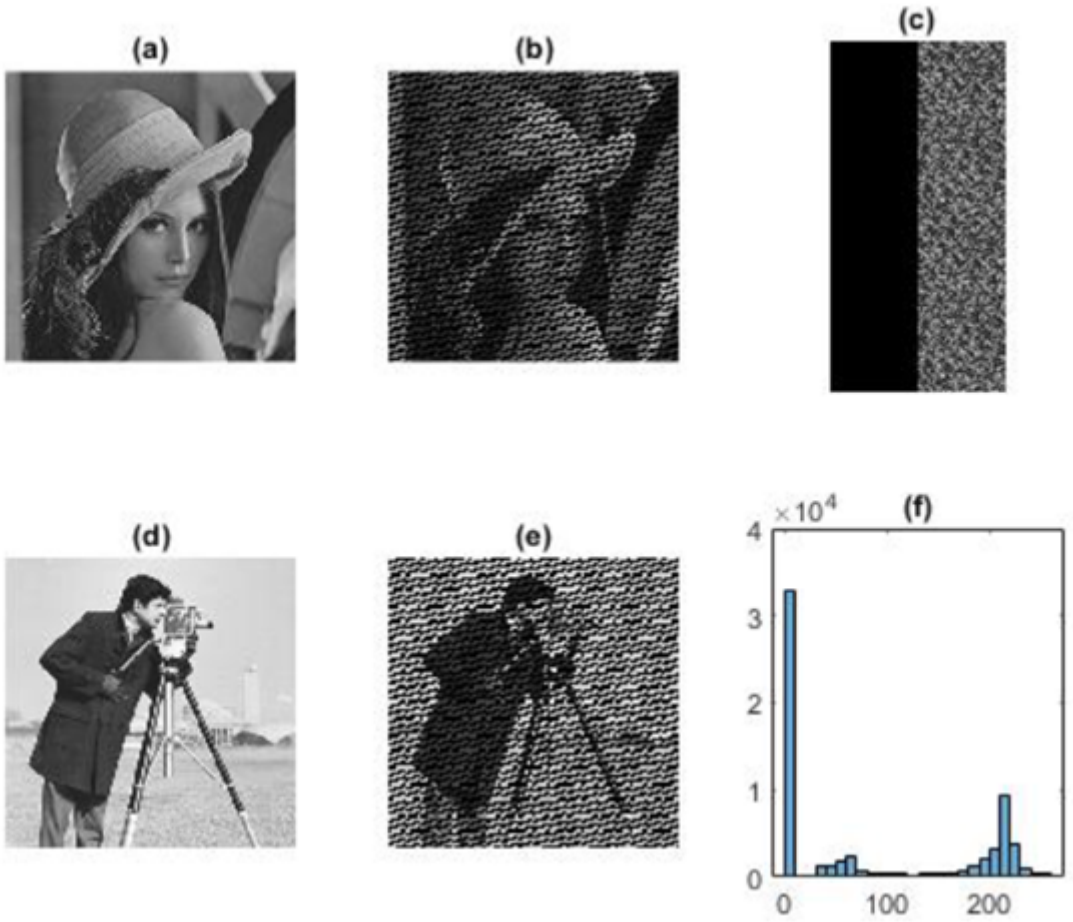

## Figure 8

(a) and (d) are 256×256 plain images, (b) is the decrypted image for (a) after 1/16 cropping attack in one round, (e) is the decrypted image for (d) after 116 cropping attack in one round, (c) is the 512×256 two plain image single encrypted image after 1/16 cropping attack, (f) is the histogram of (e)



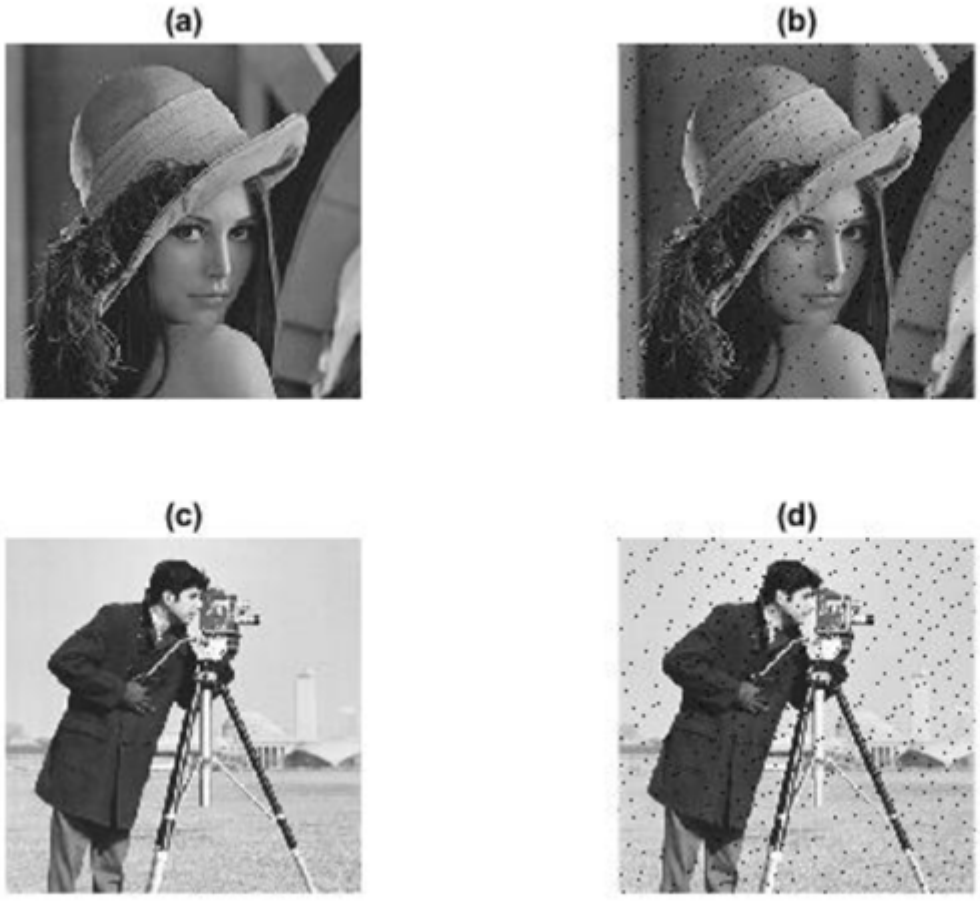

## Figure 9

a) and (d) are 256×256 plain images, (b) is the decrypted image for (a) after 1/4 cropping attack, (e) is the decrypted image for (d) after 1/4 cropping attack, (c) is the 512×256 two plain image single encrypted image after 1/4 cropping attack, (f) is the histogram of (e)




## Figure 10

(a) and (d) are 256×256 plain images, (b) is the decrypted image for (a) after 1/2 cropping attack, (e) is the decrypted image for (d) after 1/2 cropping attack, (c) is the 512×256 two plain image single encrypted image after 1/2 cropping attack, (f) is the histogram of (e)




## Figure 11

a) and (c) are 256×256 plain images, (b) is the decrypted image for (a) after 5% salt and pepper attack, (d) is the decrypted image for (c) after 5% salt and pepper attack

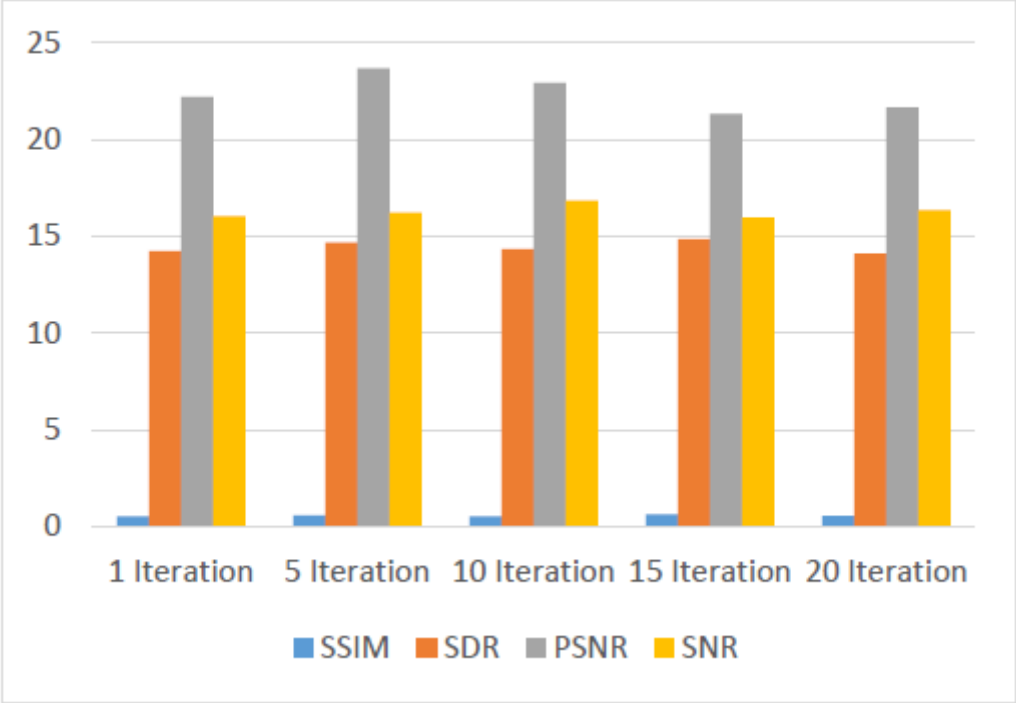



**Figure 12**

Evaluating parameters for various iterations, and 1/16 cropping attack


**Figure 13**

Evaluating parameters for various iterations, and 1/4 cropping attack

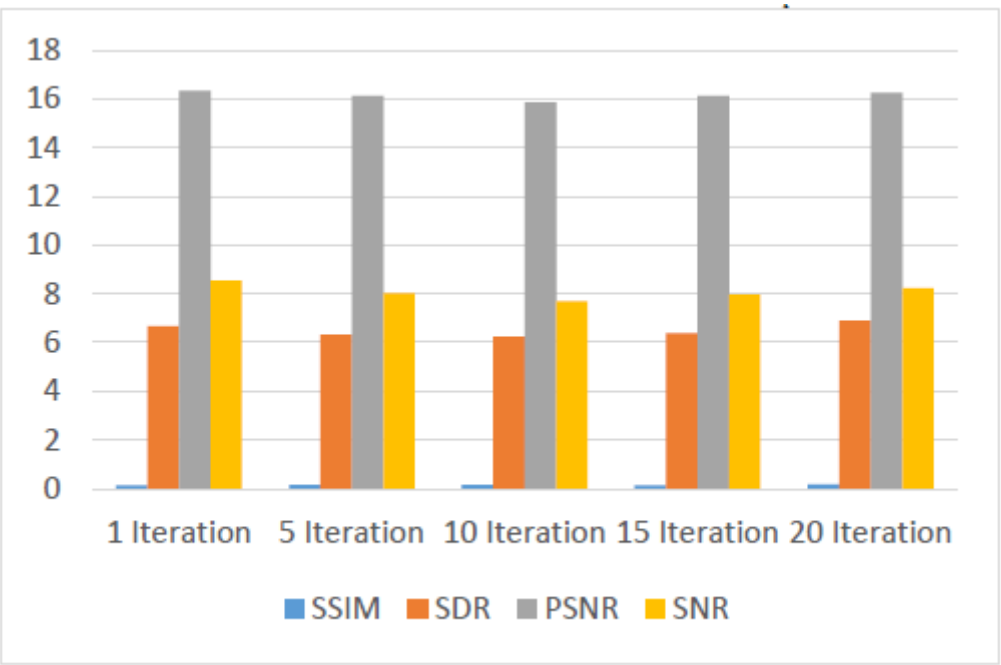



**Figure 14**

Evaluating parameters for various iterations, and 1/2 cropping attack