Homomorphic image encryption

Article *in* Journal of Electronic Imaging · July 2009

DOI: 10.1117/1.3167847 · Source: DBLP

5 authors, including:

Ibrahim Elashry
University of Wollongong
17 PUBLICATIONS **115** CITATIONS
SEE PROFILE

Osama S. Farag Allah
Minoufiya University
136 PUBLICATIONS **917** CITATIONS
SEE PROFILE

Alaa M. Abbas
39 PUBLICATIONS **193** CITATIONS
SEE PROFILE

El-Sayed Mahmoud El-Rabaie
Faculty of Electronic Engineering, Menouf
386 PUBLICATIONS **826** CITATIONS
SEE PROFILE

Homomorphic image encryption

Ibrahim F. Elashry
Kafrelshiekh University
Faculty of Engineering
Department of Electrical Communications
Kafrelshiekh, Egypt

Osama S. Farag Allah
Menoufia University
Faculty of Electronic Engineering
Department of Computers Engineering
Menouf, Egypt

Alaa M. Abbas
S. El-Rabaie
Fathi E. Abd El-Samie
Menoufia University
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menouf, Egypt
E-mail: fathi_sayed@yahoo.com

Abstract. *This paper presents a new homomorphic image cryptosystem. The idea of this system is based on encrypting the reflectance component after the homomorphic transform and embedding the illumination component as a least significant bit watermark into the encrypted reflectance component. A comparison study is held between the RC6 block cipher algorithm and the chaotic Baker map algorithm for the encryption of the reflectance component. We present a security analysis for the proposed cryptosystem against the entropy, brute-force, statistical, and differential attacks from a strict cryptographic viewpoint. Experimental results verify and prove that the proposed homomorphic image cryptosystem is highly secure from the cryptographic viewpoint. The results also prove that this cryptosystem has a very powerful diffusion mechanism (a small change in the plain text makes a great change in the cipher image). The homomorphic encryption using RC6 algorithm is more secure than that using the chaotic Baker map algorithm but not robust to noise. Thus, the proposed homomorphic cryptosystem can be used in different applications, depending on the core algorithm used. © 2009 Society of Photo-Optical Instrumentation Engineers.* [DOI: 10.1117/1.3167847]

1 Introduction

Today, more and more information is transmitted over the Internet. This information is not only text, but also audio, image, and other multimedia. Images are widely used in our daily life. However, the more extensively we use the images, the more important their security will be. For example, it is important to protect diagrams of army emplacements, diagrams of bank-building construction, and the important data captured by military satellites. In addition, the number of computer crimes has recently increased. For these reasons, image security has become an important topic in the current computer world.

Most of the traditional or the modern cryptosystems have been designed to protect textual data.[1–7] The original plain text is converted into cipher text, which is apparently random nonsense. Once the cipher text has been produced, it is stored or transmitted over a network. Upon reception, the cipher text can be transformed back into the original plain text by using a decryption algorithm. For the encryption of images using traditional cryptosystems, such as the Rivest Shamir Adleman (RSA) or the data encryption standard cryptosystems, the images must first be converted into one-dimensional arrays.[5]

Cryptography aims at achieving three major requirements: diffusion, confusion, and dependence on keys. These requirements are readily satisfied by chaotic functions because of their sensitive dependence on initial conditions, topological transitivity, and ergodicity.[8–12] This makes chaos theory a strong candidate for the design of efficient image cryptosystems. Fridrich has proposed a general framework for the application of chaotic maps in image encryption.[10] In this framework, the analog chaotic map is first discretized. Then, it is generalized by the introduction of some parameters. The parameters of the map constitute the key for the image cryptosystem.

In this paper, we propose a new image cryptosystem. This system is based on homomorphic image processing, which has evolved primarily as a tool of image enhance-

Paper 08144RR received Sep. 1, 2008; revised manuscript received May 8, 2009; accepted for publication May 26, 2009; published online Jul. 14, 2009.

1017-9909/2009/18(3)/033002/14/$25.00 © 2009 Society of Photo-Optical Instrumentation Engineers.

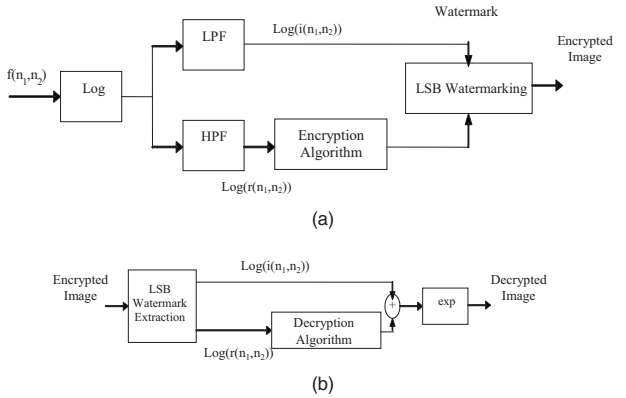


Fig. 1 Proposed homomorphic image cryptosystem: (a) Encryption subsystem and (b) decryption subsystem.

ment for images captured in bad lighting conditions.[12,13] The main idea of homomorphic image processing is based on modeling the image as a product of a constant illumination and a varying reflectance. The product is dealt with as a summation using the logarithmic operation. The reflectance component can be separated using a high-pass filter, while the illumination component can be separated using a low-pass filter. Most of the image details lie in the reflectance component while the illumination component is approximately constant. We can carry out the encryption process in the homomorphic domain on the reflectance component, which is the most significant component of the image. Rather than encrypting the illumination component, which causes redundancy in the image information, it is appended as a least significant bit (LSB) watermark in the encrypted reflectance component. We use two algorithms for the encryption of the reflectance component—the RC6 block cipher algorithm and the chaotic Baker map algorithm—and make a comparison between them.

Unlike optical encryption,[14] which deals only with light and depends on certain parameters, such as wavelength, phase, and polarization of light waves, the proposed image cryptosystem works directly on digital images. There is no need in the proposed cryptosystem to deal with light using expensive optical fiber circuits. Optical encryption also has a disadvantage represented in the difficulty of implementation of simple encryption operations such as the Xor operation implemented easily in the proposed cryptosystem.[15]

The rest of this paper is organized as follows. Section 2 explains the design principles of an image cryptosystem. Section 3 presents a description of the architecture and the specifications of the proposed homomorphic image cryptosystem. The detailed security analysis of the proposed cryptosystem, including the information entropy analysis, the key space analysis, the statistical analysis, and the differential analysis, is made in Sec. 4. The effect of noise on the decryption process is discussed in Sec. 5, and Sec. 6 gives the concluding remarks.

2 Design Principles of an Image Cryptosystem

An efficient image cryptosystem must have a high overall security performance in addition to being flexible. Image security requires the following characteristics:[16]

1. The encryption system should be computationally secure. It must require an extremely long computation time to break. Thus, unauthorized users should not be able to read privileged images.
2. Encryption and decryption should be fast enough to keep the high performance of the system. The algorithms for encryption and decryption must be simple enough to be carried out by users with a personal computer.
3. The security mechanism should be as widespread as possible. It must be widely acceptable to design a cryptosystem like a commercial product.
4. The security mechanism should be flexible.
5. There should be no expansion of the encrypted image data.

3 Proposed Homomorphic Cryptosystem

The idea of the proposed cryptosystem is based on homomorphic image processing. It is known that the image intensity can be represented as follows:[15,16]

$$f(n_1,n_2) = i(n_1,n_2)r(n_1,n_2), \tag{1}$$

where $i(n_1,n_2)$ is the light illumination and $r(n_1,n_2)$ is the reflectance of the object to be imaged. Taking the log of both sides leads to

$$\log[f(n_1,n_2)] = \log[i(n_1,n_2)] + \log[r(n_1,n_2)]. \tag{2}$$

The illumination is approximately constant while the reflectance is variable from object to object. Thus, the term $\log[i(n_1,n_2)]$ is approximately constant. We can perform the encryption process on the $\log[r(n_1,n_2)]$ term. To avoid the redundancy resulting from the existence of two components of the image in the homomorphic domain, we can embed the illumination component as a LSB watermark to the encrypted reflectance component. The proposed encryption and decryption subsystems are shown in Fig. 1.

There are several encryption algorithms that can be used for encrypting the reflectance component. We have chosen two of these algorithms and compared them in our proposed homomorphic cryptosystem. These algorithms are the RC6 block cipher algorithm and the chaotic Baker map algorithm. The first one belongs to the family of diffusion algorithms, and the second one belongs to the family of permutation algorithms. We must decide which family is much more appropriate for the proposed homomorphic cryptosystem based on the application to be used in.

3.1 *RC6 Block Cipher Algorithm*

The RC6 block cipher algorithm belongs to the family of diffusion algorithms. It is used for data encryption and can also be adapted for image encryption. It depends mainly on the use of four working registers, each of size 32 bits. Thus, it handles 128 bits input/output blocks; 16 pixels of the image can form these 128 bits blocks. Its main parameters are the word size (w) in bits, the non-negative number of rounds (r), and the length of the encryption/decryption key (b) in bytes. The use of multiplication greatly increases the

diffusion achieved per round, allowing for a higher security, fewer rounds, and an increase in the throughput.[17]

The RC6 encryption algorithm has many advantages. Unlike many other encryption algorithms, the RC6 algorithm does not use lookup tables during the encryption. This means that the RC6 code and data can readily fit within today's on-chip cache memory.[17] This algorithm is a secure, compact, and simple block cipher algorithm. It offers good performance and considerable flexibility.

3.2 *Chaotic Baker Map Algorithm*

This algorithm belongs to the family of permutation algorithms. A chaotic map is generalized by introducing parameters and then discredited to be applied to the pixels. To encrypt an $N \times N$ image, the ciphering map is iteratively applied to the image. The construction of the cipher and its security depends on the chaotic map. The chaotic Baker map (B), is described with the following equations:[18]

$$B(x,y) = (2x, y/2) \quad \text{when } 0 \leqslant x < 1/2, \tag{3}$$

$$B(x,y) = (2x-1, y/2+1/2) \quad \text{when } 1/2 \leqslant x \leqslant 1. \tag{4}$$

Because an image is defined on a lattice of many points (pixels), a correspondingly discretized form of the basic map needs to be derived. In particular, the discretized map is required to assign a pixel to another pixel in a bijective manner. Because the discretized map is desired to inherit the properties of the continuous basic map, the discretized map should become increasingly close to the basic map as the number of pixels tends to infinity.[18]

4 Security Analysis and Test Results

A good encryption scheme should resist all kinds of known attacks, such as the known-plain-text attack, the cipher-text-only attack, the statistical attack, the differential attack, and the various brute-force attacks.[18–22] The security of the proposed homomorphic image cryptosystem is investigated for digital images under the brute-force attack, the statistical attacks, and the differential attacks.[20,24] It will be shown that the proposed homomorphic image cryptosystem is secure from the strongly cryptographic viewpoint.

The results show the satisfactory security of the proposed cryptosystem, as demonstrated in Secs. 4.1–4.4. Here, some security analysis results, including the key space analysis, statistical analysis, and differential analysis, are presented.[20,24] Tests are made on the image of Lena shown in Fig. 2.

4.1 *Information Entropy Analysis*

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon.[23] Modern information theory is concerned with error correction, data compression, cryptography, communication systems, and related topics.[25]

To calculate the entropy $H(m)$ of a source m, we use the following equation:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \text{ bits}, \tag{5}$$

where $p(m_i)$ represents the probability of occurrence of the symbol m_i. The entropy is expressed in bits.

Let us suppose that the source emits 2^8 symbols with equal probability [i.e, $m=(m_1, m_2, \ldots, m_2^8)$]. After evaluating Eq. (5), we obtain its entropy $H(m)=8$, which corresponds to a uniform random source. Actually, given that a practical information source seldom generates random messages, its entropy value is, in general, smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy of <8, then there exists a certain degree of predictability, which threatens its security.

4.2 *Statistical Analysis*

In Ref. 23, Shannon mentioned that, "It is possible to solve many kinds of ciphers by statistical analysis." Statistical analysis is performed in this paper on the proposed homomorphic image cryptosystem, demonstrating its superior confusion and diffusion properties, which strongly resist statistical attacks. This is shown by a test on the histograms of the encrypted images and on the correlation coefficients between pixels in the same place in the plain and cipher images.

4.2.1 *Histograms of encrypted images*

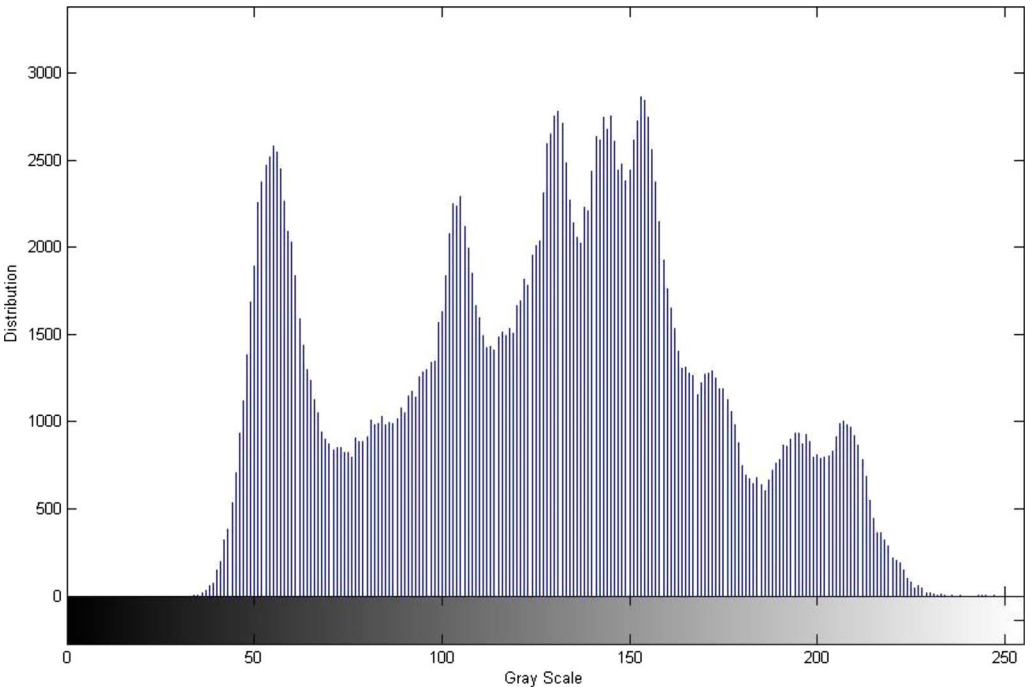
A typical example of the histogram test is shown in Figs. 3–6, from which one can see that the histogram of the encrypted image (cipher image) by the homomorphic cryptosystem using the RC6 algorithm is fairly uniform and significantly different from that of the original image (plain image), as shown in Fig. 3. A similar result is obtained for the encryption using the RC6 block cipher algorithm as shown in Fig. 4. For the homomorphic cryptosystem using the chaotic Baker map algorithm, the result is shown in Fig. 5. It is clear that the histogram is different from that obtained with the chaotic Baker map encryption algorithm, whose result is shown in Fig. 6. It is known that chaotic Baker map encryption does not change the histogram of the encrypted image from that of the original image. On the other hand, the homomorphic cryptosystem using the chaotic Baker map algorithm makes a change in the histogram of the encrypted image as shown in Fig. 5.

4.2.2 *Correlation between pixels in the same place in the plain and cipher images*

A useful measure to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels in the same place in the plain and cipher images.[26] This measure can be calculated as follows:

$$\text{cov}(x,y) = E[x - E(x)][y - E(y)], \tag{6}$$

(a)



(b)

Fig. 2 The original image of Lena: (a) The image and (b) the histogram.

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

where x and y are the gray-scale values of two pixels in the same place in the plain and cipher images. In numerical computations, the following discrete formulas can be used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2, \tag{9}$$

Table 1 Correlation coefficient between pixels in the same place in the plain and cipher images.

Encryption algorithm	Correlation coefficient
Homomorphic cryptosystem with the RC6 algorithm	0.0033
RC6 algorithm	0.0013
Homomorphic cryptosystem with the chaotic Baker map algorithm	0.0043
Chaotic Baker map algorithm	0.0032

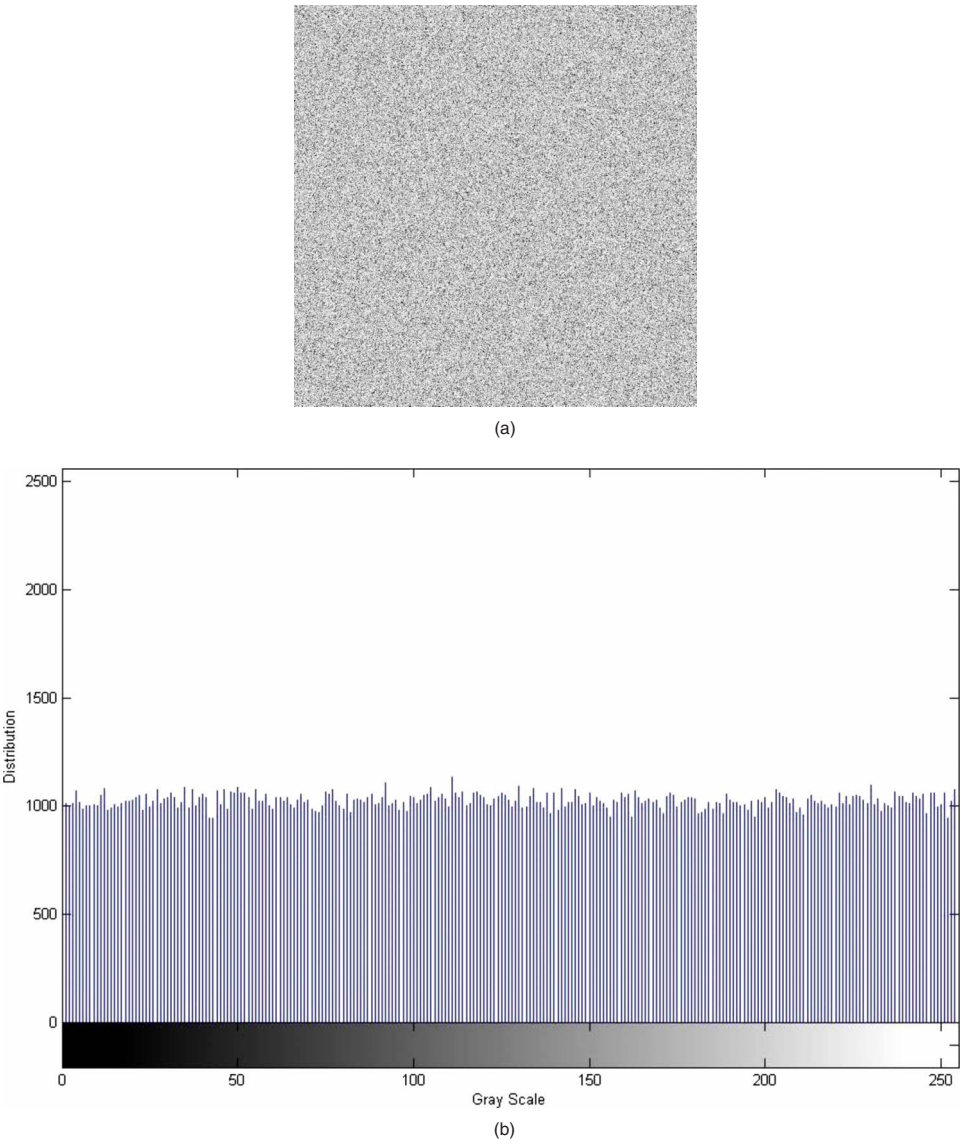


Fig. 3 Encrypted image using the homomorphic cryptosystem with the RC6 algorithm: (a) The encrypted image and (b) the histogram.

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)], \tag{10}$$

where N is the number of pixels involved in the calculations. The lower the value of the estimated correlation coefficient in the encrypted image is, the better the quality of the encryption algorithm.

The correlation coefficient results for the image cryptosystems compared in this paper are presented in Table 1. From these results, we can see that all the compared image cryptosystems have a low correlation coefficient between pixels in the same place in the plain and the cipher images, which means that they all give a good encryption quality.

4.3 *Key Space Analysis*

A good image encryption algorithm should be sensitive to the cipher keys. For the proposed homomorphic image cryptosystem, the key space analysis and test are summarized in the following Secs. 4.3.1 and 4.3.2

4.3.1 *Exhaustive key search*

For a secure image cryptosystem, the key space should be large enough to make the brute-force attack infeasible.[27] The RC6 algorithm is a 128-bit encryption scheme whose key space size ranges from 0 to 2040 bits. An exhaustive key search will take 2^k operations to succeed, where k is the key size in bits. An attacker simply tries all keys, and this will be very exhaustive. Assume that the secret key length is 128 bits. Therefore, an opponent will need $\sim 2^{128}$ operations to successfully determine the key. If the opponent employs a 1000-MIPS computer to guess the key, the computations will require:

$$\frac{2^{128}}{1000 \times 10^6 \times 60 \times 60 \times 24 \times 365} > 10.7902831 \times 10^{21} \text{ years.}$$

This is practically infeasible.

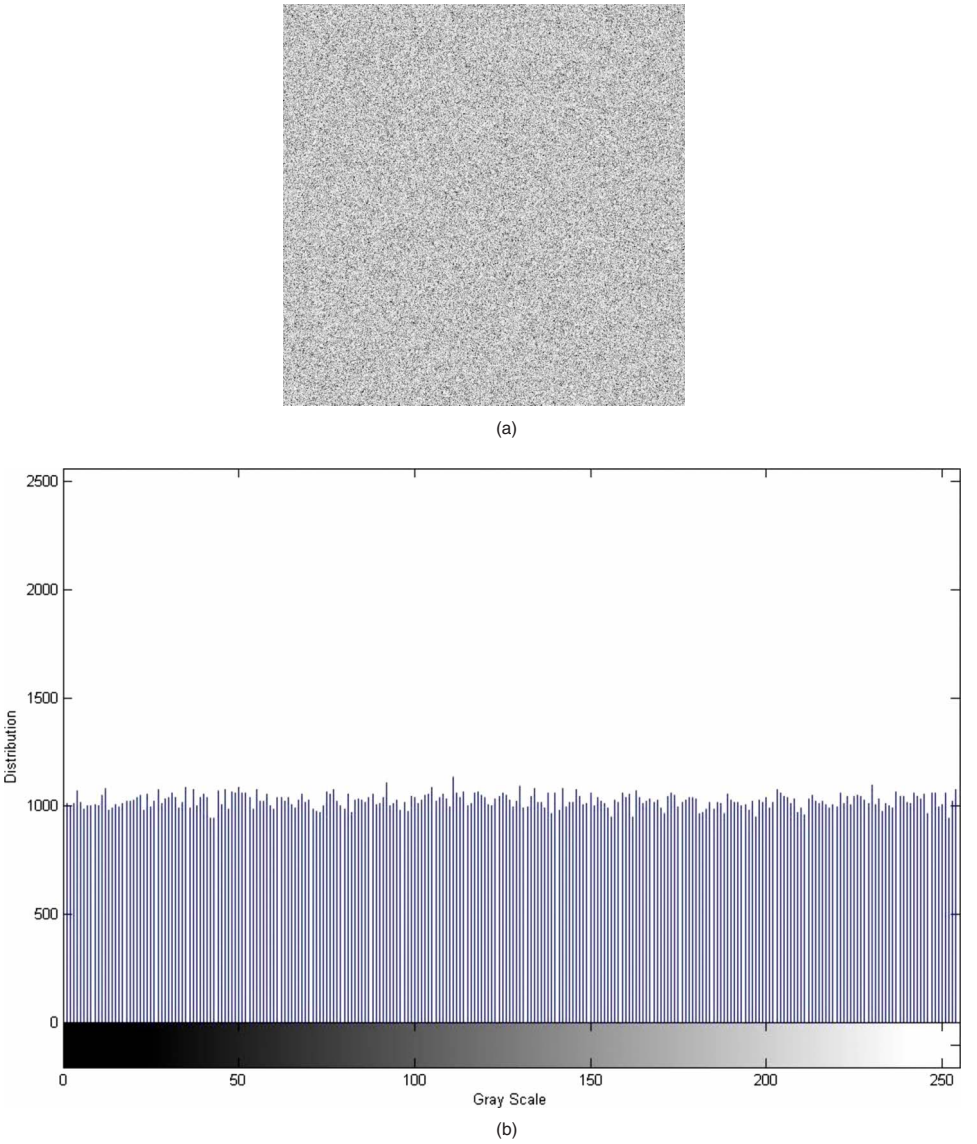


Fig. 4 Encrypted image using the RC6 algorithm: (a) The encrypted image and (b) the histogram.

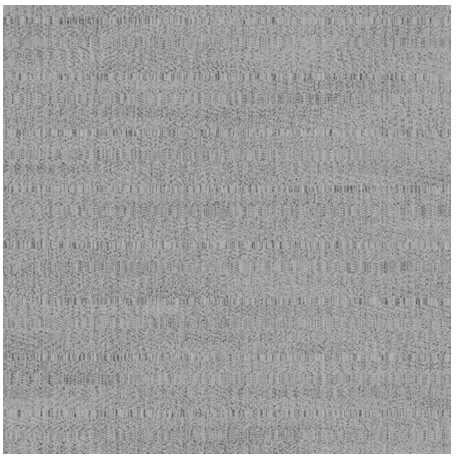
For chaotic maps encryption, the key is dependent on the width (or height) of the image to be encrypted. This is due to the scrambling phenomenon of the chaotic map. For the 512×512 Lena image, the number of possible keys $= 10^{126}$. Thus, in this case the computations will require

$$\frac{10^{126}}{1000 \times 10^6 \times 60 \times 60 \times 24 \times 365} > 3.1710 \times 10^{109} \text{ years}.$$

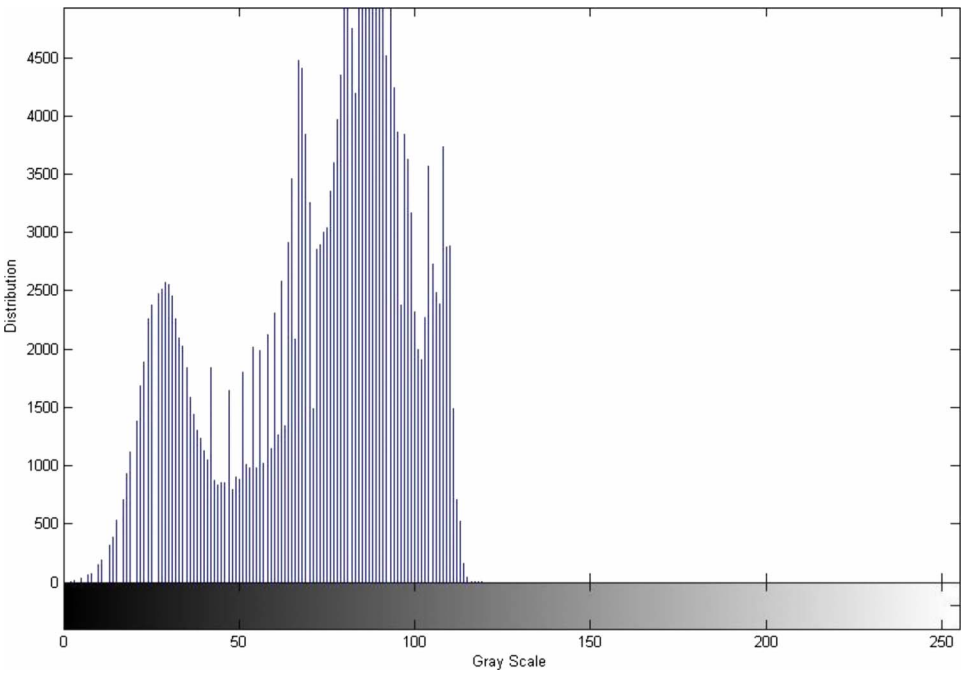
4.3.2 *Key sensitivity test*

Large key sensitivity is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly if there is only a slight difference between encryption and decryption keys.[23] Assume that a 16-character ciphering key is used.[28] This means that the key consists of 128 bits. For testing the key sensitivity of the proposed homomorphic encryption using the RC6 algorithm, we perform the following steps:

1. An image in is encrypted using the secret key of 32 zeroes (in hexadecimal), and the resultant image is referred to as encrypted image A [see Fig. 7(a)].
2. The same image is encrypted by making a slight modification in the secret key [i.e., eight and 31 zeroes (in hexadecimal)]. Change is made in the most significant digit of the secret key. The resultant image is referred to as encrypted image B [see Fig. 7(b)].
3. Again, the same image is encrypted by making another slight modification in the secret key [i.e., 31 zeroes and one (in hexadecimal)]. The change is made in the least significant digit of the secret key. The resultant image is referred to as encrypted image C [see Fig. 7(c)].



(a)



(b)

Fig. 5 Encrypted image using the homomorphic cryptosystem with the chaotic Baker map algorithm: (a) The encrypted image and (b) the histogram.

Table 2 Results of the key sensitivity test for the homomorphic cryptosystem with the RC6 algorithm.

Image 1	Image 2	Correlation coefficient
Encrypted image A	Encrypted image B	0.0034
Encrypted image B	Encrypted image C	0.00007
Encrypted image C	Encrypted image A	−0.0008

Table 3 Results of the key sensitivity test for the RC6 algorithm.

Image 1	Image 2	Correlation coefficient
Encrypted image A	Encrypted image B	0.0013
Encrypted image B	Encrypted image C	−0.0028
Encrypted image C	Encrypted image A	−0.0004

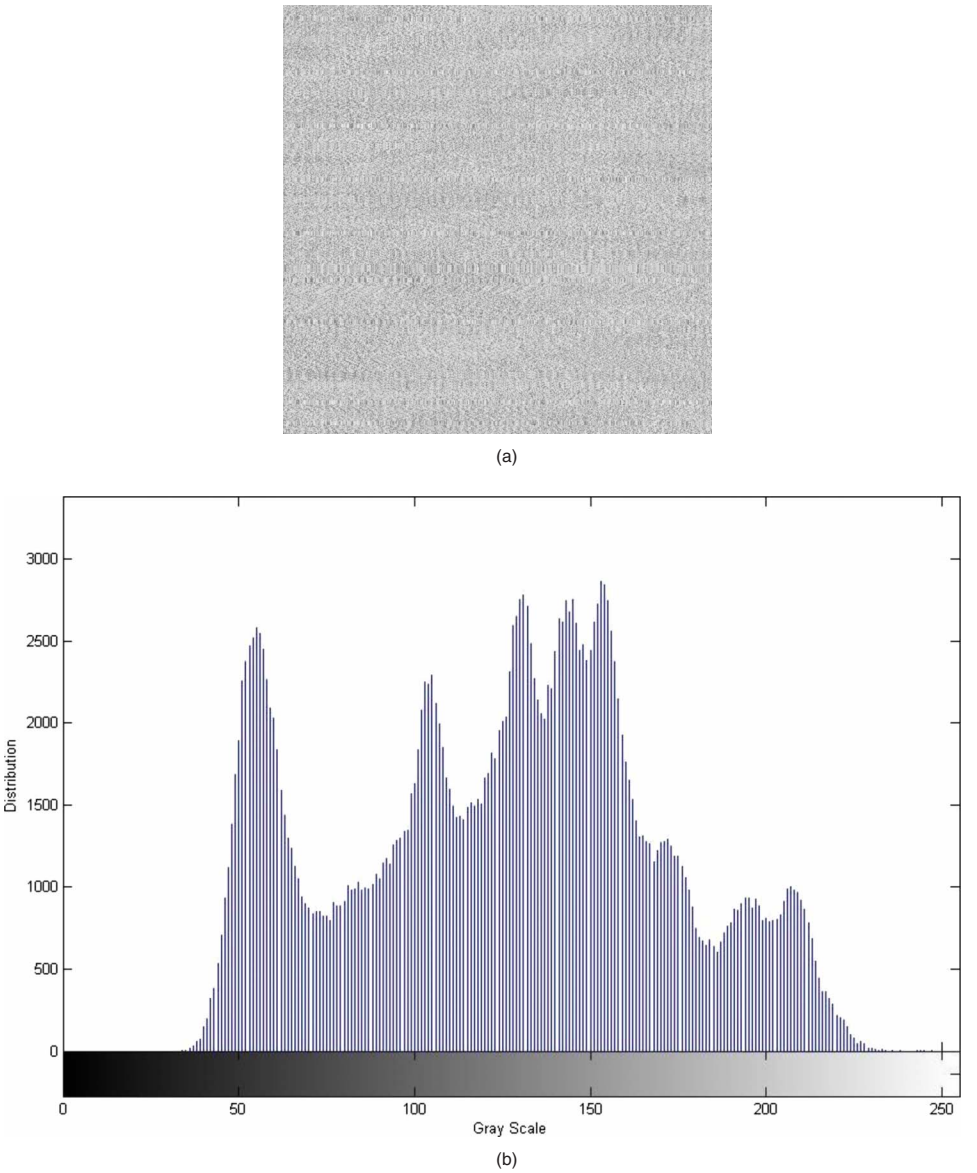


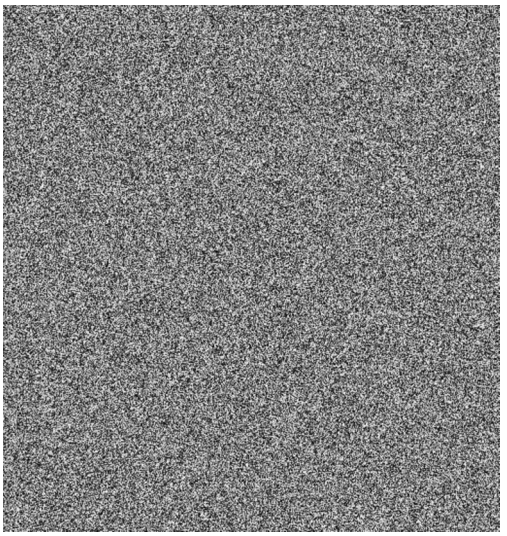
Fig. 6 Encrypted image using the chaotic Backer map algorithm: (a) The encrypted image and (b) the histogram.

4. Finally, the three encrypted images A, B, and C are compared.

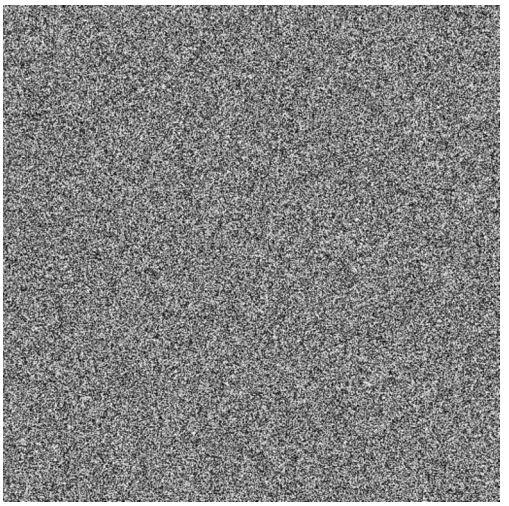
It is not easy to compare the encrypted images by simply observing them. Thus, for comparison, we can calculate the correlation coefficients between the corresponding pixels of the three encrypted images. The correlation coefficients for the three encrypted images A, B, and C are presented in Table 2. It is clear from Table 2 that no correlation exists among the encrypted images even though they have been produced using slightly different secret keys. Similar results are obtained using the RC6 algorithm, as shown in Figs. 8(a)–8(c). The results of the correlation coefficients are presented in Table 3.

For the homomorphic cryptosystem using the chaotic Baker map algorithm, we can perform the following steps:

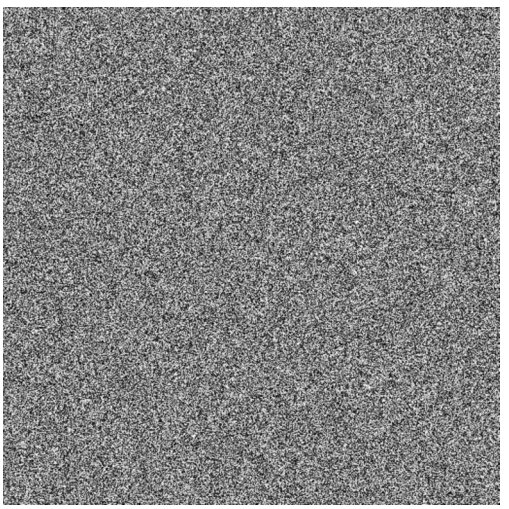
1. The original image in is encrypted using the secret key n=[10,5,12,5,10,8,14,10,5,12,5,10,8,14, 10, 5 , 12,5,10,8,14,10,5,12,5,10,8,14,10,5,12, 5 , 10 , 8,14,10 ,5 ,12 ,5,10,8,14,10,5,12,5,10,8, 14,10,5,12,5,10,8,14] 12,5,10,8,14,10,5,12,5, 10,8,14,10,5,12 , 5 ,10,8,14,10,5,12,5,10,8,14, 10,5 , 12 , 5,10,8 , 14,10,5,12,5,10,8,14]. And the resultant image is referred as the encrypted image A as shown in Fig. 9(a).
2. The same image is encrypted by making a slight modification in the secret key, i.e., n_1=[5, 5, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8,14]. Change is made in 10 to 5, 5 in the



(a)

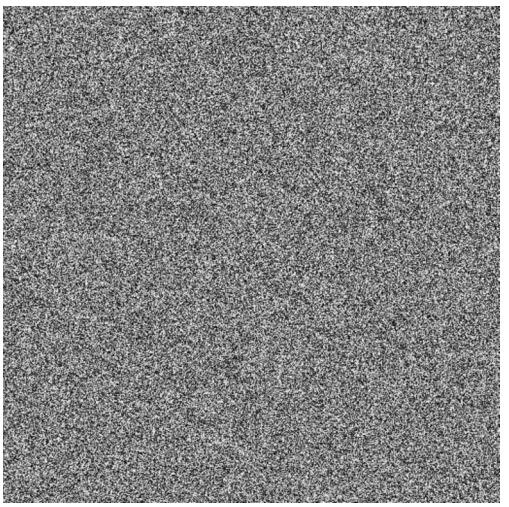


(b)

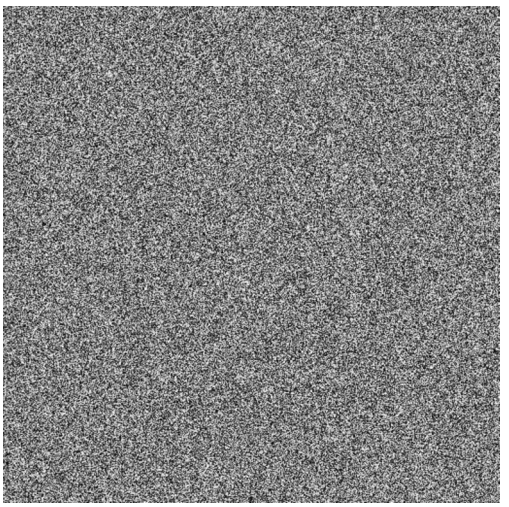


(c)

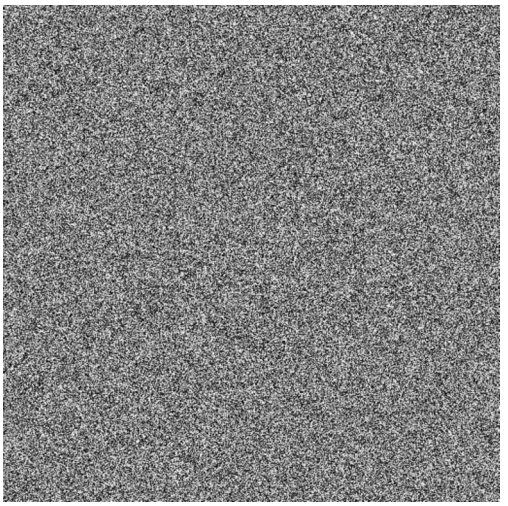
Fig. 7 Key sensitivity test of the homomorphic cryptosystem with the RC6 algorithm: (a) Encrypted image A with a key of 32 zeroes (hexadecimal), (b) encrypted image B with a key of 8 and 31 zeroes (hexadecimal), and (c) encrypted image C with a key of 31 zeroes and one (hexadecimal).



(a)

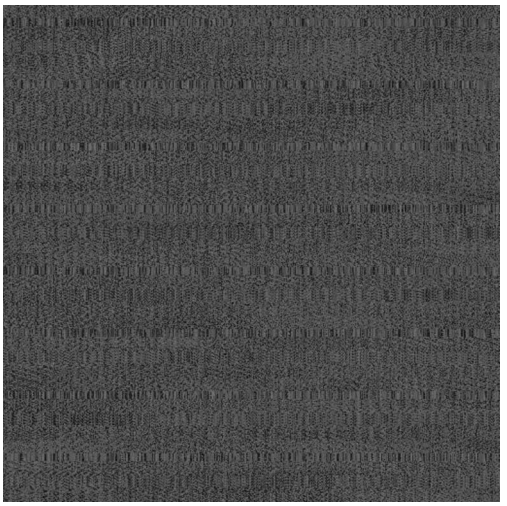


(b)

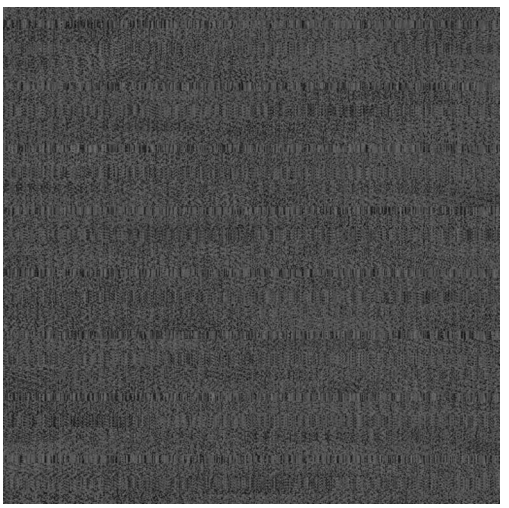


(c)

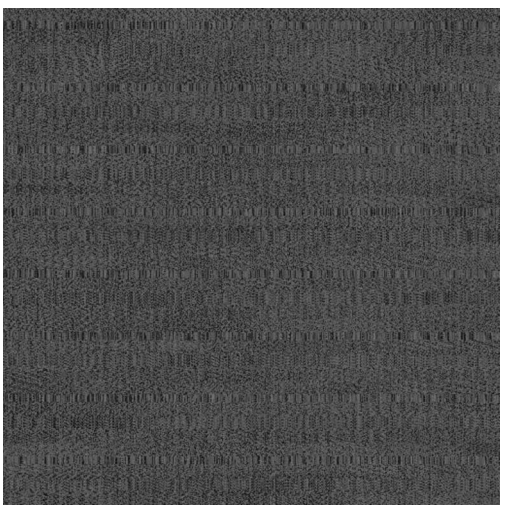
Fig. 8 Key sensitivity test of RC6 algorithm: (a) Encrypted image A with a key of 32 zeroes (hexadecimal), (b) encrypted image B with a key of 8 and 31 zeroes (hexadecimal), and (c) encrypted image C with a key of 31 zeroes and one (hexadecimal).



(a)

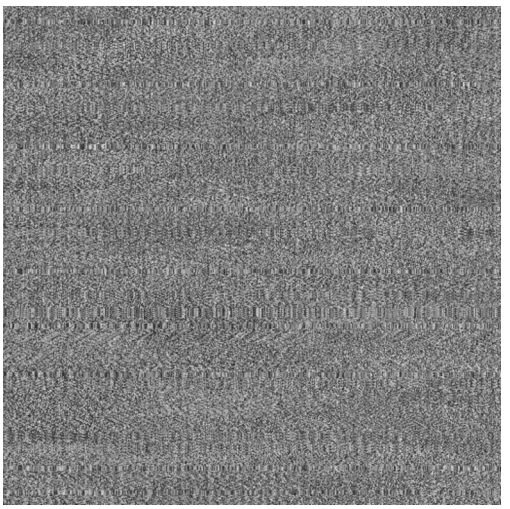


(b)

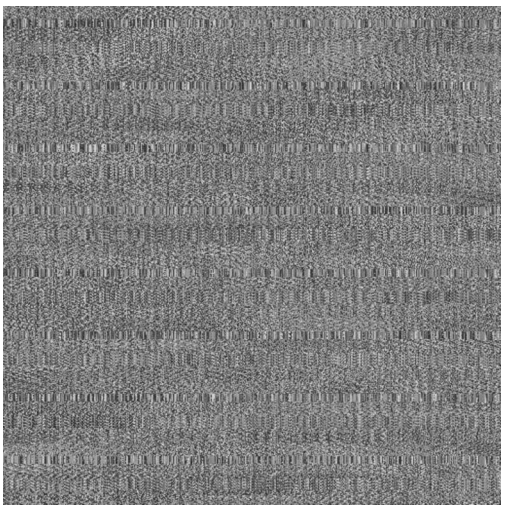


(c)

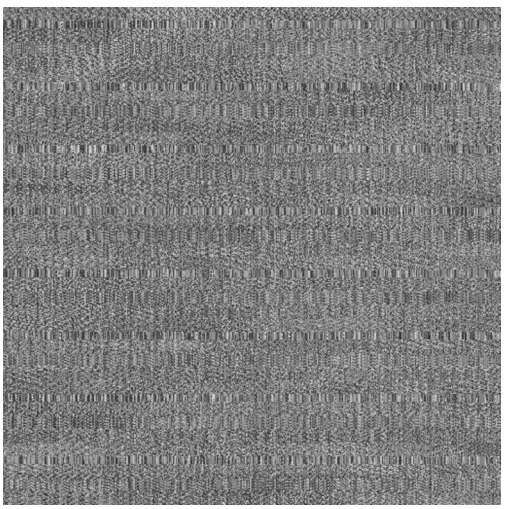
Fig. 9 Key sensitivity test of the homomorphic cryptosystem with the chaotic Baker map algorithm: (a) Encrypted image A with key n, (b) encrypted image B with key n_1, and (c) encrypted image (C) with key n_2.



(a)



(b)



(c)

Fig. 10 Key sensitivity test of the chaotic Backer map algorithm: (a) Encrypted image (A) with key n, (b) encrypted image B with key n_1, and (c) encrypted image C with key n_2.

Table 4 Results of the key sensitivity test for the homomorphic cryptosystem with the chaotic Baker map algorithm.

Image 1	Image 2	Correlation coefficient
Encrypted image A	Encrypted image B	0.9533
Encrypted image B	Encrypted image C	0.8761
Encrypted image C	Encrypted image A	0.9212

Table 5 Results of the key sensitivity test for the chaotic Baker map algorithm.

Image 1	Image 2	Correlation coefficient
Encrypted image A	Encrypted image B	0.3247
Encrypted image B	Encrypted image C	0.8762
Encrypted image C	Encrypted image A	0.2877

secret key. The resultant image is referred to as the encrypted image B as shown in Fig. 9(b).

3. Again, the same image is encrypted by making another slight modification in the secret key, i.e., $n_2 = [10,5,12,5,10,8,14,10,5,12,5,10,8,14,10,5,12,5,10,8,14,10,5,12,5,10,8,14,10,5,12,5,10,8,14,10,5,12,5,10,8,14,10,5,12,5,10,8,14,10,5,12,5,10,8,7,7]$

Change is made in 14 to 7, 7 in the secret key. The resultant image is referred to as the encrypted image C, as shown in Fig. 9(c).

4. Finally, the three encrypted images A, B, and C are compared.

The correlation coefficients between the corresponding pixels of the three encrypted images A, B, and C are tabulated in Table 4, from which it can be said that the correlation coefficients are worse than that obtained using the homomorphic cryptosystem with the RC6 algorithm. A similar result is obtained using only the chaotic Baker map encryption algorithm, as shown in Fig. 10(a)–10(c) and Table 5.

Another test for the key sensitivity of the proposed homomorphic image cryptosystem using the RC6 encryption algorithm is performed through the following steps:

1. A 512×512 image is encrypted using the secret test key of 32 zeroes.
2. The encryption key is changed by changing its LSB. The encrypting key is 31 zeroes and one.
3. The two ciphered images are compared.

The result is that the image encrypted by the key of 31 zeroes and one has differences in 99.6% of its positions from the image encrypted by the key 31 zeroes and one, although there is only one bit difference in the two keys.

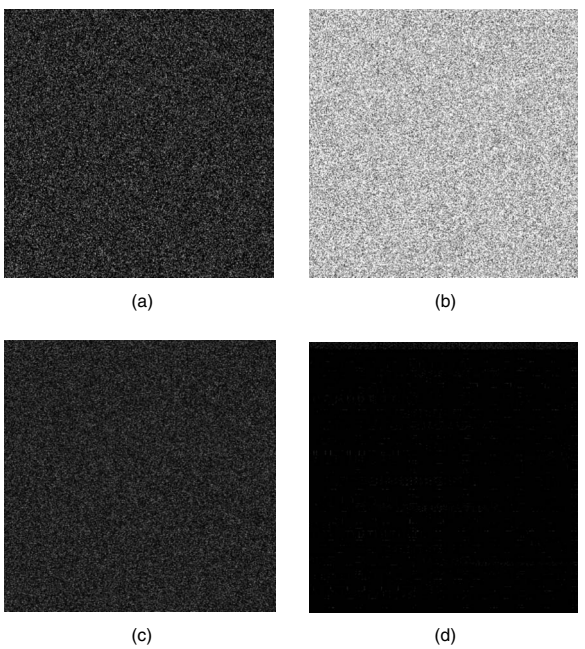


Fig. 11 Results of the difference test: (a) Difference image between the two ciphered images using the homomorphic cryptosystem with the RC6 algorithm, (b) difference image between the two ciphered images using the RC6 algorithm, (c) difference image between two ciphered images using homomorphic cryptosystem with the chaotic Baker map algorithm, and (d) difference image between two ciphered images using the chaotic Baker map algorithm.

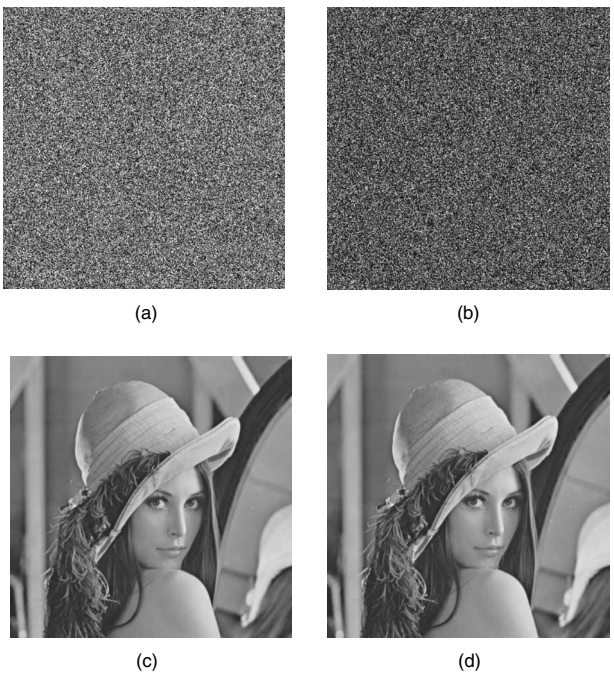


Fig. 12 Decrypted images for all encryption algorithms in the presence of noise with a signal-to-noise ratio of 50 dB. (a) The RC6 algorithm, (b) homomorphic cryptosystem with the RC6 algorithm, (c) chaotic Backer map algorithm, and (d) homomorphic cryptosystem with the chaotic Baker map algorithm.

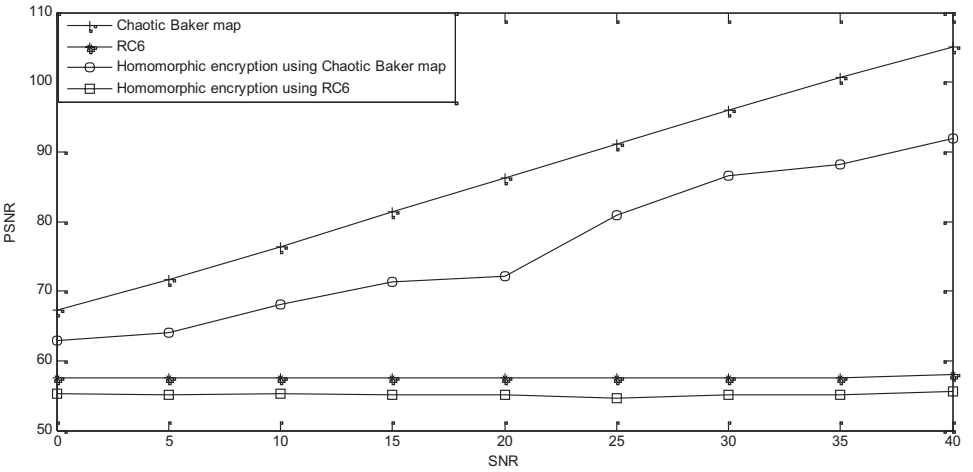


Fig. 13 Variation of the PSNR of the decrypted image with the SNR of the encrypted image for all encryption algorithms.

Figure 11(a) shows the difference image between the two ciphered images. This test is also applied to the RC6 encryption algorithm, and the result is shown in Fig. 11(b).

For the homomorphic image cryptosystem using the chaotic Baker map algorithm, the test is performed through the following steps:

1. A 512×512 image is encrypted using the secret test key n.
2. The encryption key is changed to n_1.
3. The two ciphered images are compared.

The result of this test is shown in Fig. 11(c). This test is also applied for the chaotic Baker map algorithm only, and the result is shown in Fig. 11(d).

4.4 *Differential Analysis*

A desirable property for the proposed Homomorphic cryptosystem is the high sensitivity to small changes in the plain image (single bit change in the plain image). In general, an opponent may make a slight change, such as modifying only one pixel of the original image, and then observing the change of the result. In this way, he may be able to find out a meaningful relationship between the plain image and the cipher image. If a minor change in the plain image can cause a significant change in the cipher image, then this differential attack would become very inefficient and practically useless.[29,30]

To test the influence of a one-pixel change on the whole image encrypted by the proposed homomorphic cryptosystem, two common measures may be used: the number-of-pixels change rate (NPCR) and the unified average changing intensity (UACI).[20,21,25] Let two ciphered images, whose corresponding plain images have only one-pixel difference, be denoted by C_1 and C_2. Label the gray-scale values of the pixels at grid (i,j) in C_1 and C_2 by $C_1(i,j)$ and $C_2(i,j)$, respectively. Define a bipolar array (D) with the same size as the images C_1 and C_2. Then, $D(i,j)$ is determined by $C_1(i,j)$ and $C_2(i,j)$. If $C_1(i,j)=C_2(i,j)$, then $D(i,j)=1$; otherwise, $D(i,j)=0$.

The NPCR is defined as

$$\mathrm{NPCR}=\frac{\Sigma_{i,j}D(i,j)}{WH}\times100\,\%\,, \tag{11}$$

where W and H are the width and height of C_1 or C_2. The NPCR measures the percentage of the number of different pixels to the total number of pixels between these two images.

The UACI is defined as

$$\mathrm{UACI}=\frac{1}{WH}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right]\times100\,\%\,, \tag{12}$$

It measures the average intensity of differences between the two images. A test is performed on the one-pixel change influence on the 256 gray-level Lena image of size 256×256, and the results are tabulated in Table 6.

With respect to the NPCR and UACI results in Table 6, the RC6 and chaotic Baker map encryption schemes have no sensitivity to small changes in the plain image, but the homomorphic cryptosystem using both schemes is highly sensitive to small changes in the plain image. Generally, these obtained results show that the proposed homomorphic cryptosystem has a very powerful diffusion mechanism.

5 Effect of Noise

The effect of noise on the proposed homomorphic image cryptosystem is studied in this section. The test results

Table 6 NPCR and UACI results.

Algorithms	NPCR	UACI
Homomorphic with RC6	0.395	16.775
RC6	99.9939	.0005
Homomorphic with chaotic Baker map	~=0	7.2314
Chaotic Baker map	~=100	~=0

shown in Figs. 12(a) and 12(b) reveal that the RC6 algorithm and the proposed homomorphic cryptosystem using the RC6 algorithm are very sensitive to noise. Thus, they are suitable for a noise-free environment. For the chaotic Baker map algorithm and the homomorphic cryptosystem using the chaotic Baker map algorithm, the results shown in Figs. 12(c) and 12(d) reveal that both algorithms are more robust to noise and can work in a noisy environment.

Figure 13 shows the variation of the peak signal-to-noise ratio (PSNR) of the decrypted image with the SNR of the encrypted image for all encryption algorithms. The performance of the RC6 algorithm and the proposed homomorphic cryptosystem using the RC6 algorithm get worse in the presence of noise. This is because the RC6 algorithm has a diffusion mechanism in its equation $f(x)=x(2x+1)(\mathrm{mod}2^w)$, which leads to a less noise immunity. The chaotic Backer map algorithm and the proposed homomorphic cryptosystem using the chaotic Baker map are more robust to noise.

6 Conclusions

A new homomorphic image cryptosystem is proposed and analyzed using several tests. Security analysis experimental results show that, taking into account the trade-off between attack expense and information value as well as other issues, such as operational speed, computational cost, and implementation simplicity, this kind of image cryptosystems will be very practical. This system has multilevels of security because encryption is performed in the homomorphic domain and because of the watermarking of the reflectance component by the illumination component of the image. This system has a very powerful diffusion mechanism (a small change in plain image makes a large change in cipher image). The homomorphic cryptosystem using the RC6 algorithm is more suitable for a noise-free environment. On the other hand, the homomorphic cryptosystem using the chaotic Baker map algorithm can work properly in a noisy environment.

References

1. National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication No. 46, U.S. Government Printing Office, Washington, DC (1977).
2. National Bureau of Standards, Data Encryption Standard Modes of Operation, Federal Information Processing Standards Publication No. 81, U.S. Government Printing Office, Washington, DC (1980).
3. R. L. Rivest, "The RC5 encryption algorithm," *Dr. Dobb's J.* **226**(3), 146–148 (1995).
4. J. Daemen and V. R. Rijndael, "The advanced encryption standard," *Dr. Dobb's J.* **26**(3), 137–139 (2001).
5. N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Opt. Lasers Eng.* **46**(2), 117–123 (2007).
6. G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos Appl. Sci. Eng.* **16**(8): 2129–2151 (2006).
7. S. C. Koduru, and V. Chandrasekaran, "Integrated confusion-diffusion mechanisms for chaos based image encryption" in *IEEE 8th Int. Conf. Computer and Information Technology Workshops*, pp. 260–263 (2008).
8. Y. B. Mao, G. Chen, and S. G. Lian, "A novel fast image encryption scheme based on the 3D chaotic baker map," *Int. J. Bifurcation Chaos Appl. Sci. Eng.* **14**(10), 3613–3624 (2004).
9. E. Bradley, "Autonomous exploration and control of chaotic systems," *IEEE Trans. Syst. Man Cybern.* **26**(5), 499–519 (1995).
10. J. Fridrich, "Secure image ciphering based on chaos," Final report (April, 1997).
11. G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons Fractals* **21**(3), 749–761 (2004).
12. J. S. Lim, *Two-Dimensional Signal and Image Processing*, Prentice Hall, Englewood Cliffs, NJ (1990).
13. S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic encryption scheme for real-time digital video," *Proc. SPIE* **4666**, 149–160 (2002).
14. S. Lee, J. Wook Han, and D. Seo, "Optical encryption and decryption using personal fingerprint image," presented at the 6th Int. at Conf. on Advanced Communi. Technol., Vol. 1, pp. 413–415 (2004).
15. B. Schneier, *Applied Cryptography—Protocols, algorithms, and source code in C*, 2nd ed., Wiley, Hoboken, NJ (1996).
16. H. E. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images," *Int. J. Comput. Inf. Sys. Sci. Eng.* **1**(1), 33–39 (2007).
17. R. L. Fivest, M. J. B. Robshad, R. Sidney, and Y. L. Yin, "The RC6 block cipher," MIT Laboratory for Computer Science, Cambridge, MA, and RSA Laboratories, San Mateo, CA (1998).
18. J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos Appl. Sci. Eng.* **8**(6), 1259–1284 (1998).
19. J. Peng, S. Jin, G. Chen, Z. Yang, and X. Liao, "An image encryption scheme based on chaotic map," presented at the 4th Int. Conf. on Natural Computation, Vol. 4, pp. 595–599 (2008).
20. S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, Chap. 4, CRC Press, Boca Raton, FL (2004).
21. N. El-Fishawy and O. M. Abu Zaid, "Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms," *Int. J. Network Security* **5**(3), 241–251 (2007).
22. Y. Zhai, S. Lin, and Q. Zhang, "Improving image encryption using multi-chaotic map," presented at *Workshop on Power Electronics and Intelligent Transportation System*, pp. 143–148 (2008).
23. C. E. Shannon, "Communication theory of secrecy system," *Bell Syst. Tech. J.* **28**, 656–715 (1949).
24. Y. B. Mao and G. Chen, "Chaos-based image encryption," in *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neuralcomputing and Robotics*, E. Bayro, Ed., pp. 231–265 Springer-Verlag, Berlin (2005).
25. C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *J. Syst. Softw.* **58**, 83–91 (2001).
26. C. Alexopoulos, N. Bourbakis, and N. Ioannou, "Image encryption method using a class of fractals," *J. Electron. Imaging* **4**(3), 251–259 (1995).
27. C. J. Kuo, "Novel image encryption technique and its application in progressive transmission," *J. Electron. Imaging* **2**(4), 345–351 (1993).
28. H. K. C. Chang and J. L. Liu, "A linear quadtree compression scheme for image encryption," *Signal Process. Image Commun.* **10**(4), 279–290 (1997).
29. A. Sinha and K. Singh, "A technique for image encryption using digital signature," *Opt. Commun.* **21**(8), 229–234 (2003).
30. H. El-din, H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption," *Informatica* **31**(1), 121–129 (2007).

Ibrahim F. Elashry graduated from the Faculty of Engineering, Kafrelshiekh University, Egypt in 2007. He is now a teaching assistant and MSc student. His interest is in security over wired and wireless networks and image processing.

Osama S. Farag Allah received his BS in 1997, MSc in 2002, and PhD in 2007, all in computer science and engineering, from Menoufia University, Faculty of Electronic Engineering, Egypt. He was a demonstrator at the Department of Computer Science and Engineering, at Menoufia University, from 1997 to 2002, became an assistant lecturer in 2002, and was promoted to a lecturer in 2007. His research interests cover computer networks, network security, cryptography, Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, and chaos theory.

Alaa M. Abbas received his BSc, MSc, and PhD in electrical engineering from Menoufia University, Egypt, in 1996, 2001, and 2008, respectively. He is currently a lecturer in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His areas of interest are digital signal processing, image processing, motion estimation, pattern recognition, and face detection and recognition.

S. El-Rabaie received the BSc (with Honors) in radio communications from Tanta University, Egypt, 1976, MSc in communication systems from Menoufia University, Egypt, 1981, and a PhD in microwave device engineering from the Queen's University of Belfast in 1986. He Was a postdoctoral fellow in the Queen's University Department of Electronic Engineering until 1989. In 1992, he was a Research Fellow at the North Arizona University, College of Engineering and Technology, and in 1994 he served as a visiting professor at Ecole Polytechnique de Montreal, Quebec, Canada. Prof. El-Rabaie has authored and coauthored more than 70 papers and technical reports, and 15 books. In 1993, he was awarded the Egyptian Academic Scientific Research Award (Salah Amer Award of Electronics), and in 1995, he received the Award of Best Researcher on CAD from Menoufia University. He is now the vice dean of postgraduate studies and research, Faculty of Electronic Engineering, Menoufia University.

Fathi E. Abd El-Samie received his BSc, and MSc, and PhD in electrical engineering from Menoufia University, Egypt, in 1998, 2001, and 2005, respectively. He is currently a lecturer in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He received the most cited paper award from *Digital Signal Processing Journal* in 2008. His areas of interests are signal processing, image enhancement, restoration, super resolution and interpolation, and digital communications.