The Scientific World Journal
Volume 2012, Article ID 286741, 10 pages
doi:10.1100/2012/286741

The ScientificWorldJOURNAL

Research Article

A Novel Image Encryption Algorithm Based on DNA Subsequence Operation

Qiang Zhang, Xianglian Xue, and Xiaopeng Wei

Key Laboratory of Advanced Design and Intelligent Computing, Ministry of Education of Dalian University, Dalian 116622, China

Correspondence should be addressed to Qiang Zhang, zhangq30@yahoo.com

Received 3 May 2012; Accepted 8 July 2012

Academic Editors: P. K. Egbert and M. Engin

We present a novel image encryption algorithm based on DNA subsequence operation. Different from the traditional DNA encryption methods, our algorithm does not use complex biological operation but just uses the idea of DNA subsequence operations (such as elongation operation, truncation operation, deletion operation, etc.) combining with the logistic chaotic map to scramble the location and the value of pixel points from the image. The experimental results and security analysis show that the proposed algorithm is easy to be implemented, can get good encryption effect, has a wide secret key's space, strong sensitivity to secret key, and has the abilities of resisting exhaustive attack and statistic attack.

1. Introduction

Nowadays, the computer network has changed the mode of people's communication. People can easily transfer the various multimedia information through the network. However, because of the openness of the network, people have to take more and more attention on security and confidentiality of multimedia information. The digital image is an important information vector of multimedia communication, thus how to protect the image information becomes a universal concern problem for people. The traditional image encryption methods (such as DES, IDEA, and AES) are not suitable for image encryption due to the different storage format of an image. The new research algorithms of image encryption are needed urgently.

As an example, due to chaotic system with like-random, high sensitivity to initial value, and unforeseeable properties, chaos based cryptosystems have become current research hotspot. According to the object of scrambling, the chaos-based algorithms operate in two stages: the shuffling stage and the substitution stage. In the shuffling stage, the position of pixels from original image is changed by chaotic sequences [1] or by some matrix transformation, such as Arnold transform, magic square transform, and so forth. These shuffling algorithms are easy to be realized and have better encryption effect. Due to these shuffling algorithms, just changing the position of pixels but not changing the pixel values leads to the histogram of the encryption image is the same as the original image, and thus its security is threatened by the statistical analysis. In the substitution stage, the pixel values are changed by chaotic sequences. Most of these encryption methods are directly implemented by overlaying a chaotic sequence generated by a single chaotic map and the pixel grey value from the image. Comparing with the method of the shuffling, the method of value substitution may lead to higher security, but from the vision angle the encryption effect is not good. Thereby, in order to improve the security and the encryption effect, the shuffling and the value substitution are combined by some researchers, the readers can refer to [2, 3]. However, only using a single chaotic map to encrypt image may result in lower security and smaller key space. Ren et al. [1] presented a chaotic algorithm of image encryption based on dispersion sampling; their algorithm has better scrambling effect, but has small key space. Zhang et al. [4] use logistic and standard systems to scramble the location and the value of pixel points from the image, and they have got better result; however, no security analysis in their paper was given. Recently, Lian et al. [5–7] used some multidimensional chaotic maps (such as the chaotic standard map, the chaotic neural networks, and spatiotemporal chaos system) to encrypt images and make a detailed analysis for the security of algorithms. Their algorithms have satisfactory security with a low cost. A new image encryption algorithm based on multiple chaos system is proposed by Zuo et al. [8]. Similarly, Liu et al. [9] also used multiple chaotic maps to encrypt image. All of their algorithms have a large key space, high sensitivity to key variation, and unforeseeable and have the ability of resisting traditional attacks. Generally speaking, to improve the security of encryption algorithm, researchers usually try to use more complex chaotic system or combine some new encryption methods with the existing chaotic systems to implement image encryption. However, some chaotic systems have been proven to be insecure [10–12].

With the rapid development of DNA computing, DNA cryptography, as a new field, has come into being. A method for hiding message in DNA microdots was proposed by Clelland et al. [13]. Clelland used DNA microdots to hide message to implement the protection of information. For instance, letter A is expressed as DNA sequence GGT by complex biological operation. Obviously, it is difficult to be implemented and is not suitable for image encryption. Gehani et al. presented an encryption algorithm of the one-time pad cryptography with DNA strands [14]; Gehani's method is effective, but the process of encryption must utilize complex biological operations, which are difficult to be controlled under the experimental environment. So the method is not easy to be realized. In fact, since the high-tech laboratory requirements and computational limitations, combining with the labor intensive extrapolation means, researches of DNA cryptography are still much more theoretical than practical. Recently, Kang presented a pseudo DNA cryptography method [15]. Kang's method not only has the better encryption effect, but also does not require complex biological operation. However, it was only used for encrypting text files.

In this paper, we do not use biological operation to implement image encryption, but adopt the rule of DNA subsequence operation such as truncation operation, deletion operation, transformation operation and so forth, then combine DNA subsequence operation with chaos system to scramble the location and the value of pixel point from the image.

The structure of this paper is as follows. In Section 2, we will introduce the basic theory of the proposed algorithm. The design of the proposed image encryption scheme is discussed in the Section 3. In Section 4, some simulation results and security analysis are given. In Section 5, we compare our algorithm with other encryption algorithms. Section 6 draws the conclusion.

2. Basic Theory of the Proposed Algorithm

2.1. Generation of the Chaotic Sequences. The chaotic system is a deterministic nonlinear system. It possesses a varied characteristics, such as high sensitivity to initial conditions and system parameters, random-like behaviors, and so forth. Chaotic sequences produced by chaotic maps are pseudo-random sequences; their structures are very complex and difficult to be analyzed and predicted. In other words, chaotic systems can improve the security of encryption systems. Thus, it is advisable to encrypt digital image with chaotic systems [16–24]. Here, we introduce the following two chaotic maps, one is logistic map, and the other is 2D logistic map. In the paper, we use 2D logistic map to produce the eight parameters as the initial values and system parameters of four logistic maps.

Logistic map is an example for chaotic map, and it is described as follows:

$$x_{n+1} = \mu x_n (1 - x_n), \tag{1}$$

where $\mu \in [0,4]$, $x_n \in (0,1)$, and $n = 0, 1, 2, \ldots$. The research result shows that the system is in chaotic state under the condition that $3.56994 < \mu \leq 4$.

2D logistic map is described in (2) [25] as follows:

$$\begin{aligned} x_{i+1} &= \mu_1 x_i (1 - x_i) + \gamma_1 y_i^2 \\ y_{i+1} &= \mu_2 y_i (1 - y_i) + \gamma_2 (x_i^2 + x_i y_i). \end{aligned} \tag{2}$$

When $2.75 < \mu_1 \leq 3.4$, $2.75 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$ and, $0.13 < \gamma_2 \leq 0.15$, the system is in chaotic state and can generate two chaotic sequences in the region (0,1]. Due to the system parameter γ_1 and γ_2 which have smaller value range, we set $\gamma_1 = 0.17$ and $\gamma_2 = 0.14$, other parameters can be seen as secret keys.

2.2. DNA Sequence Encryption

2.2.1. DNA Encoding and Decoding for Image. A single DNA sequence is made up of four nucleic acid bases: A (adenine), C (cytosine), G (guanine), and T (thymine), where A and T are complements, and C and G are complements. Let binary number 0 and 1 be complements, so 00 and 11 are complements, and 01 and 10 are complements. Thus we can use these four bases: A, T, G, and C to encode 01, 10, 00, and 11, respectively. The encoding method still satisfies the Watson-Crick complement rule [25]. Usually, each pixel value of the 8 bit grey image can be expressed to 8 bits binary stream. The binary stream can be encoded to a DNA sequence whose length is 4. For example: if the first pixel value of the original image is 75, convert it into a binary stream [01001011]. By using the above DNA encoding rule to encode the stream, we can get a DNA sequence [$AGTC$], whereas we use A, T, G, and C to express 01, 10, 00, and 11, respectively. We can get a binary sequence [01001011].

2.2.2. DNA Subsequences Operation. In this section we use the idea of [26] to define the DNA subsequence and the corresponding operation. We define that a DNA sequence P_k contains m strands of DNA subsequences according to the order, in the P_k, the number of bases is k $(m \leq k)$. The expression is $P_k = P_m P_{m-1} \cdots P_2 P_1$. The number of bases for the corresponding DNA subsequences is $l_m l_{m-1} \cdots l_2 l_1$, respectively. Apparently, $k = l_m + l_{m-1} + \cdots l_2 + l_1$. Based on the above DNA subsequence expression, we described the following five kinds of DNA subsequence operation; they are elongation operation, truncation operation, deletion operation, insertion operation, and transformation operation.

(1) DNA subsequence elongation operation.

Definition 1. We suppose that there is an original DNA sequence P_1, the subsequence P_2, whose length is l_1, is elongated to the tail of P_1. After elongation operation, we can get a new DNA sequence $P' = P_1P_2$. The expression is as follows:

$$P_1 + P_2 \longrightarrow P_1P_2. \tag{3}$$

(2) DNA subsequence truncation operation.

Definition 2. The truncation operation and the elongation operation are contrary. Truncating the end of the subsequence P_2 in the DNA sequence P_1P_2, we will obtain a new DNA sequence $P' = P_1$. The expression is as follows:

$$P_1P_2 - P_2 \longrightarrow P_1. \tag{4}$$

(3) DNA subsequence deletion operation.

Definition 3. We suppose that there is an original DNA sequence $P = P_3P_2P_1$. Deleting the subsequence P_2, then we will obtain a new DNA sequence $P' = P_1P_3$. The expression is as follows:

$$P_3P_2P_1 - P_2 \longrightarrow P_3P_1. \tag{5}$$

(4) DNA subsequence insertion operation.

Definition 4. The deletion operation and the insertion operation are contrary. We suppose that there is an original DNA sequence $P = P_3P_1$, inserting a subsequence P_2, whose length is l_2, into P. The expression is as follows:

$$P_3P_1 + P_2 \longrightarrow P_3P_2P_1. \tag{6}$$

(5) DNA subsequence transformation operation.

Definition 5. In brief, the locations of two subsequences are transformed. If the original DNA sequence is $P = P_5P_4P_3P_2P_1$. Transforming the locations of P_4 and P_2, we will get a new DNA sequence $P' = P_5P_2P_3P_4P_1$. The expression is as follows:

$$P_5P_4P_3P_2P_1 \longrightarrow P_5P_2P_3P_4P_1. \tag{7}$$

We introduced five kinds of DNA subsequence operations, where the inverse operation of elongation operation is truncation operation and the inverse operation of deletion operation is insertion operation. In our algorithm, we use elongation operation, truncation operation, deletion operation, and transformation operation and combined with the use of the Logistic chaotic map we will realize the image encryption algorithm. However, the insertion operation is just used in the decryption process.

3. Algorithm Description

3.1. Generation of Chaotic Sequences. Input initial state (x_0, μ_1, y_0, μ_2), by using 2D Logistic to produce eight parameters $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ after iterating 1000 times. We Use the following formulas to produce four groups of parameters:

$$\begin{aligned} x_1 &= x_1, & u_1 &= 3.9 + 0.1 \times x_2, \\ y_1 &= x_3, & u_2 &= 3.9 + 0.1 \times x_4, \\ z_1 &= x_5, & u_3 &= 3.9 + 0.1 \times x_6, \\ q_1 &= x_7, & u_4 &= 3.9 + 0.1 \times x_8. \end{aligned} \tag{8}$$

Then, by using logistic chaotic map to generate four chaotic sequences under the condition that the four groups of initial values are (x_1, u_1), (y_1, u_2), (z_1, u_3), and (q_1, u_4), their length are $m \times n$, respectively.

3.2. Generation of DNA Subsequences

Step 1. Input an 8 bit grey image $A(m, n)$, as the original image, where m and n is rows and columns of the image.

Step 2. Convert image A into binary matrix A' whose size is $(m, n \times 8)$ and divide A' into eight bit-planes. Here, the first bitplanes and the eighth bitplanes, the second bitplanes and the seventh bitplanes, the third bitplanes and the sixth bitplanes, and the forth bit-planes and the fifth bit-planes are composed, respectively. Then we obtain four bit-planes.

Step 3. Carry out DNA encoding operation according to Section 2.2.1 for the four bitplanes, then we get four coding matrices P_1, P_2, P_3, P_4, all of their sizes are (m, n).

Step 4. Convert P_1, P_2, P_3, P_4 into P'_1, P'_2, P'_3, P'_4 whose sizes are $(1, (m \times n))$, then divide P'_1, P'_2, P'_3, P'_4 into DNA subsequence; the average length of subsequences are $l_1 = 128$, $l_2 = 64$, $l_3 = 32$, and $l_4 = 8$, respectively. So, there are the following conclusions:

$$\begin{aligned} P'_1 &= p_{11}p_{12} \cdots p_{1(mn/l_1)}, \\ P'_2 &= p_{21}p_{22} \cdots p_{2(mn/l_2)}, \\ P'_3 &= p_{31}p_{32} \cdots p_{3(mn/l_3)}, \\ P'_4 &= p_{41}p_{42} \cdots p_{4(mn/l_4)}, \end{aligned} \tag{9}$$

where p_{ij} are DNA subsequences, l_i are lengths of these subsequences, $i \in [1, 4]$, and $j \in [1, mn/l_i]$.

3.3. Deletion Operation

Step 1. We suppose that there is a chaotic sequence $X = \{x_1, x_2 \cdots x_{mn/l_i}\}$.

Step 2. If $x_i < 0.5$, delete the ith subsequence according to Section 2.2.2, otherwise save the subsequence.

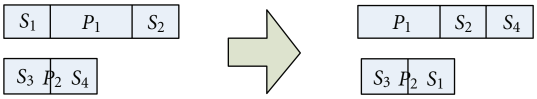


Figure 1: Elongation and truncation operation of DNA subsequences.

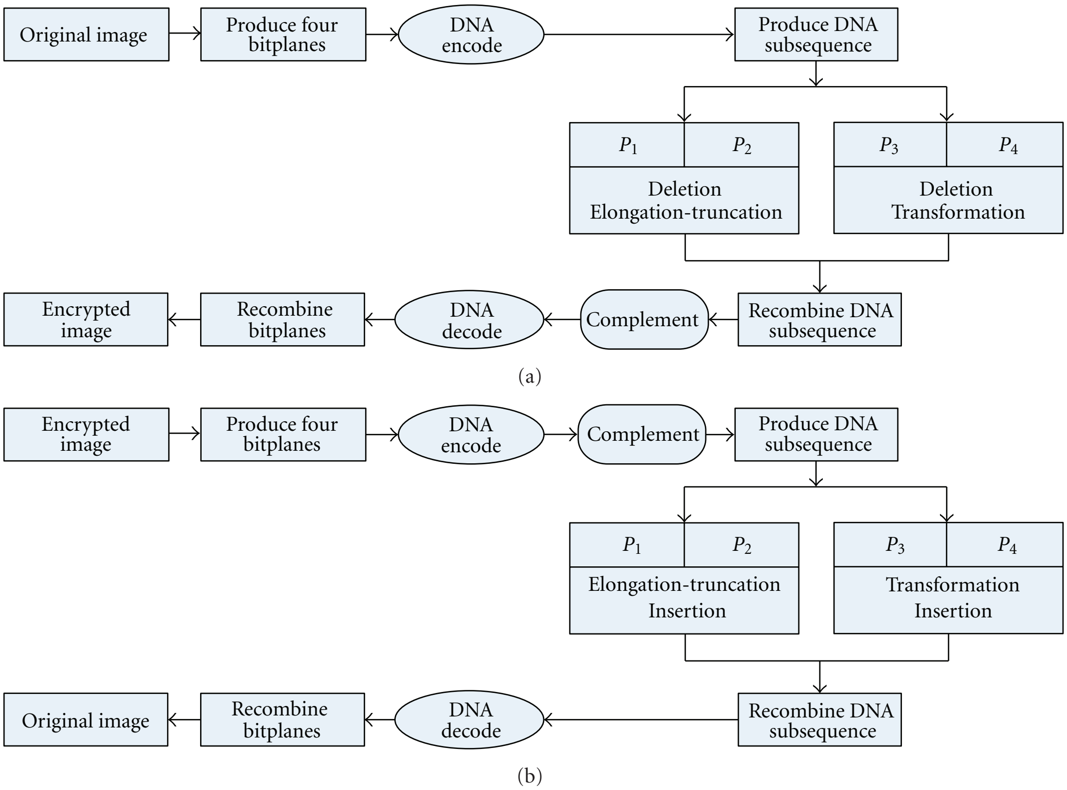


Figure 2: The block diagram of the proposed algorithm. (a) The block diagram of the encryption algorithm. (b) The block diagram of the decryption algorithm.

Step 3. Those deleted subsequences are moved to the end of the saved subsequences.

3.4. Transformation Operation

Step 1. We suppose that there is a chaotic sequence $X = \{x_1, x_2 \cdots x_{mn/l_i}\}$.

Step 2. To sort X by ascending, we get a new sequence $X' = \{x'_1, x'_2 \cdots x'_{mn/l_i}\}$.

Step 3. If $x_i < 0.5$, the ith subsequence and the i'th subsequence from the location of X' are transformed according to Section 2.2.2.

3.5. Elongation and Truncation Operation. As shown in Figure 1, P_1 and P_2 are two DNA subsequences from any of two bit-planes, we suppose that the length of P_1 is 128, the length of P_2 is 64, S_1 and S_2, S_3, and S_4 are DNA subsequences of P_1 and P_2, respectively. First, we truncate S_1 and S_4, then elongate S_1 to the tail of P_2, elongate S_4 to the tail of P_1.

3.6. Complement Operation. Complement operation is carried out for every one dimension bit-plane whose size is $(1, m \times n)$, we suppose there is a chaotic sequence $X = \{x_1, x_2 \cdots x_{mn/l_i}\}$. If $x_i < 0.5$, the nucleic acid base of the ith location is complemented, otherwise, it is unchanged.

3.7. The Procedure of Image Encryption and Decryption. The proposed encryption algorithm includes three steps: first, by using the method proposed in the Section 3.1 to produce four groups of DNA sequences P_1, P_2, P_3, and P_4, where P_i $(i = 1, 2, 3, 4)$ is made up of many DNA subsequences. Then, to disturb the position and the value of pixel points from image by combining the logistic map, generate chaotic sequences and DNA subsequence operations (such as elongation operation, truncation operation, deletion operation, transformation, etc.). At last, the encrypted image is obtained by DNA decoding and recombining bit-planes. The block diagram of the proposed algorithm is shown in Figure 2, the block diagram of the encryption algorithm is shown in Figure 2(a), and Figure 2(b) shows the block diagram of the decryption algorithm. We can see that the procedure of

```
Input: An 8-bit image $A$ and chaotic parameters $(x_0, \mu_1, \gamma_1, y_0, , \mu_2, \gamma_2)$
Output: The encrypted image $B$
(1)  $[S_1, S_2, S_3, S_4]$ := four DNA sequences obtained from image $A$;
(2)  $[P_1, P_2, P_3, P_4]$ := four groups of DNA subsequences obtained from
     image $[S_1, S_2, S_3, S_4]$;
(3)  $[x_1, u_1, y_1, u_2, z_1, u_3, q_1, u_4]$ := eight chaotic parameters obtained by 2D
     Logistic map under chaotic initial parameters $(x_0, \mu_1, \gamma_1, y_0, , \mu_2, \gamma_2)$;
(4)  $[X, Y, Z, Q]$ := four chaotic sequences obtained by Logistic map under
     the chaotic parameters $(x_1, u_1, y_1, u_2, z_1, u_3, q_1, u_4)$;
(5)  $A_1 = Deletion(P_1, X)$;
(6)  $A_2 = Deletion(P_2, Y)$;
(7)  $[E_1, E_2] = Elongation - truncation(A_1, A_2)$;
(8)  $A_3 = Deletion(P_3, Z)$;
(9)  $A_3^{'} = Transformation\ (A_3, Z)$;
(10) $A_4 = Deletion(P_4, Q)$;
(11) $A_4^{'} = Transformation\ (A_4, Q)$;
(12) $[B_1, B_2, B_3, B_4] = Recombine - subseqence(E_1, E_2, A_3^{'}, A_4^{'})$;
(13) $[B_1^{'}, B_2^{'}, B_3^{'}, B_4^{'}] = Complement(B_1, B_2, B_3, B_4)$;
(14) $B$ := carry out DNA decoding and recombining binary bitplanes for $B_1^{'}, B_2^{'}, B_3^{'}, B_4^{'}$;
```

Algorithm 1: An image encryption algorithm based on DNA subsequence operation.

```
Input: The decrypted image $B$ and chaotic parameters $(x_0, \mu_1, \gamma_1, y_0, \mu_2, \gamma_2)$
Output: The encrypted image $A$
(1)  $[B_1, B_2, B_3, B_4]$ := four DNA sequences obtained from image $B$;
(2)  $[B_1^{'}, B_2^{'}, B_3^{'}, B_4^{'}] = Complement(B_1, B_2, B_3, B_4)$;
(3)  $[P_1, P_2, P_3, P_4]$ := four groups of DNA subsequences obtained from image $[B_1^{'}, B_2^{'}, B_3^{'}, B_4^{'}]$;
(4)  $[x_1, u_1, y_1, u_2, z_1, u_3, q_1, u_4]$ := eight chaotic parameters obtained by 2D Logistic map under
     chaotic initial parameters $(x_0, \mu_1, \gamma_1, y_0, \mu_2, \gamma_2)$;
(5)  $[X, Y, Z, Q]$ := four chaotic sequences obtained by Logistic map under the chaotic
     parameters$(x_1, u_1, y_1, u_2, z_1, u_3, q_1, u_4)$;
(6)  $[E_1, E_2] = Elongation - truncation(P_1, P_2)$;
(7)  $M_1 = Insertion(E_1, X)$;
(8)  $M_2 = Insertion(E_2, Y)$;
(9)  $E_3 = Transformation\ (P_3, Z)$;
(10) $M_3 = Insertion(E_3, Z)$;
(11) $E_4 = Transformation\ (E_4, Q)$;
(12) $M_4 = insertion(E_4, Q)$;
(13) $[A_1, A_2, A_3, A_4] = Recombine - subseqence(M_1, M_2, M_3, M_4)$;
(14) $A$ := carry out DNA decoding and recombining binary bit-planes for $A_1, A_2, A_3, A_4$;
```

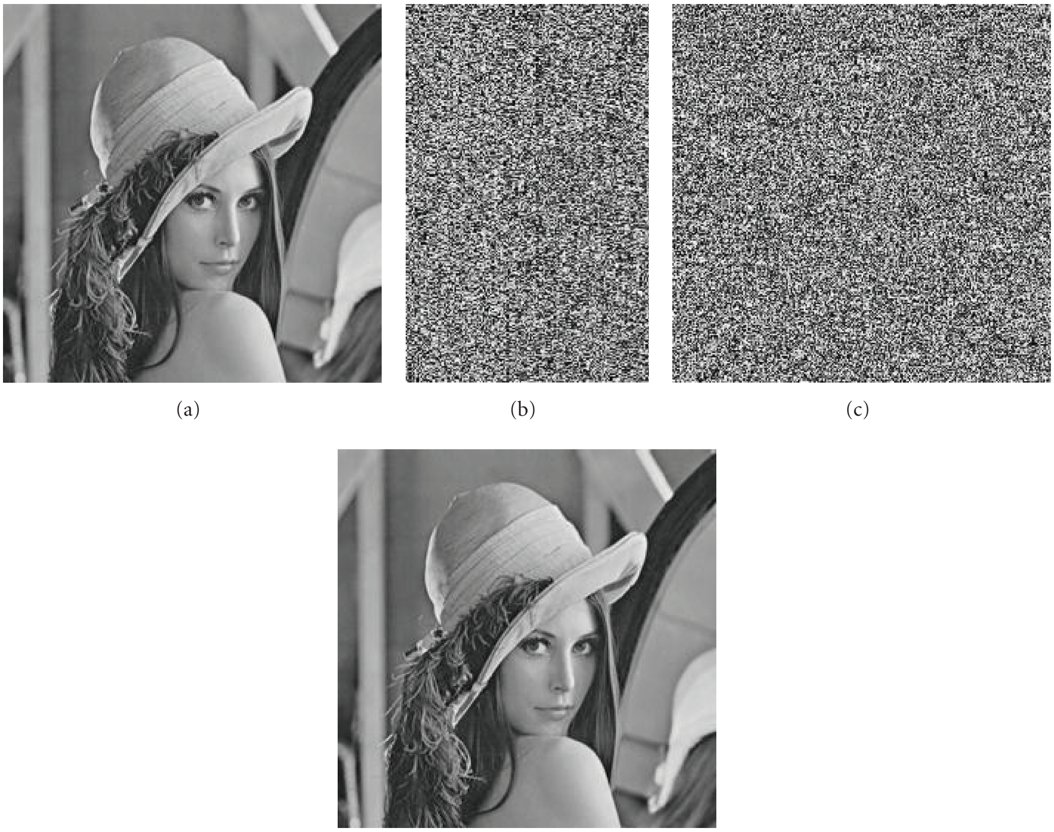
Algorithm 2: An image decryption algorithm based on DNA subsequence operation.

image decryption is inverse procedure of image encryption from Figure 2. The detailed procedure of our encryption and decryption algorithms are explained in the following pseudocodes (Algorithms 1 and 2).

The functions and parameters in Algorithms 1 and 2 are the same as Sections 3.1–3.6, where DNA decoding and recombining are the inverse process of Steps 3 and 2 in Section 3.2. The procedure of acquiring the original image from the encryption image is an inverse operation according to Algorithm 2, where deletion operation is replaced by insertion operation.

4. Simulation Result and Security Analysis

4.1. Simulation Result. In this paper, for standard 256 × 256 gray image Lena, we use Matlab 7.1 to simulate experiment. In our experiment, we set $x_0 = 0.95$, $\mu_1 = 3.2$, $\gamma_1 = 0.17$, $y_0 = 0.25$, $\mu_1 = 3.3$, $\gamma_2 = 0.14$. The original image is shown



(a)

(b)

(c)

(d)

Figure 3: Encrypted image and decrypted image. (a) The original image. (b) The encrypted image. (c) The decrypted image under the wrong secret keys. (d) The decrypted image under the correct secret keys.

in Figure 3(a), Figure 3(b) shows encrypted image, and Figure 3(b) points out that it is difficult to recognize the original image. Figures 3(c) and 3(d) show the decrypted image under the wrong secret keys and the right secret keys, respectively. From Figure 3(c), we know that it has not any connection with the original image, but Figure 3(d) is as same as the original image.

4.2. Secret Key's Space Analysis. In the proposed algorithm, the initial value and the parameter of the system of 2D logistic are identified as secret keys of this algorithm. Therefore, our algorithm has six secret keys x_0, μ_1, γ_1, y_0, μ_2, γ_2. If the precision is 10^{-14}, the secret key's space is $10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{84} \approx 2^{279}$. It is shown that the secret key's space is large enough to resist exhaustive attack.

4.3. Secret Key's Sensitivity Analysis. The chaotic map is very sensitive to the initial value in chaotic state, in other words, it also ensured the sensibility of this encryption algorithm to the secret key. In this paper, if the initial values from three chaotic maps are changed a little, the recovering image is not allowed to be read, but we can get the original image from the encrypted image by using the correct secret keys. The experiment results are shown in Figure 4, where Figure 4(a) shows the decrypted image under the secret keys $(0.95000000000001, 3.2, 0.17, 0.25, 3.3, 0.14)$. The corresponding histogram is shown in Figure 4(b), and we can see that the histogram of the decrypted image is very uniform. The sensitivity of other parameters is similar. From Figure 4, we can see that only when all secret keys (the chaotic initial value and system parameter) are correct, the original image can be obtained. Otherwise the decrypted image will have no connection with the image. Based on the above argument, our algorithm has strong sensitivity to secret key and we can say again that our algorithm can resist exhaustive attack.

4.4. Statistical Analysis

4.4.1. The Grey Histogram Analysis. We compare the grey histogram of the image before and after encryption to analyze the statistical performance. Figure 5(a) shows the grey histogram of the original image and Figure 5(b) shows the grey histogram of the encrypted image. From the two figures, we can see that the original pixel grey values are concentrated on some value, but the pixel grey values after the encryption are scattering in the entire pixel value space, namely, two images have lower similarity. Clearly, it is difficult to use the statistical performance of the pixel grey value to recover the original image. Thereby, our algorithm has strong ability of resisting statistical attack.

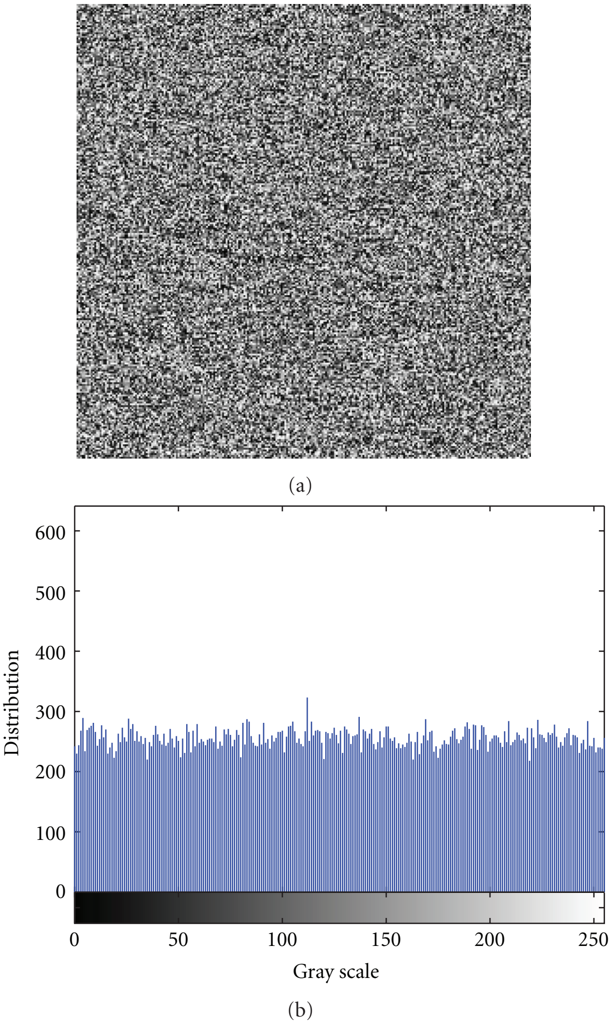


Figure 4: The sensitivity of secret key x_0. (a) The decrypted image with secret key (0.95000000000001, 3.2, 0.17, 0.25, 3.3, 0.14). (b) The corresponding histogram.

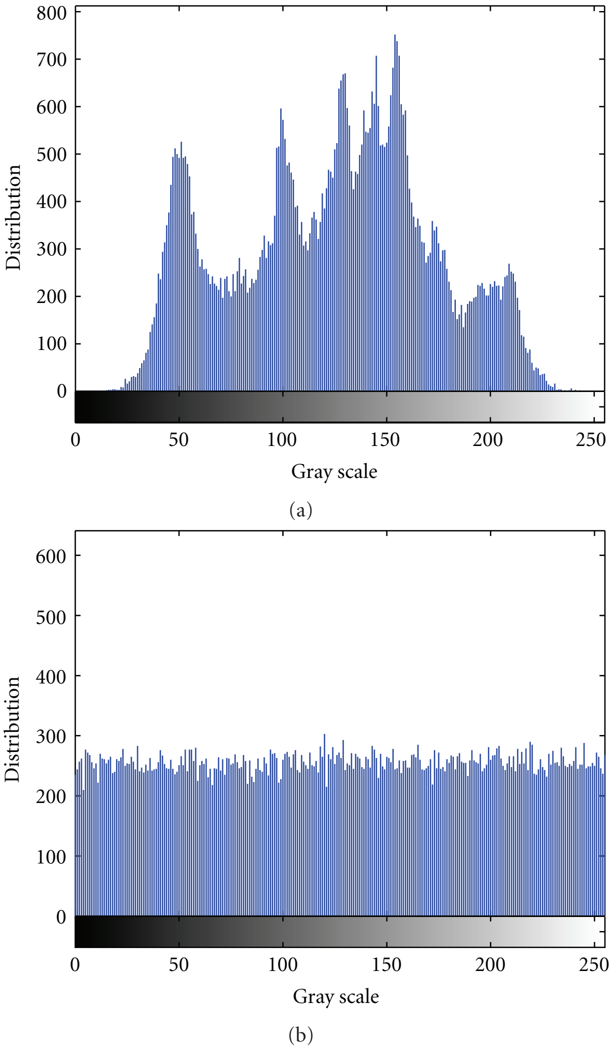


Figure 5: The grey histogram of the original image and the encrypted image. (a) The grey histogram of the original image. (b) The grey histogram of the encrypted image.

4.4.2. Correlation Coefficient Analysis. The correlation of the adjacent pixels in original image is very high, an effective encryption algorithm can reduce the correlation of between adjacent pixels. Here, we randomly select 3000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image, then by using the following formulas to calculate the correlation coefficient:

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \\ \operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \\ r_{xy} &= \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}}, \end{aligned} \tag{10}$$

where x and y are grey value of two adjacent pixels in the image.

Figures 6(a) and 6(b) show the correlation of two horizontally adjacent pixels in the original image and that in the encrypted image, where the correlation coefficients are 0.9432 and 0.1366, respectively. Other results are shown in Table 1. From Figure 6(b) and Table 1, we can see that the correlation coefficient of the adjacent pixels in encrypted image is low, which is close to 0. It follows from Figure 6(b) and Table 1 that the proposed image encryption algorithm has strong ability of resisting statistical attack.

4.4.3. Information Entropy. It is well known that information entropy can measure the distribution of grey value in the image. We can make sure that the bigger information entropy the more uniform for the distribution of grey value. The definition of information entropy is as follows:

$$H(m) = -\sum_{i=0}^{L} P(m_i)\log_2 P(m_i), \tag{11}$$

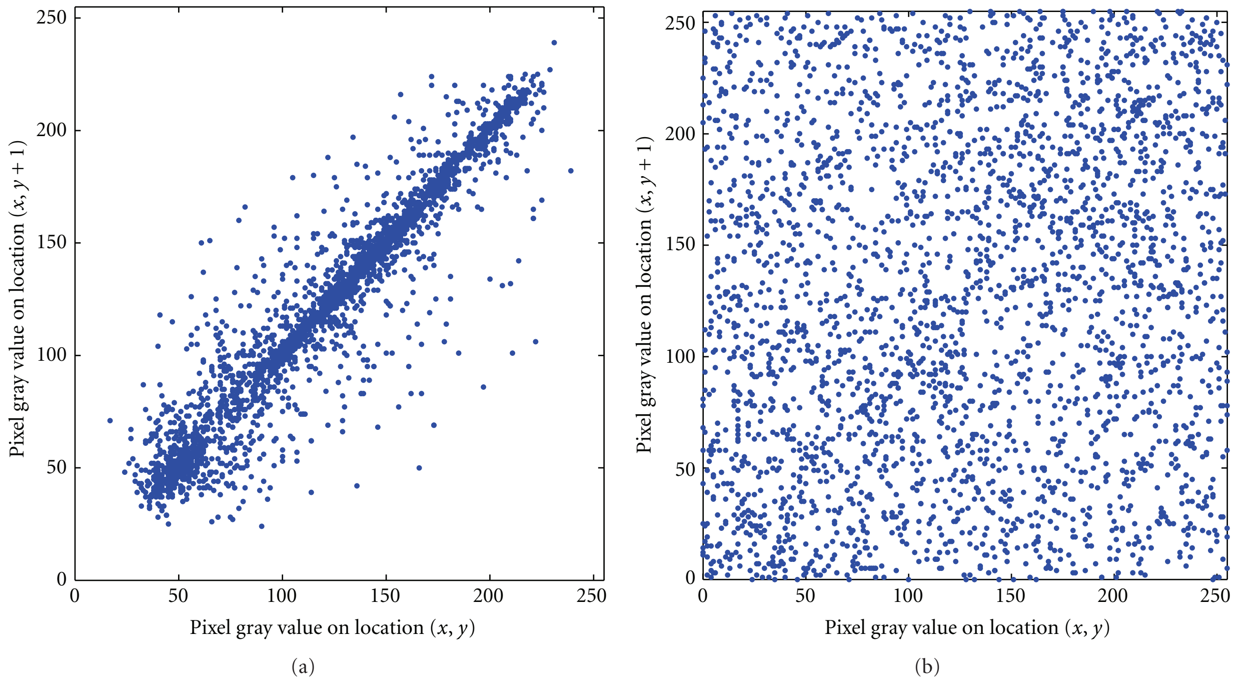


Figure 6: Correlation of two horizontally adjacent pixels in the original image and in the encrypted image.

Table 1: Correlation coefficients of two adjacent pixels in two image.

Model	The original image	The encrypted image
Horizontal	0.9432	0.1366
Vertical	0.9688	0.0166
Diagonal	0.9148	0.0021

Table 2: Comparison with other chaos-based encryption algorithms.

Considered items for 256 × 256 lena image	Proposed	Reference [16]	Reference [17]	Reference [18]	Reference [1]
Key space	2^{279}	2^{233}	N/A	2^{260}	2^{99}
Key sensitivity	Yes	Yes	N/A	Yes	Yes
information entropy	7.9975	N/A	7.99732	7.9968	N/A
Chaotic system used	DNA operation and logistic system	Chen's chaotic system	Chen's chaotic system	Coupled chaotic system	Logistic chaotic system

Table 3: Comparison with other DNA-based encryption algorithms.

Considered items	Proposed	Clelland et al. [13]	Gehani et al. [14]	Kang [15]
Image	Yes	No	Yes	No
Text	Yes	Yes	Yes	Yes
Security analysis	Yes	No	No	Yes
Biology operation	No	Yes	Yes	No
Method	DNA subsequence operation chaotic maps	Messages encoded as DNA stands	Use micro-array technology	A pseudo DNA cryptography

where m_i is the ith grey value for L level grey image and $P(m_i)$ is the emergence probability of m_i. The information entropy of an idea random image is 8. For the proposed algorithm, the information entropy is 7.9975. It is very close to 8.

5. Comparison with Other Encryption Algorithms

In this section, we will compare our proposed algorithm with existing chaos-based and DNA-based encryption algorithms. We focus on the security consideration in the comparative aspects of chaos-based and focus on the encryption objects and environment in the comparative aspects of DNA-based. The comparison results are shown in Tables 2 and 3. From Table 2, we can see that the key space and the information entropy of our proposed algorithm are larger than others. However the methods in [17, 18] can resist differential attack, the proposed method in this paper cannot resist differential attack. From Table 3, we easily found that only our algorithm and [14] can implement image encryption. But the algorithm proposed in [14] is difficult to be implemented owing to the complex biologic operation. Kang's encryption effect [15] is better than others. However, his algorithm can only encrypt the text. After comparing with other encryption algorithms proposed in Tables 2 and 3, the proposed algorithm is better than other DNA-based encryption algorithm and has larger key space and high key sensitivity, but the disadvantage is that the algorithm cannot resist differential attack. This is our next study work.

6. Conclusion

A novel image encryption algorithm based on DNA subsequence operation is proposed in this paper. The simulation experimental results and security analysis show that the encryption algorithm is effective, easy to be realized, has larger key space, and is sensitive to the secret key. Our algorithm can also resist statistical analysis and exhaustive attacks. Furthermore, it avoids complex biological experiment in traditional DNA cryptography. But because DNA subsequence operation is based on horizontal, or the length of the subsequences selected is longer, it may lead to the horizontal correlation of the adjacent pixels in original image a bit high. We can improve the horizontal correlation through changing the lengths of DNA subsequences from each bit-planes. In addition to that, the weak ability of resisting differential attack is also a defect of this algorithm. They are our next research works.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (nos. 31170797, 30870573), Program for Changjiang Scholars and Innovative Research Team in University (no. IRT1109), the Program for Liaoning Innovative Research Team in University (no. LT2011018), the Program for Liaoning Excellent Talents in University (no. LR201003), the Program for Liaoning Innovative Research Team in University (no. LT2011018) and the Program for Liaoning Science and Technology Research in University (no. LS2010179).

References

[1] H. Ren, Z. Shang, Y. Wang, and J. Zhang, "A chaotic algorithm of image encryption based on dispersion sampling," in *Proceedings of the 8th International Conference on Electronic Measurement and Instruments (ICEMI '07)*, vol. 2, pp. 836–839, August 2007.

[2] C. Fu and Z. Zhu, "A chaotic image encryption scheme based on circular bit shift method," in *Proceedings of the 9th International Conference for Young Computer Scientists (ICYCS '08)*, vol. 522, pp. 3057–3061, November 2008.

[3] H. E. Ren, J. Zhang, X. J. Wang, and Z. W. Shang, "Block sampling algorithm of image encryption based on chaotic scrambling," in *Proceedings of the International Conference on Computational Intelligence and Security Workshops (CIS '07)*, vol. 109, pp. 773–776, December 2007.

[4] Y. H. Zhang, B. S. Kang, and X. F. Zhang, "Image encryption algorithm based on chaotic sequence," in *Proceedings of the 16th International Conference on Artificial Reality and Telexistence—Workshops (ICAT '06)*, vol. 29, pp. 221–223, December 2006.

[5] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," *Chaos, Solitons and Fractals*, vol. 40, no. 5, pp. 2509–2519, 2009.

[6] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons and Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[7] S. Lian, "A block cipher based on chaotic neural networks," *Neurocomputing*, vol. 72, no. 4–6, pp. 1296–1301, 2009.

[8] Y. Z. F. Zuo, Z. Zhai, and C. Xiaobin, "A new image encryption algorithm based on multiple chaos system," in *Proceedings of the International Symposium on Electronic Commerce and Security (ISECS '08)*, vol. 142, pp. 347–350, August 2008.

[9] J. M. Liu, S. S. Qiu, F. Xiang, and H. J. Xiao, "A cryptosystem based on multiple chaotic maps," in *Proceedings of the International Symposium on Information Processing (ISIP '08) and International Pacific Workshop on Web Mining and Web-Based Application (WMWA '08)*, vol. 99, pp. 740–743, May 2008.

[10] 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.

[11] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of an ergodic chaotic cipher," *Physics Letters A*, vol. 311, no. 2-3, pp. 172–179, 2003.

[12] I. S. Mohamed and R. S. Alaa-eldin, "Methods of attacking chaotic encryption and countermeasures," in *Proceedings of the IEEE Interntional Conference on Acoustics, Speech, and Signal Processing*, pp. 1001–1004, Salt Lake, Utah, USA, May 2001.

[13] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.

[14] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," in *Proceedings of the DIMACS Workshop on DNA Based Computers*, June 1999.

[15] N. Kang, "A pseudo DNA cryptography method," http://arxiv.org/abs/0903.2693.

[16] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[17] S. J. Xu, J. Z. Wang, and S. X. Yang, "An improved image encryption algorithm based on chaotic maps," *Chinese Physics B*, vol. 17, no. 11, pp. 4027–4032, 2008.

[18] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons and Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[19] Y. Xiao and L. Xia, "A new hyper-chaotic algorithm for image encryption," in *Proceedings of the 9th International Conference for Young Computer Scientists (ICYCS '08)*, pp. 2814–2818, November 2008.

[20] Y. Zhai, S. Lin, and Q. Zhang, "Improving image encryption using multi-chaotic map," in *Proceedings of the Workshop on Power Electronics and Intelligent Transportation System (PEITS '08)*, vol. 10, pp. 143–148, August 2008.

[21] X. Zhang and W. Chen, "A new chaotic algorithm for image encryption," in *Proceedings of the International Conference on Audio, Language and Image Processing (ICALIP '08)*, pp. 889–892, July 2008.

[22] L. Wang, Q. Ye, Y. Xiao, Y. Zou, and B. Zhang, "An image encryption scheme based on cross chaotic map," in *Proceedings of the 1st International Congress on Image and Signal Processing (CISP '08)*, vol. 3, pp. 22–26, May 2008.

[23] J. Peng, D. Zhang, and X. Liao, "A digital image encryption algorithm based on hyper-chaotic cellular neural network," *Fundamenta Informaticae*, vol. 90, no. 3, pp. 269–282, 2009.

[24] C. Çokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 373, no. 15, pp. 1357–1360, 2009.

[25] J. D. Watson and F. H. C. Crick, "Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid," *Nature*, vol. 171, no. 4356, pp. 737–738, 1953.

[26] W. C. Chen, Z. Y. Chen, Z. H. Chen et al., "Operational rules of the digital coding of DNA sequences in high dimension space," *Acta Biophysica Sinica*, vol. 17, no. 3, pp. 542–549, 2001.

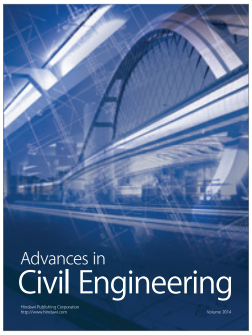
Journal of
Engineering

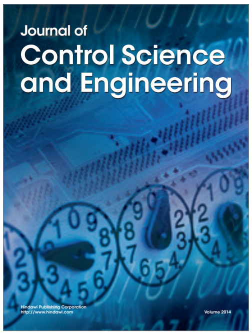
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

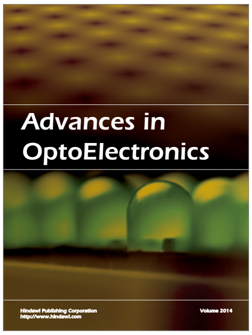
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

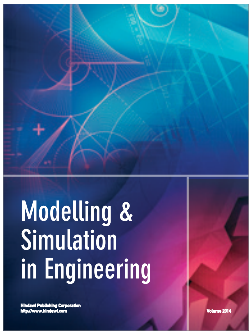
Journal of
Robotics

Journal of
Electrical and Computer Engineering

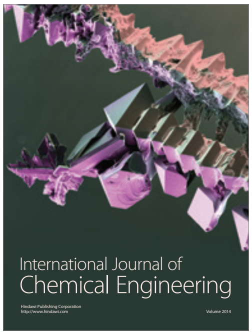

Advances in
OptoElectronics

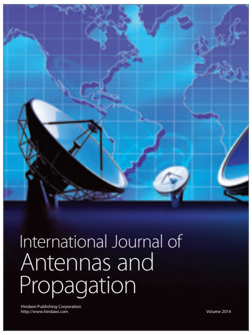
VLSI Design

International Journal of
Navigation and Observation

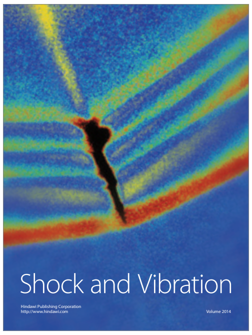

Modelling &
Simulation
in Engineering

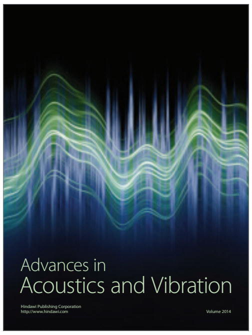
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration