Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 341729, 10 pages
http://dx.doi.org/10.1155/2015/341729

Research Article

Image Encryption Algorithm Based on Chaotic Economic Model

S. S. Askar,[1,2] A. A. Karawia,[2] and Ahmad Alshamrani[1]

[1]*Department of Statistics and Operations Researches, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia*
[2]*Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt*

Correspondence should be addressed to S. S. Askar; s.e.a.askar@hotmail.co.uk

Received 18 November 2014; Revised 23 December 2014; Accepted 24 December 2014

Academic Editor: Wang Xing-yuan

In literature, chaotic economic systems have got much attention because of their complex dynamic behaviors such as bifurcation and chaos. Recently, a few researches on the usage of these systems in cryptographic algorithms have been conducted. In this paper, a new image encryption algorithm based on a chaotic economic map is proposed. An implementation of the proposed algorithm on a plain image based on the chaotic map is performed. The obtained results show that the proposed algorithm can successfully encrypt and decrypt the images with the same security keys. The security analysis is encouraging and shows that the encrypted images have good information entropy and very low correlation coefficients and the distribution of the gray values of the encrypted image has random-like behavior.

1. Introduction

Up-to-date development and progress in the means of multimedia industry and the ways of communications have made researches focus on creating new schemes to enhance security of transmission and storing multimedia data over open channels including the internet and wireless networks. One of the challenges that researchers face nowadays is how to protect in a confidential manner a secure route for the transmission of multimedia data through digital networks. Due to the spread of the advances of new technologies in networks, people from all over the world can send and receive information, perform projects, and communicate with friends by sending images and videos through the internet. Sending and receiving such information using images and videos via internet and other networks require some kind of secure routes. That is because images and videos may incorporate secret or sensitive information such as patients' medical surveys, personal information, high expensive marketable designs, and secret manuscripts.

It has been reported in literature [1–4] that an encryption tool is an effective approach to protect such information when sending and receiving data through multiple ways of communications. This is because the only one who can decrypt and see such information is the only authorized entities that have security keys of decryption. In an encryption process, the security keys are the core of any encryption and decryption algorithm. They are used to convert the data from a readable state to an apparent nonsense and vice versa. The designer of an encryption scheme should share the security keys needed to recover the original information with intended recipients and consequently other unwanted individuals can be precluded [5–7].

Recently, the theory of mathematics and programming languages have been used intensively in modern cryptography; cryptographic algorithms are built based on computational and complex assumptions by which breaking such algorithms in practice by any adversary is very hard [8–12]. The high efficiency of any cryptographic algorithm is the most important criterion by which the robustness of encryption is measured. For instance, the data encryption standard (DES) as a traditional algorithm [13, 14] faces problems when used to encrypt large images and therefore its efficiency becomes low and weak. Other traditional encryption algorithms such as international data encryption algorithm (IDEA) require a large computational time and super computers when used in encrypting real time images [14]. Cryptographic algorithms that use less time are much

more preferable for encrypting such real time images. In addition, some encryption schemes may be run very slowly and this increases the degree of security features yet they would be of little use when dealing with real time images.

Chaos theory has been raised in different fields of physics, engineering, biology, and economy in the past two decades. Since the 1990s, many researches and scientists have done extensive studies in the chaotic systems emanated from this theory. Due to such studies, researchers have come up with the fact that there is a close relationship between cryptography and chaos. Chaotic systems such as logistic and other systems have got much attention and have been applied in the process of encryption [7]. What makes the encryption algorithms based on such systems more robust and reliable than other algorithms is the complex properties of such chaotic systems. Such complex properties can be summarized as sensitivity to the initial conditions of the systems' parameters, nonperiodicity of systems' equilibrium states, the topological transitivity of the systems' behaviors, and the pseudorandom property. Since the appearance of the first algorithm in images' encryption that entirely depended on chaos by Matthews [1], many chaos-based encryption algorithms of images have been introduced in literature. Some of those cryptosystems have used one or several dimensional maps such as baker's and cat's maps serving the purpose of encryption of images [2–7]. Wang et al. [8] have used an extension of fractal Fourier transformation and a digital holographic scheme to propose a cryptographic algorithm. Due to the parameters used in this scheme, enhancement security of the encryption process has been provided. Furthermore, many cryptographic algorithms have adopted popular chaotic models that represent chaos by using mathematical models such as logistic map, Lorenz map, Henon map, and Rössler attractor. Lorenz map is characterized by its attractor having two nonlinear terms while in Rössler attractor there is only one nonlinear term and this makes the complexity of Lorenz attractor and its chaos higher than those in Rössler attractor. Other algorithms have divided the images into several blocks and tried to define a permutation for each block using a logistic map to encrypt the original image.

Other chaotic image encryption algorithms that incorporate several parameters and work under frequency domain are more powerful in the encryption procedures because of the strength of the security provided by such algorithms [9–14]. Kuo has introduced a novel image encryption method in [9]. The way this method works is by making a random change in the phase spectra of the original image. This can be done by using a pseudonoise image with binary phase spectra embedded in the phase spectra of the original image. This methodology of adding such noise is actually a security key system. With this methodology, a part of the encrypted image with such noise can be used to obtain a full recovery of the original image without any drawbacks. Therefore, encryption algorithms based on such noise are more suitable for secure transmission of data through different ways of communications. This is due to the ability of the algorithms to recover the original image to some extent with partial access to the encrypted image. In [15], a high-dimensional Lorenz chaotic system with perceptron model within a neural network has been introduced. Liu and Wang [16] have designed a stem-cipher algorithm using the piecewise linear chaotic map as a generator of a pseudorandom key stem sequence in order to robust the security and improve the dynamic degradation. Furthermore, in order to get a robust security, Liu and Wang [17] proposed a bit-level permutation with a high-dimensional chaotic map in order to encrypt color image. A novel color image encryption algorithm based on chaos has been proposed by Wang et al. [18]. In [19], the potential flaws of Zhu's algorithm have been analyzed. Zhang and Wang have proposed an encryption algorithm based on a spatiotemporal chaos of the mixed linear-nonlinear coupled map lattices [20]. Based on spatiotemporal nonadjacent coupled map lattices, Zhang and Wang [21] have proposed an encryption algorithm.

Chaotic economic systems such as monopoly and duopoly are sophisticated systems on which the chaos that occurs in them is more difficult than those found in Lorenz, logistic, and Rössler. In [22], the author has introduced a new Cournot duopoly model on which an unknown demand function without inflection points has been studied. This model has shown complex dynamical properties such as hard bifurcation and bad chaos. In comparison with logistic and other models, the Cournot model can be used extensively in the encryption scheme and thus strength cryptographic algorithm can be presented. To the reader's knowledge, such chaotic economic models have not been used in literature before. Other chaotic economic systems can be found elsewhere [23–28] that are suitable in the encryption process for many reasons as they share some characteristics with cryptography. Of these reasons is that they have much more security keys, sensitive dependence to the initial conditions, hard bifurcation, and bad chaos. Nonlinear dynamical systems are characterized by their complex behavior such as bifurcation and chaos. The real-life applications originated by those systems have been extensively investigated. These applications may be classified into two parts: man-made applications and other applications simulated from nature. Due to the complex behavior of those applications which results because of chaos, several cryptographic techniques have been proposed and discussed in literature in the last two decades [29–33]. In [34], a detailed survey on chaotic cryptographic techniques has been elaborately reported. A hyperchaotic map has been used in [29] in order to encrypt and decrypt images in such a manner that the security of breaking the encryption is very difficult. What makes the encryption process difficult in this algorithm is that in the algorithm a permutation of the image that needs to be encrypted is done by an ergodic matrix of a hyperchaotic sequence. In [30], new novel image encryption and decryption techniques have been introduced. The Poker shuffle approach has been used to control the process of encryption. Multi-chaotic systems have been used to encrypt color images in [31]. In this study, four chaotic maps have been incorporated in the encryption scheme. The authors in [31] have used the so-called Henon map in encrypting a gray image. In this algorithm, the Arnold cat map is combined with Henon map in order to shuffle the pixels' position of an image and hence an encrypted image is yielded. More

papers on different types of cryptographic techniques that use chaotic systems in the encryption process can be found in [35–41].

The proposed algorithm covers many challenges which can be addressed as follows. (1) Robust images encryption and decryption techniques: an encryption algorithm can be used to convert the data into a strong encrypted file and therefore secure transmission of them via different sort of nowadays communications. This will save the data from unauthorized people and intentionally reduce the quality of perception. (2) Algorithmic code: the algorithmic steps of the encryption and decryption scheme should be prepared in a way that facilitates handling compressed format of multimedia. Based on that the encrypted and decrypted files will be modified without any crashing or damages. (3) Time complexity: many algorithms face problems when dealing with large multimedia data. It is important for cryptographic algorithms to overcome this disadvantage and speed up the behavior of the algorithm. One way to do that is to try to encrypt important parts of the multimedia data in such a way that makes the inverse process of encryption very quick without any crashing. (4) Chaotic economic systems: introducing new chaotic economic systems with hard bifurcation and bad chaos is obligatory in order to get a robust encryption algorithm. This is the motivation of our proposed paper. It is shown in literature that no one has used such systems in the encryption scheme; however, they can be used to introduce strong encryption and decryption techniques. Some of those systems can be found elsewhere [42–49].

The paper is organized as follows. In Section 2, the chaotic economic map is presented. In Section 3, the algorithmic steps of our proposed algorithm are outlined. Some experimental results are obtained in Section 4 and then some conclusion is given in Section 5.

2. Chaotic Economic Map (CEM)

In literature, it is known that the logistic map $x_{n+1} = \alpha x_n(1 - x_n)$, where $\alpha \in (0, 4)$ and $n = 0, 1, 2, \ldots$, is a one-dimensional discrete chaotic map. It has been used recently as a scheme for the process of images encryption. Its parameter α represents the key security in the encryption process. This parameter has a great impact on the complex behavior of this map. It is reported that when $\alpha \in (0, 3)$ with certain initial value of x_0, the equilibrium point of the map becomes asymptotically stable and hence cannot be used in encryption. In $\alpha \in [3, 3.6)$, the map will behave periodically and therefore very weak encryption can be raised. Chaotic behavior of the map can be found in $\alpha \in [3.6, 4)$ with periodicity disappearing. In the latter case however the chaos exists but the encryption scheme based on this map with $\alpha \in [3.6, 4)$ is still weak. This weakness is due to the small key security this map is based on. To overcome this limitation, we suggest the following proposed map:

$$x_{n+1} = x_n + k\left[a - c - b(1 + \gamma)x_n^{\gamma}\right]. \quad (1)$$

Equation (1) is a nonlinear chaotic economic map that incudes six important parameters. The parameter $a > 0$ captures the size of the market demand while $b > 0$ represents the slope of the market price. The parameter $c \geq 0$ is a fixed marginal cost and $k > 0$ is called the speed of adjustment parameter. $\gamma \in \mathbb{R}$ is a constant. The chaotic behavior of the map is shown in Figure 1 at $\gamma = 3, 4, 5$, respectively, and $a = 4$, $b = 0.6$, and $c = 0.5$. It is clear that the proposed map includes periodic windows in the third case which in turn make the map unsuitable for the encryption scheme. These windows can be eliminated using different values for the map's parameters as we will see in the correlation analysis.

Map (1) is more difficult in comparison with the logistic map since it contains 6 security keys. As one can see from Figure 1, the map exhibits a period doubling route to chaos.

3. Encryption Algorithm Based on CEM

The proposed image encryption algorithm in this paper is based on the CEM map. It depends on creating a chaotic sequence by the CEM $(x_1, x_2, \ldots, x_{200})$ map to encrypt the image data. The elements in this sequence consist of decimal fractions numbers while the image consists of pixels. Therefore, a function is required to transfer the fraction decimals to integers. Then, the plain image can be encrypted using the new integers sequence. The algorithmic steps can be outlined as follows.

(i) *Step 1.* Import a color image and then convert it to gray scale image (Gimage) of size $M \times N$.

(ii) *Step 2.* Set the initial condition x_0 and the keys k_1, a, c, b, γ and generate the chaotic sequence $\{x_1, x_2, \ldots, x_{200}\}$ using the CEM map.

(iii) *Step 3.* Calculate a_{ij}, $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$, using $a_{ij} = x_{\text{new}}$ and $x_{\text{new}} = x_{\text{old}} + k_1[a - c - b(1 + \gamma)x_{\text{old}}^{\gamma}]$, $x_{\text{old}} = x_{201}$.

(iv) *Step 4.* Set initials for k_2 and x_{old}.

(v) *Step 5.* Calculate b_{ij}, $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$, using $b_{ij} = x_{\text{new}}$ and $x_{\text{new}} = x_{\text{old}} + k_2[a - c - b(1+\gamma)x_{\text{old}}^{\gamma}]$.

(vi) *Step 6.* Set initials for k_3 and x_{old}.

(vii) *Step 7.* Calculate c_{ij}, $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$, using $c_{ij} = x_{\text{new}}$ and $x_{\text{new}} = x_{\text{old}} + k_3[a - c - b(1+\gamma)x_{\text{old}}^{\gamma}]$.

(viii) *Step 8.* Preprocess $a_{ij} = 10^6 a_{ij} - \text{floor}(10^6 a_{ij})$; $b_{ij} = 10^6 b_{ij} - \text{floor}(10^6 b_{ij})$; $c_{ij} = 10^6 c_{ij} - \text{floor}(10^6 c_{ij})$.

(ix) *Step 9.* Set initial conditions for t, w_0, w_1, w_2 and calculate w using $w = w_0(1 - t)^2 + 2w_1 t(1 - t) + w_2 t^2$.

(x) *Step 10.* Calculate p_{ij} using $p_{ij} = (w_0 a_{ij}(1 - t)^2 + 2w_1 b_{ij} t(t - 1) + w_2 c_{ij} t^2)/w$, $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$.

(xi) *Step 11.* Calculate $e = \text{round}(255 \times p_{ij})$.

(xii) *Step 12.* Get the encrypted image using CEM $= t \times$ Gimage $+ (1 - t) \times e \bmod 256$, $t \in (0, 1)$.

(xiii) *Step 13.* End.

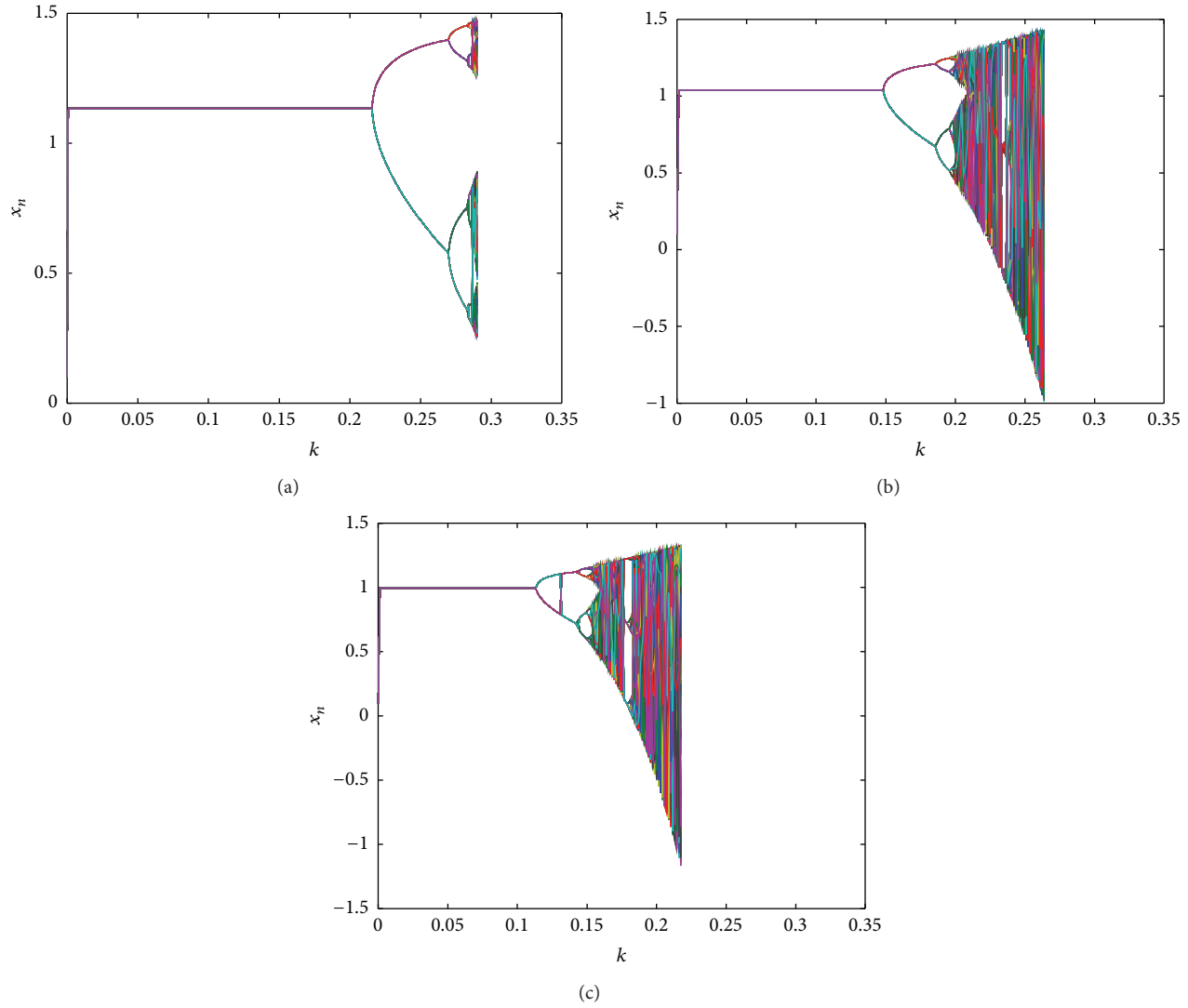


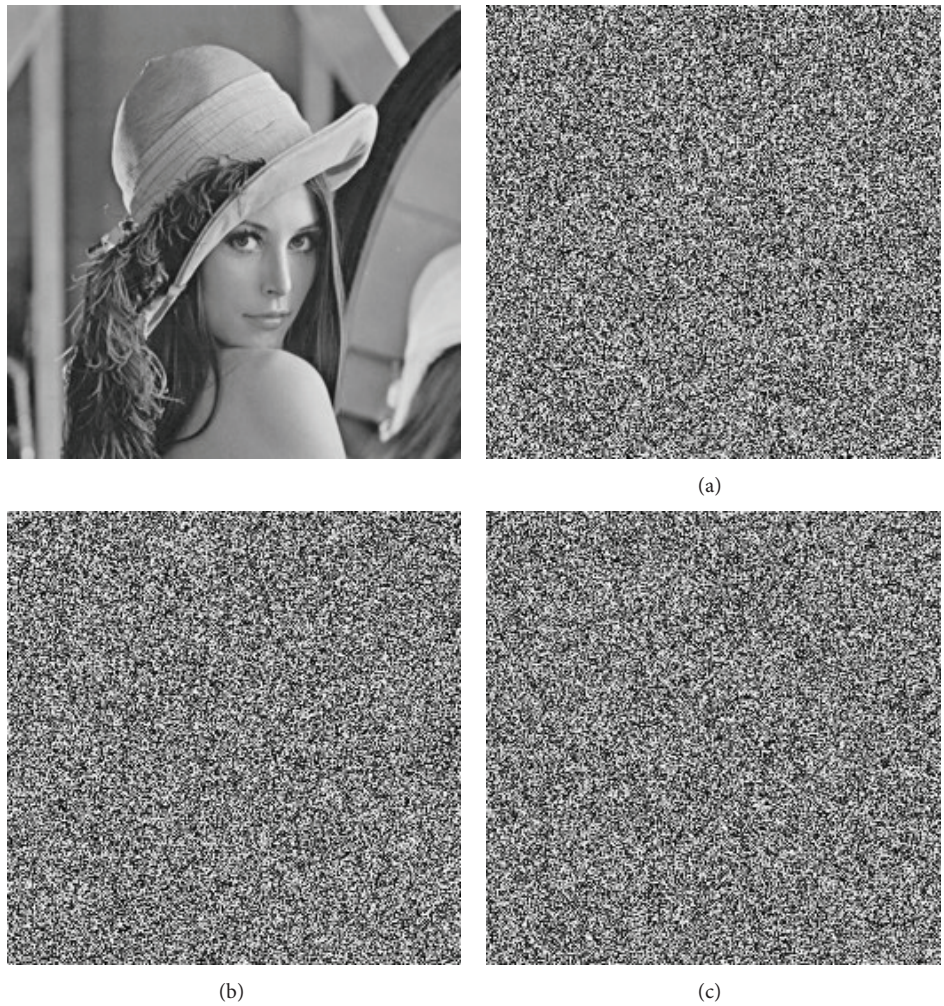
FIGURE 1: The chaotic behavior of the map (1) at $\gamma = 3, 4, 5$ and $a = 4$, $b = 0.6$, $c = 0.5$, $x_0 = 0.1$, $k \in [0, 0.3]$.

4. Experimental Results

In this section, the algorithm is applied with some different cases using the same image to illustrate its performance. The popular image known as Lena is used as a plain image in this experiment. It is shown in Figure 2 as a 256-gray-scale Lena plain image of size 256×256. Figure 2(a) presents its encrypted image using the encryption keys $\gamma = 3$ and $a = 4$, $b = 0.6$, $c = 0.5$, $x_0 = 0.1$, $k \in [0, 0.3]$. As one can see, the encrypted image is rough and entirely unknowable. According to these keys, the encrypted image is rough in comparison with the encrypted one on which the logistic map was used.

The reason is that the proposed algorithm uses many security keys in comparison with the logistic map and furthermore the bifurcation in the economic model used is much harder than those in the logistic map. Figures 2(b) and 2(c) show an encryption for the same image with the same keys but $\gamma = 4, 5$. These two cases are much more complicated than the previous case where $\gamma = 3$.

Figure 3(a) provides the histogram of the encrypted image at the parameters $a = 4$, $b = 0.6$, $c = 0.5$, $x_0 = 0.1$, and $\gamma = 3$ while Figure 3(b) shows the histogram of the original Lena image. It is clear that the two histograms are entirely different. Figure 3(a) shows uniformity distribution of gray scale of the encrypted image that is much different from the histogram of the plain image. The histogram distribution of the encrypted image shown in Figure 3(a) demonstrates that the proposed encryption algorithm has covered up all the characters of the plain image and shows a good balance property. The encrypted image does not provide any information about the original image for whom they are interested in breaking such kind of encryption. Figures 3(c) and 3(d) show the histograms for the image at the same parameters but $\gamma = 4$ and $\gamma = 5$. As in Figure 3(a), those histograms present good cover of the characteristics of



(a)

(b) (c)

Figure 2: Encryption results: plain image and encrypted image at $a = 4$, $b = 0.6$, $c = 0.5$, $x_0 = 0.1$, $k \in [0, 0.3]$ and (a) $\gamma = 3$, (b) $\gamma = 4$, and (c) $\gamma = 5$.

the plain image and hence the proposed algorithm provides a robust resistance against any type of attacks.

4.1. Key Sensitivity Analysis. The cryptographic system used in this paper consists of six different parameters that are a, b, c, x_0, k, and γ. Those parameters can be used as secret keys of encryption and decryption process. A cryptographic system should be sensitive to all these keys and hence a robust cryptographic system must be sensitive to any small change in one or all secret keys. Our algorithm is very sensitive to any small change in one of all the keys. If one takes $\gamma = 3.99\cdots$ in the second case then the obtained decrypted image will be completely different from the plain image. Figure 4(a) shows the decrypted image of the original one using the correct security keys. It is easy to see that the decrypted image and its histogram shown in Figure 4(b) are exactly the same as the plain image and its histogram. Therefore, the proposed algorithm is successful in decrypting the plain image using the correct security keys without losing any information of the characteristics of the plain image. The key space of the proposed algorithm is 10^{84} if the security parameters have the precision of 10^{-14}. This means that our algorithm possesses a large enough key space as in [21] to prevent any brute-force attacks. Therefore, the proposed encrypted algorithm is good at resisting brute-force attacking.

Figure 4(c) shows that when one changes a little one of the security keys, that is, $\gamma = 3.99999999999999$, the decrypted image becomes miserable and entirely different from the plain image shown in Figure 4(a). Furthermore, the decrypted image appears like a black one and therefore the proposed algorithm cannot be broken by hackers and also is very sensitive to any little changes in the security keys. For the other two cases, similar results are obtained.

4.2. Correlation Analysis. In order to evaluate the encryption quality of the proposed algorithm, the correlation coefficient is used. It is important to calculate the correlation coefficients of two adjacent pixels of the encrypted image through

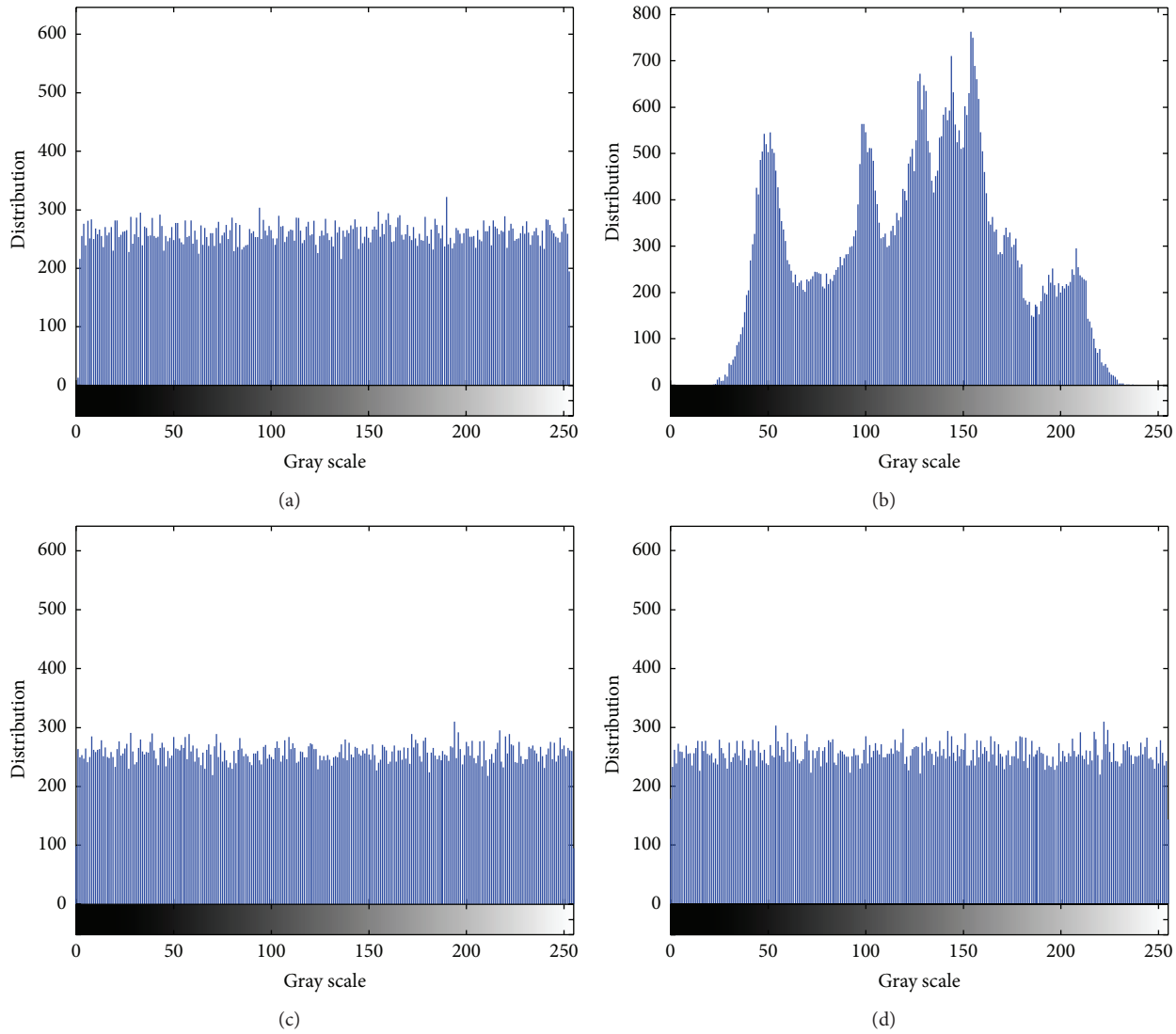


Figure 3: Histograms of plain image and encrypted image at $a = 4$, $b = 0.6$, $c = 0.5$, $x_0 = 0.1$, $k \in [0, 0.3]$ and (a) $\gamma = 3$, (b) plain image, (c) $\gamma = 4$, and (d) $\gamma = 5$.

horizontal, vertical, and diagonal directions. To do that, we use the following relations [2]:

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

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{2}$$

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

where $E(x)$ is the estimation of the mathematical expectation of x, $D(x)$ is the estimation of the variance of x, and $\operatorname{cov}(x, y)$ is the estimation of the covariance between two gray scale x and y values of two adjacent pixels in the image. One thousand pairs of adjacent pixels have been randomly selected and their correlation coefficients are separately calculated in three directions: vertical (V), horizontal (H), and diagonal (D). For the plain image, the correlation coefficients among the adjacent pixels in those directions are close to 1. This means that the adjacent pixels are highly correlated to each other. On the other hand, the correlation coefficients of the encrypted image are close to 0 and hence the adjacent pixels in the encrypted image are entirely uncorrelated to each other. Ideally, there should not be any relation between the adjacent pixels in the encrypted image in the three directions and this is what is observed from the results obtained using the proposed algorithm. The correlation coefficients of the plain and the encrypted images for some key values are shown in Tables 1, 2, and 3 while Table 4 presents existing results in literature. As one can see, the absolute values of

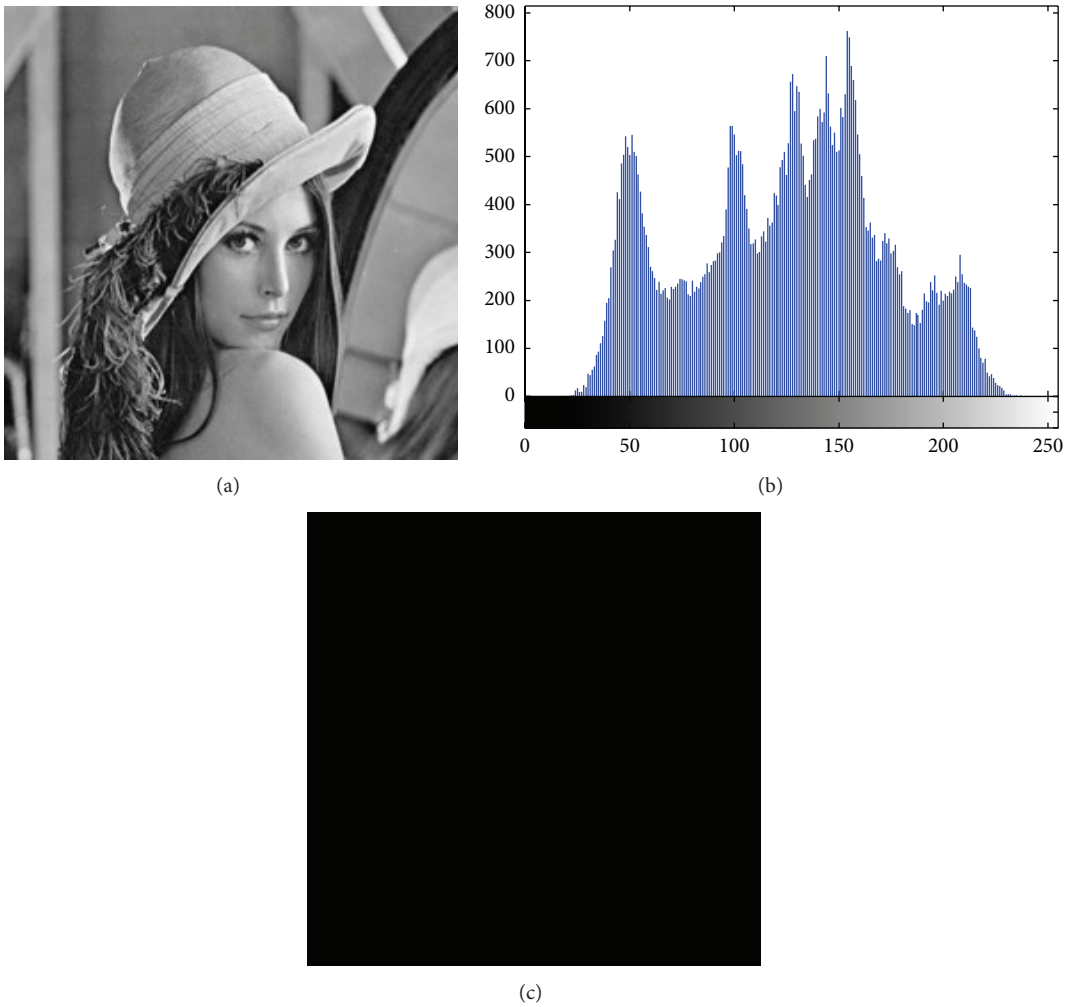


Figure 4: Decrypted results (a) at $a = 4, b = 0.6, c = 0.5, x_0 = 0.1, k \in [0, 0.3], \gamma = 4$, (b) histogram of (a), and (c) decrypted image at $a = 4, b = 0.6, c = 0.5, x_0 = 0.1, k \in [0, 0.3], \gamma = 3.99999999999999$.

Table 1: Correlation coefficients of two adjacent pixels in plain and encrypted images at $a = 4, b = 0.6, c = 0.5, x_0 = 0.1, k \in [0, 0.3]$.

	Plain image	Using logistic map	Case I ($\gamma = 3$)	Case II ($\gamma = 4$)	Case III ($\gamma = 5$)
H	0.9660	−0.0145	0.0122	0.0075	−0.0038
V	0.9395	−0.0060	−0.0456	−0.0079	0.0093
D	0.9191	0.0102	−0.0188	−0.0093	−0.0189

the correlation coefficients in the proposed algorithm are close to those in Zhang's algorithm and better than those of Hongjun algorithm.

4.3. Analysis of Information Entropy. In this subsection, information entropy analysis is carried out to show the distribution of the gray values. One can use in this analysis the well-known formula for calculating entropy as follows [40]:

$$H(s) = -\sum_{i=1}^{N-1} p(s_i)\log_2 p(s_i), \quad (3)$$

Table 2: Correlation coefficients of two adjacent pixels in plain and encrypted images at Case I: $a = 5, b = 0.6, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, Case II: $a = 5, b = 0.1, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, and Case III: $a = 5, b = 0.2, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$.

	Plain image	Case I ($\gamma = 3$)	Case II ($\gamma = 4$)	Case III ($\gamma = 5$)
H	0.9660	−0.0122	−0.0067	−0.0092
V	0.9395	−0.0270	0.0140	−0.0134
D	0.9191	−0.0084	−0.0012	0.0121

where $p(s_i)$ is the probability of symbol s_i and the entropy is expressed in bits. It is reported elsewhere [30] that the ideal entropy value for an encrypted image should be 8. This means that the more the distribution of a gray value is uniform, the greater the information entropy becomes. Therefore, a value below 8 would give a possibility of breaking the image security of the encrypted image. Our analysis shows that the results obtained are close to the ideal value 8. This indicates that the rate of information leakage in the proposed algorithm

Table 3: Correlation coefficients of two adjacent pixels in plain and encrypted images at Case I: $a = 4, b = 0.6, c = 0.5, x_0 = 0.1, k \in [0, 0.3]$, Case II: $a = 5, b = 0.1, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, and Case III: $a = 5, b = 0.2, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$.

	Plain image	Case I ($\gamma = 0.3$)	Case II ($\gamma = 4.1$)	Case III ($\gamma = 0.1$)
H	0.9660	0.1088	−0.0165	−0.0179
V	0.9395	0.0241	0.0241	−0.0205
D	0.9191	0.3093	0.0186	0.0197

Table 4: Correlation coefficients of two adjacent pixels in plain and encrypted images.

	Plain image	Zhang and Wang [21]	Plain image	Liu and Wang [17]
H	0.969679241	0.0024	0.9230	−0.0035
V	0.987698390	−0.0007	0.9271	−0.0574
D	0.967310389	0.0012	0.9847	0.0578

Table 5: Information entropy of image at $a = 4, b = 0.6, c = 0.5, x_0 = 0.1, k \in [0, 0.3]$.

Image	Information entropy
Plain image	7.4467
Using logistic map	7.9940
Case I ($\gamma = 3$)	7.9754
Case II ($\gamma = 4$)	7.9947
Case III ($\gamma = 5$)	7.9961

Table 6: Average ciphering speed of different sized colored images at Case I: $a = 5, b = 0.6, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, Case II: $a = 5, b = 0.1, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, and Case III: $a = 5, b = 0.2, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$.

Image size (in pixels)/ average time (s)	Case I ($\gamma = 3$)	Case II ($\gamma = 4$)	Case III ($\gamma = 5$)
256×256	0.1825	0.1915	0.1868
512×512	1.0832	1.1016	1.1453
1024×1024	7.3967	7.8270	7.6266

is negligible and the encrypted image using our algorithm is secure against any kind of entropy attack. The entropy values of encrypted image of our cases are listed in Table 5. Table 6 shows the encryption time complexity for different image sizes. Compared with those algorithms [19, 21], our algorithm is much faster. Table 7 shows the contrast analysis of some certain cases of the proposed algorithm.

5. Conclusion

In this paper, we have presented a new algorithm of encryption and decryption of images based on a chaotic economic map. To the best of our knowledge, this work is the first attempt to apply a chaotic economic map in the construction of chaotic cryptography. All the simulation and experimental results have shown that the proposed image encryption and decryption algorithm has (1) a very large key space 10^{84}, (2) high sensitivity to all the secret keys, (3) information entropy that is close to the ideal value 8, and (4) low correlation coefficients that are close to the ideal value 0. Therefore, these results lead to the effectiveness and robustness of the proposed image algorithm. In addition, the results lead us to suggest application of other well-known chaotic economic systems such as duopoly and tripoly economic systems.

Table 7: Contrast analysis at Case I: $a = 5, b = 0.6, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, case II: $a = 5, b = 0.1, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$, and case III: $a = 5, b = 0.2, c = 0.3, x_0 = 0.1, k \in [0, 0.3]$.

Image	Contrast
Plain image	0.3563
Case I ($\gamma = 3$)	10.1655
Case II ($\gamma = 4$)	10.3909
Case III ($\gamma = 5$)	10.3971

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding this research group (no. RG-1435-054).

References

[1] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[2] C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, 2001.

[3] P. Li, Z. Li, W. A. Halang, and G. Chen, "A stream cipher based on a spatiotemporal chaotic system," *Chaos, Solitons and Fractals*, vol. 32, no. 5, pp. 1867–1876, 2007.

[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[5] X. Tong and M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," *Signal Processing*, vol. 89, no. 4, pp. 480–491, 2009.

[6] F. J. Dyson and H. Falk, "Period of a discrete cat mapping," *The American Mathematical Monthly*, vol. 99, no. 7, pp. 603–614, 1992.

[7] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213–220, 2008.

[8] X. Wang, D. Zhao, and L. Chen, "Image encryption based on extended fractional Fourier transform and digital holography technique," *Optics Communications*, vol. 260, no. 2, pp. 449–453, 2006.

[9] C. J. Kuo, "Novel image encryption technique and its application in progressive transmission," *Journal of Electronic Imaging*, vol. 2, no. 4, pp. 345–351, 1993.

[10] Y. V. Mitra, S. Rao, and S. R. Prasanna, "A new image encryption approach using combinational permutation techniques," *International Journal of Computer Science*, vol. 1, no. 2, pp. 127–131, 2006.

[11] S. R. Prasanna, V. Y. Rao, and A. Mitra, "An image encryption method with magnitude and phase manipulation using carrier images," *International Journal of Communication Systems*, vol. 1, pp. 132–137, 2006.

[12] H. S. Kwok and W. K. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons & Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[13] F. Sun, S. Liu, Z. Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons and Fractals*, vol. 38, no. 3, pp. 631–640, 2008.

[14] B. Preneel, "Design principles for dedicated hash functions," in *Fast Software Encryption*, vol. 809 of *Lecture Notes in Computer Science*, pp. 71–82, Springer, Berlin, Germany, 1994.

[15] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[16] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[17] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[18] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[19] Y.-Q. Zhang and X.-Y. Wang, "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation," *Nonlinear Dynamics*, vol. 77, pp. 687–698, 2014.

[20] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[21] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[22] S. S. Askar, "The impact of cost uncertainty on Cournot duopoly game with concave demand function," *Journal of Applied Mathematics*, vol. 2013, Article ID 809795, 5 pages, 2013.

[23] S. S. Askar, "The impact of cost uncertainty on Cournot oligopoly game with concave demand function," *Applied Mathematics and Computation*, vol. 232, pp. 144–149, 2014.

[24] S. S. Askar, "Complex dynamic properties of Cournot duopoly games with convex and log-concave demand function," *Operations Research Letters*, vol. 42, no. 1, pp. 85–90, 2014.

[25] S. S. Askar, "On complex dynamics of monopoly market," *Economic Modelling*, vol. 31, no. 1, pp. 586–589, 2013.

[26] S. S. Askar, "The rise of complex phenomena in Cournot duopoly games due to demand functions without inflection points," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1918–1925, 2014.

[27] S. S. Askar, "On Cournot-Bertrand competition with differentiated products," *Annals of Operations Research*, vol. 223, no. 1, pp. 81–93, 2014.

[28] S. S. Askar and A. Alshamrani, "The dynamics of economic games based on product differentiation," *Journal of Computational and Applied Mathematics*, vol. 268, pp. 135–144, 2014.

[29] V. Grigorasl and C. Grigoras, "Chaos encryption method based on large signal modulation in additive nonlinear discrete-time systems," in *Proceedings of the 5th WSEAS International Conference on Non-Linear Analysis, Noninear Systems and Chaos*, Bucharest, Romania, 2006.

[30] C. Wei-bin and Z. Xin, "Image encryption algorithm based on Henon chaotic system," in *Proceedings of the International Conference om Image Analysis and Signal Processing (IASP '09)*, pp. 94–97, 2009.

[31] X. Wang and J. Zhang, "An image scrambling encryption using chaos-controlled Poker shuffle operation," in *Proceedings of the International Symposium on Biometrics and Security Technologies (ISBAST '08)*, pp. 1–6, Islamabad, Pakistan, April 2008.

[32] H. H. Nien, W. T. Huang, C. M. Hung et al., "Hybrid image encryption using multi-chaos-system," in *Proceedings of the 7th International Conference on Information, Communications and Signal Processing (ICICS '09)*, pp. 1–5, Macau, China, December 2009.

[33] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, pp. 130–141, 1963.

[34] T. Yang, "A survey of chaotic secure communication systems," *International Journal of Computational Cognition*, vol. 2, pp. 81–130, 2004.

[35] M. I. Sobhy and A. R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '01)*, pp. 1001–1004, IEEE, Salt Lake City, Utah, USA, 2001.

[36] S. J. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '02)*, vol. 2, pp. 708–711, Phoenix-Scottsdale, Ariz, USA, 2002.

[37] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *International Journal of Bifurcation and Chaos*, vol. 3, no. 6, pp. 1619–1627, 1993.

[38] S. Li, X. Mou, and Y. Cai, "Improving security of a chaotic encryption approach," *Physics Letters A*, vol. 290, no. 3-4, pp. 127–133, 2001.

[39] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A new chaotic algorithm for video encryption," *IEEE Transactions on Consumer Electronics*, vol. 48, no. 4, pp. 838–843, 2002.

[40] G. Jakimoski and L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters A*, vol. 291, no. 6, pp. 381–384, 2001.

[41] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[42] A. Naimzada and G. Ricchiuti, "Monopoly with local knowledge of demand function," *Economic Modelling*, vol. 28, no. 1-2, pp. 299–307, 2011.

[43] R. W. Clower, "Some theory of an ignorant monopolist," *The Economic Journal*, vol. 69, no. 276, pp. 705–716, 1959.

[44] E. Ahmed, A. S. Hegazi, M. F. Elettreby, and S. S. Askar, "On multi-team games," *Physica A: Statistical Mechanics and its Applications*, vol. 369, no. 2, pp. 809–816, 2006.

[45] E. Ahmed, M. F. Elettreby, and A. S. Hegazi, "On quantum team games," *International Journal of Theoretical Physics*, vol. 45, no. 5, pp. 907–913, 2006.

[46] A. K. Naimzada and G. Ricchiuti, "Complex dynamics in a monopoly with a rule of thumb," *Applied Mathematics and Computation*, vol. 203, no. 2, pp. 921–925, 2008.

[47] A. K. Naimzada and L. Sbragia, "Oligopoly games with nonlinear demand and cost functions: two boundedly rational adjustment processes," *Chaos, Solitons and Fractals*, vol. 29, no. 3, pp. 707–722, 2006.

[48] G. I. Bischi, A. K. Naimzada, and L. Sbragia, "Oligopoly games with local monopolistic approximation," *Journal of Economic Behavior and Organization*, vol. 62, no. 3, pp. 371–388, 2007.

[49] S. S. Askar, "On dynamical multi-team Cournot game in exploitation of a renewable resource," *Chaos, Solitons & Fractals*, vol. 32, pp. 264–268, 2006.