Image Encryption Based On Nonlinear Chaotic Algorithm

Amit Gupta,Master of Engineering Scholar,
Shri Shankarcharya Group of Institution, Bhilai, India
Chandrashekhar Kamargaonkar, Associate Professor, Faculty of Engineering,
Shri Shankarcharya Group of Institution, Bhilai, India
Monisha Sharma, PhD,Sr. Associate professor, Faculty of Engineering,
Shri Shankarcharya Group of Institution, Bhilai, India

Abstract
This paper published on image encryption process. Its encryption method based on nonlinear chaotic algorithm which uses tangent and power function. The drawbacks of linear chaotic sequence are small key space and weak security in one dimentional its characteristics parameters are found by experimental analysis one time one password is generated by this algorithm. Nonlinear chaotic algorithm has advantage of large key space and high security level

Index Terms—Nonlinear chaotic sequence, Encryption,Decryption

I. INTRODUCTION
Image encryption is needed for secure transmission through wireless networks and internet. Traditional image encryption algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large [1,2]. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. After Matthews proposed the chaotic encryption algorithm in 1989 [3], increasing researches of image encryption technology are based on chaotic systems [4–8]. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, nonperiodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography [4]. Therefore, chaotic cryptosystems have more useful and practical applications. One-dimensional chaotic system with the advantages of high-level efficiency and simplicity [14], such as Logistic map, has been widely used now. But their weakness, such as small key space and weak security, is also disturbing [15,16]. To overcome these drawbacks, the objective of this paper is to design a new chaotic algorithm. In Section 2, we propose a new nonlinear chaotic algorithm (NCA). Section 3 presents the encryption algorithm based on NCA. Section 4 gives the experimental analysis. In Section 5, security of the chaotic encryption algorithm is discussed. It is proved that the new algorithm has the advantages of high-level security, large key space and zero co-correlation while maintaining acceptable efficiency. Finally, Section 6 concludes the paper.

II. A NEW NONLINEAR CHAOTIC ALGORITHM (NCA)
A. Logistic map analysis
The cryptosystems, based on widely-used one-dimensional discrete chaotic maps, such as Logistic map, are weak in security. As known Logistic map is
defined as: \( x_{n+1} = k \cdot x_n \cdot (1 - x_n) \), where \( k \in (0, 4) \), \( n = 0, 1, \ldots \) [17]. The parameter \( k \) and initial value \( x_0 \) may represent the key. The parameter \( k \) can be divided into three segments, which can be examined by experiments on following conditions: \( x_0 = 0.3 \). When \( k \in (0, 3) \), as shown in Fig. 1(a), the calculation results come to the same value after several iterations without any chaotic behavior. When \( k \in [3, 3.6) \), the phase space concludes several points only, as showed in Fig. 1(b), the system appears periodicity. While \( k \in [3.6, 4) \), it becomes a chaotic system with periodicity disappeared. So we can draw the following conclusions: (1) The Logistic map does not satisfy uniform distribution property. When \( k \in [0, 3.6) \) the points concentrate on several values and could not be used for encryption purpose. (2) Cryptosystems based on Logistic map has small key space and weak security.

B. The NCA map design

To overcome those limitations, this paper intends to design a new nonlinear chaotic algorithm (NCA). In [18], the authors demonstrate that chaotic encryption systems can be easily attacked and, in order to improve security, they suggested the adoption of nonlinear functions, limited in time and space, to change the key continuously. In accordance with such a principle, in this paper the NCA map uses power function \((1 - x)^b\) and tangent function instead of linear function. The NCA is defined as

\[
  x_{n+1} = k \cdot \tan(x_n) \cdot (1 - x_n)^b
\]

where \( x_n \in (0, 1) \), \( n = 0, 1, 2, \ldots \)

The ranges of parameters \( k, a \) and \( b \) will be discussed as follows. Firstly, they are positive. Secondly, the absolute value of the slope of the curve at fixed point should not be less than 1 [19], and \( x_{n+1} > x_n \) when \( x_n = 1/(1 + b) \), therefore \( k \) may be defined as

\[
  k = \mu \cdot \tan\left(\frac{a}{1+b}\right) \cdot (1 + \frac{1}{b})^{-1} \quad \mu > 0
\]

Finally, parameter \( l \) is obtained by experimental analysis; as a result, \( k = 1 - b^4 \). So the NCA map is defined as follows:

Fig. 1. The limitations of Logistic iteration map: (a) iteration property when \( k = 2.8 \), (b) iteration property when \( k = 3.2 \).
### Table 1
Iteration experiments of the NCA map

<table>
<thead>
<tr>
<th>Sr no</th>
<th>Experimental conditions</th>
<th>Experimental results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a = 0.13, b = 4.909702$</td>
<td>$x_{3318} = x_{3270}$</td>
</tr>
<tr>
<td>2</td>
<td>$a \in (0, 1.4], b \in [5, 43]$</td>
<td>${x_n}_{n=0}^{1000000}$ is chaotic sequence</td>
</tr>
<tr>
<td>3</td>
<td>$a = 1.4, b = 43.984711$</td>
<td>$x_{4897} = 0$</td>
</tr>
<tr>
<td>4</td>
<td>$a = 1.41, b = 8.889831$</td>
<td>$x_{243642} = x_{237260}$</td>
</tr>
<tr>
<td>5</td>
<td>$a \in (1.4, 1.5], b \in [9, 38]$</td>
<td>${x_n}_{n=0}^{1000000}$ is chaotic sequence</td>
</tr>
<tr>
<td>6</td>
<td>$a = 1.5, b = 38.5$</td>
<td>$x_{432916} = 0$</td>
</tr>
<tr>
<td>7</td>
<td>$a \in (1.5, 1.57], b \in [3, 15]$</td>
<td>${x_n}_{n=0}^{1000000}$ is chaotic sequence</td>
</tr>
<tr>
<td>8</td>
<td>$a = 1.57, b = 15.199957$</td>
<td>$x_{31271} &gt; 1$</td>
</tr>
</tbody>
</table>

Furthermore, to evaluate the property of the NCA map, other experiments have been done as follows:

**Step 1:** Set $x_0 = 0.3$, $a = 0.02$ and $b = 5$, do iteration test as formula (3) for one million times. This experiment shows that the one million data are different from each other and satisfy zero correlation.

**Step 2:** Do such test experiment as above by changing the value of $b$ from $b = 5$ to $b = 43$, with 0.01 increment of $b$ for each experiment.

**Step 3:** Randomly select 100 values of $a$ among $(0, 1.4]$, and for each $a$ do such test experiments as step 2.

**Step 4:** Similar experiments have been done when $a \in (1.4, 1.5], b \in [9, 38]$ and $a \in (1.5, 1.57], b \in [3, 15]$. All these experimental data prove that systems described by formula (3) are chaotic systems with good properties of balanced 0–1 ratio, zero correlation and ideal nonlinearity, while maintaining acceptable efficiency.

**Fig. 2** shows the iteration curve of the NCA map when $x_0 = 0.3$, $\beta = 3.5$. From these statistical data, we can see that the new chaotic algorithm spreads the initial region over the entire chaotic sequence.

### III. Encryption Algorithm

The image encryption algorithm is based on the proposed NCA map. It uses chaotic sequence generated by NCA map to encrypt image data with different keys for different images. Original chaotic sequence $\{x_0, x_1, x_2, \ldots\}$ consists of decimal fractions. However images are all digital. So a map is defined to transform the chaotic sequence to another sequence which consists of integers. Then plain-image can be encrypted by use of XOR operation with the integer sequence.

**Fig. 3** shows the block diagram of the chaotic encryption algorithm. The encryption steps are as follows:

**Step 1:** Set encryption key for the plain-image, including structural parameters $a$, $b$ and initial value $x_0$.

**Step 2:** Do 100 times of chaotic iteration as formula (3), and obtain the decimal fraction $x_{100}$.

**Step 3:** If the encryption work is finished, then go to step 6; otherwise do three times of chaotic iteration; and as a result, a decimal fraction, such as $x_{103}$, will be generated, which is a double value and we choose its first 15 significant digits.

**Step 4:** Divide the 15 digits into five integers with each integer consisting of three digits. For each integer, do mod 256 operation, and another 5 bytes of data will be generated.

**Step 5:** Do XOR operation using the 5 bytes of data with 5 bytes of image data (grey value or color RGB value). Output the calculation result to the object image and go to step 3.
Fig. 2. Iteration property of the NCA map.

n(a=1.57, b=3.5)

The decryption algorithm is similar to the encryption algorithm but receiving encryption key and operating with the encrypted image.

The first 100 points of the chaotic iteration curve are abnegated in order to avoid the harmful effect of transitional procedure. Furthermore, to improve system security, we selected the pseudo-random numbers discontinuously; as shown in Fig. 3, one was selected after two abnegated points

IV. EXPERIMENTAL ANALYSIS

Experimental analysis of the new algorithm presented in this paper has been done with several images. Fig. 4 shows the experimental results with Lena BMP image. Fig. 4(a) is the 256 grey-scale Lena plain-image of size 256 × 256. Fig. 4(b) is its encrypted image with the encryption key K = (x0, a, b) = (0.987654321012345, 1.1, 5). As we can see, the encrypted image is rough-and-tumble and unknowable. Fig. 4(c) is the decrypted image by use of the decryption algorithm with the same key. It can be seen that the decrypted image is clear and correct without any distortion. But if we use the wrong key, we will get an unexpected image. For example, Fig. 4(d) shows the decrypted image using the wrong key K1 = (x0, a, b) = (0.987654321012346, 1.1, 5). So it can be concluded that the chaotic encryption algorithm is sensitive to the key, a small change of the key will generate a completely different decryption result and can not get the correct plain-image.

With a statistical analysis of Lena image and its encrypted image, their grey-scale histograms are given in Fig. 5. Fig. 5(b) shows uniformity distribution of grey-scale of the encrypted image. It demonstrates that the encryption algorithm has covered up all the characters of the plain image and shows good performance of balanced 0–1 ratio, zero cocorrelation and high-level security.
Fig. 4. Image encryption and decryption experimental result: (a) plain-image, (b) encrypted image, (c) decrypted image.

Fig. 5. Histograms of the plain-image and the cipher-image: (a) histogram of plain-image, (b) histogram of cipher-image.

V. CONCLUSIONS
To overcome the drawbacks of small key space and weak security in the widely used one-dimensional Logistic systems, this paper presents a new nonlinear chaotic algorithm. Its structural parameters and initial value can all be used as encryption key in chaotic cryptosystems. Experimental analysis demonstrates that the image encryption algorithm based on NCA shows advantages of large key space and high-level security, while maintaining acceptable efficiency. It is particularly suitable for Internet image encryption and
transmission applications. Although the algorithm presented in this paper aims at the image encryption, it is not just limited to this area and can be widely applied in other information security fields.

References


Author profile

Amit Gupta is a scholar of master of engineering in the department of Electronic & Communication Engineering at Shri Shankarcharya Group of Institution.,Bhilai India. He has received bachelor Degree(B.E.) in electronics and telecommunication from SSCET, Bhilai. His current area of research include Image encryption and decryption.

Chandrashekhar Kamargoonkar is an associated professor in the department of Electronic & Communication Engineering at Shri Shankarcharya Group of Institution.,Bhilai India. He is M.E. Coordinator in the Department of Electronic &Communication Engineering at S.S.G.I. Bhilai India.He has more than 9 year experience in teaching. He has received Master Degree(M.E.) in digital electronics from S.S.G.M. College of Engineering, Shegaon India. His current area of research include Image Processing, Digital Communication, Microcontroller & Embedded System.
Dr. Monisha Sharma is an Sr. associated professor in the department of Electronic & Communication Engineering at Shri Shankarcharya Group of Institution, Bhilai, India. She was awarded Ph.D. (Electronics) degree on “Development of Highly Secured Image Encryption algorithm using multi chaotic sequences” from C.S.V.T.U., Bhilai on 2010. She has published more than 46 papers in national/ international journals/conferences. She Awarded as Chhattisgarh Young Scientist Award in 2008 for “Generation of secured image for Telemetry using Adaptive Genetic Algorithm” by C.G Council of Science and Technology. Her research interests include Digital Image Processing, Secure communication, Cryptography, Stenography, Steganalysis, Cryptanalysis, Error Codes.