Secure Image Encryption Based on an Ideal New Nonlinear Discrete Dynamical System

R. M. Lin and T. Y. Ng

School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore 639798

Correspondence should be addressed to R. M. Lin; mrmlin@ntu.edu.sg

Received 2 November 2017; Accepted 26 March 2018; Published 3 May 2018

1. Introduction

Chaos is an inherent dynamic behavior associated with many nonlinear systems called chaotic systems [1]. These systems have some very important and unique characteristics such as extreme sensitivities of system responses to system parameters and initial conditions, leading to unpredictable system behavior, and periodic doublings, leading to nonperiodicity and seeming randomness. These complex dynamic properties are exactly what are desired in cryptography [2] since when they are used in data encryption, they serve to achieve the required diffusion and mixing of data to enhance security. These observations have recently led to the development of a number of data encryption algorithms based on chaotic sequence, which have since found useful and practical applications.

Synchronized continuous chaotic systems have been recently employed to achieve secure communications. Most of these methods are based on the principle that message signals can be mixed with a carrier signal from a chaotic system and subsequently sent through the transmission channels. The message is then recovered through chaos synchronization and subtraction of the received masked signals. To ensure successful communications, synchronization of the chaotic carrier signals between sender and receiver becomes paramount. A Lorenz chaotic system was implemented at circuit level and was used to demonstrate that synchronization of such a system can be achieved when used in communication [3]. The possibility of synchronization coupled with chaos to be used to implement secure communication systems which is inherently error-free in contrast with the signal-maskingschemes proposed in [3] was discussed in [4]. A general approach for constructing chaotic synchronized dynamical systems used for communication was examined based on a decomposition of a given system into active and passive parts [5]. For enhanced security, additive noise was added to chaotic signals to generate encryption keys [6] and an effective error function attack approach was proposed to critically evaluate the latent security of existing chaos synchronization based encryption schemes [7].
In digital communications, data encryption such as image encryption schemes has been vigorously investigated to meet the ever-growing demand for real-time secure image transmissions over the Internet and through wireless networks. Traditional data encryption methods such as the Data Encryption Standard (DES) suffer from extremely low efficiency when bulk data such as images are involved [8]. To significantly improve efficiency needed while maintaining required security, encryption schemes developed based on discrete chaotic dynamical systems have been recently sought. The earliest attempt in this direction seemed to be the chaotic encryption algorithm proposed by Matthews [9]. Based on the classical one-dimensional Logistic map, which has been known to become chaotic under some system parameters, a number of image encryption methods have been developed and have met some success. By directly using the chaotic sequence generated from a Logistic map, a pixel by pixel image encryption algorithm was designed and was found to be effective [10]. Detailed cryptanalysis of the Logistic map based algorithms was conducted by Li et al. [11] and Arroyo et al. [12], revealing some of the pitfalls and recommending some possible improvement. Logistic map was also employed to construct Block Encryption Ciphers to enhance efficiency [13]. Intertwining Logistic map was investigated by Wang and Xu [14] to overcome some of the shortcomings of the conventional Logistic map.

Higher dimensional chaotic maps have also been investigated in their potential for image encryption applications. A 2D logistic map together with DNA sequence operations was examined by Wang et al. [15] for image encryption applications. A 2D Bakers map was first generalized and then discretized to create a symmetric block encryption scheme [16] and its detailed security analysis was carried out by Solak et al. [17]. A 2D Arnold cat map was examined and found to have desirable characteristics for image encryption [18]. The map was further generalized and extended to three dimensions (3D), which was then effectively employed to encrypt image data [19]. Attempts have been undertaken to couple two different chaotic systems to further enhance security [20, 21]. Cryptanalysis of these encryption schemes based on composition maps was accomplished by Li et al. [22]. Such coupling produces additional security feature similar to those of high dimensional chaotic maps. Further, general spatiotemporal chaotic systems have been proposed to achieve better trade-off between level of security and efficiency [23], as well as chaotic maps with local and global feedback and multilevel perturbations [24]. In addition to applications of chaotic cryptography to image encryptions, further researches on applications of joint image encryption with compression [25] as well as video encryptions [26, 27] have been recently carried out.

Much progress has been made to date on image encryption based on chaotic systems. However, most existing methods suffer from some or all of these problems: (i) limited key space since chaotic behavior only occurs under certain system parameter settings; (ii) presence of periodic behavior within key space which undermines security; and (iii) weakness in any possible known-plain-text attack due to the known correlation among the chaotic sequence used. The data sequences generated based on most chaotic systems within stable strange attractors are chaotic but not completely random, while ideal encryption security requires truly random data sequences. To overcome these existing problems, this paper presents a new highly nonlinear discrete dynamical system with ideal chaotic characteristics for secure image encryption. Transcendental functions are introduced together with modulo operations which physically represent discontinuous time varying nonlinearities, leading to extremely complex chaotic behavior which is highly sensitive to system parameters and initial conditions, both of which can be considered as the keys for the cryptosystem. Extensive numerical experiment results have revealed that proposed image encryption algorithm offers advantages of unlimited key space and high-level security, since those problematic periodic windows are no longer present within the key space, and it is extremely robust against known-plain-text attack, since the chaotic sequence generated bears no correlation whatsoever due to the folding effect of modulo operation. The algorithm is believed to make truly efficient yet highly secure image encryption a reality.

2. A New Highly Nonlinear Discrete Dynamical System

The proposed discrete dynamical system and its application to encryption can be considered as an improved Logistic map [28] into which a new transcendental function and a new floating modulo operation are introduced. Mathematically, the system is simply defined as

\[ x_{n+1} = \lambda x_n (1 - \sin x_n) \mod 1. \]  

Without the modulo operation, the thus defined new map is very similar to the classical Logistic map except that, in this case, a transcendental sine function is used instead of a linear function. As a result, the proposed new system essentially becomes more nonlinear and possesses, as expected, much wider ranges of system parameters in which complex desirable chaotic behavior is observed. Such increases in the complexity of system dynamic chaotic behavior as well as in system parameter domain over which complex chaotic behavior occurs are ideal for effective, efficient, and more secure data encryption applications.

2.1. Improved Performance over Logistic Map. To compare these characteristics, bifurcation diagrams and Lyapunov exponents for both the Logistic map and the new system have been computed with all possible system parameter λ values before divergence occurs and these are shown in Figures 1–4.

The maximum and minimum values of the proposed new system without the modulo operation for every given value of λ can be determined mathematically. Since \( x_{n+1} = \lambda x_n (1 - \sin x_n) \), the derivative becomes \( \frac{dx_{n+1}}{dx_n} = \lambda (1 - \sin x_n - x_n \cos x_n) \). Then, by letting the derivative be zero, \( \lambda (1 - \sin x_n - x_n \cos x_n) = 0 \), the \( x_n \) values in the range become \( x_n = 0.5596843072 \) and \( x_n = \pi/2 \), corresponding to a maximum value of \( x_{\text{max}} = 0.26254712771 \lambda \) and a minimum value of \( x_{\text{min}} = 0 \).
2.2. Dynamic Characteristics of the Proposed Discrete Dynamical System. It can be seen clearly that the new proposed system has a much wider range of system parameters over which the Lyapunov exponents are positive and the magnitudes of these positive Lyapunov exponents are much larger than those observed from the conventional Logistic map. These indicate that the chaotic behavior of the proposed discrete dynamical system can be far more complex than that of the conventional Logistic map. From data encryption point of view, while the new proposed system certainly offers much larger key space and better security, there still exist finite windows of system parameters in which periodic behaviors are present, as in the case of the conventional Logistic map, and these may present potential security risk if the keys chosen happen to be within these windows. For a seemingly continuous system parameter region of chaotic behavior, as shown in Figures 1 and 3, brief periodic windows are yet observed under much refined resolutions as shown in Figures 5 and 6.

Many more such periodic windows can perhaps be found if yet better resolutions are employed during numerical simulations. In fact, due to the fractal nature of all chaotic systems, it can be said that once such periodic windows coexist among largely chaotic behavior, there are infinitely many! This is easily seen from Figure 6(b), where periodic windows are interwoven infinitesimally close with chaotic ones with fractal boundaries between them. As a result, one shall obtain very similar behavior no matter how many times the boundaries are magnified as shown in Figure 7, where 100 and 10,000 times are used to magnify the region shown in Figure 6(b).

To overcome such difficulties when applied to image encryption, modulo operation is further introduced to possibly eliminate these periodic windows to further enhance security. A modulo operation, from system dynamics point of view, can be considered as discontinuity and time-varying nonlinearities which are the strongest nonlinear physical mechanisms possibly encountered in practice. Introduction of such additional nonlinear mechanism can be expected to lead to improved chaos characteristics desirable for image encryption applications. A modulo 1 operation is used as defined in (1) since each time it folds data back to the desired region of [0, 1]. The bifurcation map and Lyapunov exponents of the complete new system are shown in Figures 8 and 9. Due to the very large system parameter range ($\lambda = 0$–$10^{16}$) in this case and in different regions, characteristically distinctive dynamic behavior has been observed; the bifurcation map is presented in interval format to better illustrate the key performance of the system.

As shown in Figure 8, for small values of system parameter $\lambda$, the diagram is the same as that of Figure 3, since the modulo operation bears no effect due to small values of $x_n < 1$. As $\lambda$ increases, bifurcations and periodic windows are observed but the physical widths of these windows become
shorter. As \( \lambda \) further increases, the visible periodic windows become narrower and narrower and completely disappear when \( \lambda \) reaches around \( \lambda = 200 \). Then a very wide range of ideally chaotic and uniformly random working region is obtained. This region is called working region, since only data generated for system parameters in the region will be used for subsequent image encryption. This is further supported by the Lyapunov exponents obtained as shown in Figure 9.
The complete encryption/decryption algorithm can be summarized in the following steps:

1. Set encryption keys for the plain image which are the values for $\lambda$ and $x_0$.
(2) Perform some initial iterations to eliminate any harmful effect of transient dynamics of the system (50 is used in all simulation presented in this paper).

(3) Iterate one more time to generate a decimal fraction which is in double precision and choose the first 9 most significant digits to obtain 3 integers of 3 digits each.

(4) Three bytes of chaotic sequence are generated by performing modulo 256 operations on the 3 integers and subsequently they are XORed with 3 bytes of plain-image data (grey value or color RGB values) to form 3 bytes of encrypted image data.

(5) Repeat steps (3) and (4) until all plain-image data are encrypted and then output the completely encrypted object image data.

(6) Send the encrypted object image data through public communication channel.

(7) Pass the encryption keys through secure communication channel.

(8) End.

The decryption algorithm is similar to the encryption algorithm except that the same given encryption keys should be used and the input image data are those of the ciphered image. It is noted that only the first 9 most significant digits are extracted in a double precision decimal fraction to ensure absolute safety in accuracy across different computing architectures.

4. Experimental Analysis

The proposed new encryption algorithm has been applied to an amount of image data and very encouraging results have been achieved. Experimental analysis of the standard-color Lena plain 512 × 512 images shown in Figure 13(a) has been carried out and the results are presented. Figure 13(b) shows the encrypted cipher image with chosen encryption keys \((\lambda, x_0) = (100400, 0.75)\), indicating that the original image has been completely destroyed and randomized. On the other hand, if the cipher image is then decrypted using the same keys, the exact original image is discovered as shown in Figure 13(c). However, if wrong keys are used,
unexpected randomized decrypted images are obtained as shown in Figure 13(d), in which only very slightly different keys \((\lambda, x_0) = (100400 + 10^{-11}, 0.75)\) are used, demonstrating the extreme sensitivity of the process to system parameter \(\lambda\). Similar sensitivity to initial condition \(x_0\) has also been observed throughout the cases examined.

Statistical analysis of the Lena image and its encrypted counterpart has been examined and their histograms are shown in Figures 14 and 15. The fact that almost uniform random distributions of the encrypted histograms in all 3 color components are achieved demonstrates that the proposed algorithm is capable of covering up all characters of the plain image and has very good performance of balanced 0-1 ratios, zero correlation, and enhanced security.

To further examine the statistical correlation between adjacent pixels in plain and ciphered images, coherence values have been computed, which is defined as

\[
\gamma_{pq} = \frac{\sum_{i=1}^{N} (p_i - E(p)) (q_i - E(q))}{\sqrt{\sum_{i=1}^{N} (p_i - E(p))^2} \sqrt{\sum_{i=1}^{N} (q_i - E(q))^2}},
\]

where \((p_i, q_i)\) are the RGB values of the \(i\)th pair of 2 adjacent pixels, \(N\) is the number of such pairs formed, and \(E(p)\) and \(E(q)\) are the mean values of \(p_i\) and \(q_i\) \((t = 1, 2, \ldots, N)\). By randomly selecting 10000 \((N = 10000)\) such pairs in the horizontal, vertical, and diagonal directions, the coherence values for the RGB components of the plain and ciphered images are computed and are shown in Table 1. One typical such pair of data in the horizontal direction for the red color components of the plain and ciphered images is plotted as shown in Figure 16. As can be seen, the correlation that exists in the plain image is completely destroyed in its encrypted counterpart when the encryption algorithm is applied. This is further illustrated by the coherence values obtained, indicating that the encryption algorithm satisfies zero correlation.

Computationally, the proposed encryption/decryption algorithm is very fast and efficient. The notebook used for this test is a 2.4 GHz Fujitsu Lifebook with an Intel® Core™ i5 CPU and a 2.99 GB RAM. The total CPU time clocked for the encryption and the subsequent decryption of the Lena color image of size 512 \(\times\) 512 is 0.40221 seconds, which is much shorter than those reported [10].

### 5. Security Analysis

The new encryption algorithm developed in this paper based on the new highly nonlinear discrete dynamical system belongs to one-time one-password system that can be considered as secure according to the requirements of
information communication system discussed by Shannon [2]. Compared with existing encryption algorithms based on classical Logistic map, the new algorithm has large continuous key space by eliminating the periodic windows that undermine security, and, as shown in Figure 11(b), the chaotic sequences generated are totally uncorrelated, thereby making their reverse recovery totally hopeless! These have essentially resolved all existing security weaknesses pertaining to chaos based image encryption methods and have opened a new era for their ever-increasing practical applications.

Extensive experimental analyses have shown that chaotic data sequences generated by the proposed system are truly random, which have an ideal property of uniform distribution. When such data sequences are employed, trial tests have shown that the proposed encryption algorithm possesses many ideal characteristics of traditional cryptography, such as highly complex system behavior, ideal discontinuous and time-varying nonlinearity due to the introduction of modulo operation, zero correlation, and the irreversibility of the process of generating chaotic sequences. Because of all these desirable properties, the algorithm is believed to be able to resist grey code attack and statistical attack strongly [4].

Brute-force attack is becoming increasingly popular nowadays and the strength of a cryptosystem under such attack is mainly measured by its keys. The proposed algorithm is capable of resisting Brute-force attack, since its keys consist of 2 floating-point numbers \((\lambda, x_0)\). If one uses the first 15 digits of a floating-point number in double precision, then the key will have altogether \(15 + 15 = 30\) digits. This represents a total possible number of keys of \(10^{30}\), which is far greater than \(2^{56}\) of the most commonly used 56-bit DES [29], a publicly acknowledged secure encryption algorithm. Further, the key length of the proposed algorithm can be easily further increased. Instead of (1), the more general system can be written as

\[
x_{n+1} = \lambda x_n^\alpha (1 - \mu \sin x_n)^\beta \mod 1.
\]

As a result, 5 system parameters, \(\lambda, x_0, \mu (-1.0 < \mu < 1.0),\) \(\alpha,\) and \(\beta\) (both are short integers), can be used to form the

Figure 13: Image encryption and decryption results.
keys. The key in this case will have $15 + 15 + 15 + 5 = 50$ digits, in which the two short integers contribute roughly about 5 digits, leading to a possible number of keys of $10^{15} \times 2^8 \times 2^8 \approx 10^{50}$, which is believed to be beyond the reach of the most sophisticated attacks! One typical bifurcation diagram for the more general system with $\mu = 0.75$, $\alpha = 2$, and $\beta = 3$ is shown in Figure 17 and, as expected, similar chaotic characteristics are observed.

Most chaotic encryption algorithms are very vulnerable to known-plain-text attack due to the correlation that exists among the values of the chaotic sequence, as shown in Figure 11(a). In the case of encryption based on the Logistic map, theoretically, only 2 pixels of known-plain-text are needed to compute the hidden keys. This is a fatal weakness associated with most of the existing chaotic encryption algorithms, as far as their practical applications are concerned. The new proposed algorithm, however, has a perfect ability to resist such an attack, since there is no such correlation whatsoever among the chaotic sequence, as shown in Figure 11(b), due to the application of the modulo operation. For the case of possible possession of any known plain text, no matter how much that text may be, it is not possible to use these texts to further increase the knowledge of the hidden plain image or to use them to possibly recover the hidden keys. The keys and the remaining portion of the plain image are not in any sense undermined due to the availability of some known-plain-text, since the encryption process is irreversible unless the keys are known. In addition, only partial digits of the values of the chaotic sequence are used during encryption and this adds further mathematical complexity to that already irreversible encryption process. This enhanced security is one of the most attractive features of the new algorithm.

6. Conclusions

In this paper, a new highly nonlinear discrete dynamical system has been developed and investigated. Chaotic characteristics of the system such as bifurcations, fractal boundaries, and statistical properties of chaotic data sequence have been analyzed and have been found to be the most desirable for data encryption applications. The introductions of a transcendental sine function and a modulo operation render the system behavior extremely complex, leading to the removal of the periodic windows for large values of system parameters, the elimination of the correlation among the data sequences generated, and an almost ideally uniformly distributed random data series. The modulo function performs repeated
folding operations, thereby generating truly uncorrelated random data. Subsequently, a new image encryption algorithm has been developed, which overcomes these problems associated with existing encryption algorithms based on chaotic dynamics: (i) limited key space since chaotic behavior only occurs under limited system parameters; (ii) presence of periodic behavior within key space which undermines security; and (iii) weakness in any possible known-plain-text
attacked by the known correlation among the chaotic sequences. Extensive numerical experiments have revealed that the proposed image encryption algorithm offers advantages of unlimited key space and high-level security and is extremely robust against known-plaintext attacks. Coupled with system simplicity and computational efficiency, it is believed that the proposed algorithm will make truly efficient yet highly secure image encryptions a reality.

Conflicts of Interest

The authors declare that they have no conflict of interests.

References


