Data Encryption Scheme Based on Rules of Cellular Automata and Chaotic Map Function for Information Security

Warakorn Srichavengsup and Wimol San-Um
(Corresponding author: Warakorn Srichavengsup)

Intelligent Electronic System Research Laboratory, Faculty of Engineering, Thai-Nichi Institute of Technology
1771/1 Pattanakarn Road, Suanluang, Bangkok 10250
(Email: warakorn@tni.ac.th)

(Received Sept. 11, 2015; revised and accepted Dec. 7, 2015 & Jan. 15, 2016)

Abstract

Cryptography has recently played a significant role in secure data transmissions and storages. Most conventional data encryption schemes are relatively complicated and complexity in encrypted keys is insufficient, resulting in long computational time and low degree of security against all types of attacks. Consequently, a highly-secured and robust data encryption scheme is necessary. This paper therefore presents the data encryption scheme based on a combination of Cellular Automata (CA) and a robust chaotic system that employs absolute-value piecewise-linear nonlinearity. The proposed encryption scheme is not only applicable to image encryption but also extendable to text and Excel files. Simulation results reveal that the entropy of the encrypted image is nearly 8 corresponding to the image entropy theory, and the correlation coefficients of before-and-after encrypted images are close to zero. Besides, the histogram of the encrypted image of pixel values in the range (0-255) is apparently flat, indicating that the color in image is fully distributed. Such results indicate that the proposed data encryption scheme offers a high level of security with fast processing time duration. The implementation of image encryption Android application is demonstrated. Comparisons to other related approaches are also included.

Keywords: Cellular automata, chaotic map, data encryption, data security

1 Introduction

Advances in communications have led to great demand for secured data transmissions [7, 11] and storage for a variety of applications such as medical, industrial and military systems. The secured data transmissions greatly require reliable, fast and robust security systems, and can be achieved through cryptography, which is a technique of information privacy protection under hostile conditions [17]. Data and image cryptography may be classified into two categories, i.e. (1) pixel value substitution which focuses on the change in pixel values so that original pixel information cannot be read, and (2) pixel location scrambling which focuses on the change in pixel position. Conventional cryptography such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), and RSA algorithm may not be applicable in real-time image encryption due to high computational time and high computing power, especially for the images with large data capacity and high correlation among pixels [10].

The utilization of chaotic systems has broadly been suggested as one of potential alternative encryption techniques in secured data and image transmissions [1, 8]. In comparison to conventional encryption algorithms, chaos-based encryptions are sensitive to initial conditions and parameters while conventional algorithms are sensitive to designated keys. Furthermore, chaos-based encryptions spread the initial region over the entire phase space, but cryptographic algorithms shuffle and diffuse data by rounds of encryption [2]. Therefore, the security of chaos-based encryptions is defined on real numbers through mathematical models of nonlinear dynamics while conventional encryption operations are defined on finite sets. Such chaos-based encryption aspects consequently offer high flexibility in encryption design processes and acceptable privacy due to vast numbers of chaotic system variants and numerous possible encryption keys.

Chaos-based encryption algorithms are performed in two stages, i.e. the confusion stage that permutes the image pixels and the diffusion stage that spreads out pixels over the entire space. Most existing chaos-based encryptions based on such two-stage operations employ both initial conditions and control parameters of 1D, 2D, and 3D chaotic maps such as Baker map [23, 27], Arnold cat map [14, 24], and Standard map [12, 25] for secret key

generations. Furthermore, the combinations of two or three different maps have been suggested [4, 6] in order to achieve higher security levels. Despite the fact that such maps offer satisfactory security levels, iterations of maps require specific conditions of chaotic behaviors through a narrow region of parameters and initial conditions. Consequently, the use of iteration maps has become typical for most of proposed ciphers and complicated techniques in pixel confusion and diffusion are ultimately required.

Cellular Automata is a discrete system, which has been proven to be useful in the models of complexity and nonlinear dynamic systems. It consists of a set of cells and a new state of each cell depends on the rule number and the state of neighboring cells. Stephen Wolfram [26] initially employed a CA with the rule 30 to produce the pseudo-random number sequences, and extensive CA rules have been employed lately for data encryption [5, 15, 22].

As for compact and effective chaos-based data and image encryption, this paper presents a high-level security, very large key space and robust digital image encryption through the use of cellular automata sequences combined with chaotic systems. The proposed chaotic map uses absolute-value piecewise-linear nonlinearity and offers robust chaotic regions over broad parameter spaces with high degree of randomness through chaoticity measurements using the Lyapunov exponent. Experiments have been performed in MATLAB using standard color images. Nonlinear dynamics of the chaotic maps are initially investigated in terms of Cobweb map, chaotic attractor, Lyapunov exponent spectrum, bifurcation diagram, and 3-dimensional parameter spaces. Qualitative mesures of encryption performances are evaluated through pixel density histograms, 3-dimensional power spectral density, key space analysis, key sensitivity, and correlation plots. Additionally, quantitave measures of encryption performances are also indicated by correlation coefficients, NPCR and UACI. Practical application in Adndroid devices with correct-key and wrong-key decryptions are also demonstrated.

2 Detailed Descriptions of Proposed Chaotic Map and Cellular Automata

2.1 Proposed Chaotic Map

Chaotic system is typically a dynamic system that possesses some significant properties, involving the sensitive dependence on initial conditions and system parameters, the density of the set of all periodic points, and topological transitivity. Of a particular interest, a chaotic map is the lowest one-dimensional evolution function in discrete-time domain that exhibits chaotic behaviors. In general, chaotic systems reveal two types of chaotic attractors, i.e. (i) a fragile chaos in which the attractors disappear with perturbations of a parameter or coexist with other attractors, and (ii) a robust chaos, which is defined by the absence of periodic windows and coexisting attractors in some neighborhood of the parameter space. This paper alternatively proposes a mathematically simple chaotic map with robust chaos through the use of absolute-value piecewise-linear nonlinearity expressed as

$$x_{n+1} = |px_n - q| \tag{1}$$

As will be seen later, such mathematical simplicity of the proposed chaotic map in Equation (1) offers robustness that has no sensitivity on the change of system parameters. Investigations on chaotic behaviors of chaotic maps of Equation (1) can be achieved qualitatively and quantitatively through a bifurcation diagram and the Lyapunov Exponent (LE), respectively. The bifurcation diagram indicates possible long-term values, involving fixed points or periodic orbits, of a system as a function of a bifurcation parameter. The stable solution is represented by a straight line while the unstable solutions are generally represented by dotted lines, showing thick regions. On the other hand, the LE is defined as a quantity that characterizes the rate of separation of infinitesimally close trajectories and is expressed as

$$LE = \lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log_2 \frac{dx_{n+1}}{dx_n} \tag{2}$$

where N is the number of iterations. Typically, the positive LE indicates chaotic behaviors of dynamical systems and the larger value of LE results in higher degree of chaoticity. Dynamic properties can be described in terms of Cobweb plots, bifurcations, Lyapunov exponents, and chaotic waveforms in time domain. The system in Equation (1) possesses two fixed points P_{x1} and P_{x2} as follows

$$P_{x1} = \frac{q}{p-q} \text{ and } P_{x2} = \frac{q}{p+q} \tag{3}$$

The corresponding Jacobian is given by

$$|p \text{ sign}\,(q + px)| \tag{4}$$

The map has the only two parameters p and q that set dynamic properties of the systems. Simulation results have been performed using MATLAB with the initial condition of x_0=0.01. Figure 1 shows the Cobweb plots of the proposed chaotic map where the iterations are dense corresponding to the two fixed points described in Equation (3). Figures 2 and 3 show the bifurcation diagram and the LE spectrum of Equation (1) where p is in the region [0-2] and q is set to be 2. It is apparent in Figures 2 and 3 that there are no periodic windows appear, i.e. smooth chaos, in the bifurcation diagram and the LE spectrum is smoothly varied corresponding to the bifurcation diagram. Figure 4 shows an apparently chaotic waveform in time-domain.

2.2 Cellular Automata

Cellular Automata (CA) were first devised by Stanislaw Ulam and John von Neumann in the 1940s. Stephen Wolfram published a book entitled "A New Kind of Science"

Table 1: All possible neighborhoods and the outcome of rule 30

left	center	right	outcome
1	1	1	0
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	0

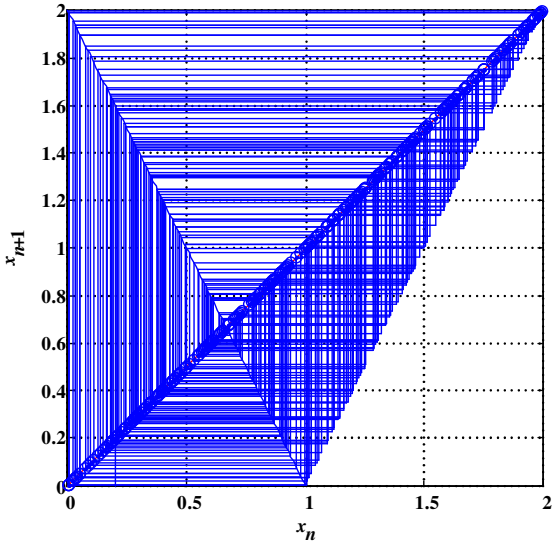


Figure 1: The Cobweb plots of the proposed chaotic map

in 2002, mentioning that cellular automata can be applied in many areas of science, including computer processors and cryptography. Elementary Cellular Automata are composed of cells positioned in a grid, each cell change a state depending on the states of its neighboring cells. For example, the outcomes of all possible neighborhoods for the rule 30 ($30 = 00011110_2$) are illustrated in Table 1 and Figure 5.

Starting with a single black cell, the first 12 steps of the evolution for rule 30 are demonstrated in Figure 6. The produced patterns of CA with some specific rules are shown in Figure 7. It can be noticed that some rules such as rules 30 and 101 potentially produce the chaotic behaviors which can be employed in the cryptography. The results of [20] concluded that rules 30, 86, 90, 101, 105, 150, 153, 165 are able to generate pseudorandom number sequences of a very high randomness quality and the CA-based system is very robust against the attempts of breaking the cryptography key.

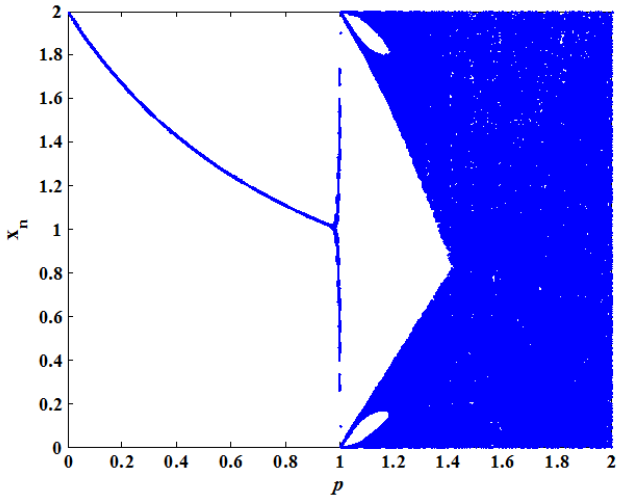


Figure 2: The bifurcation diagram in the range p=[0,2]

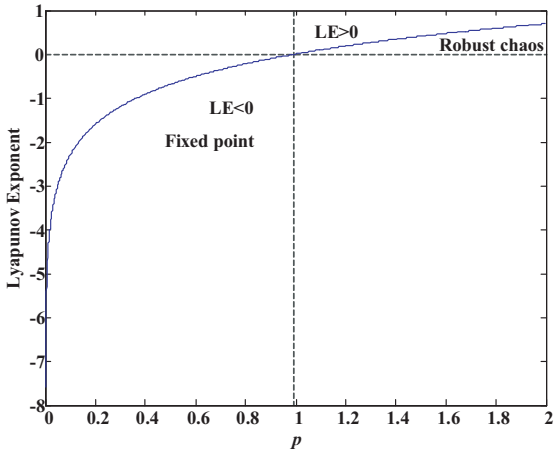


Figure 3: The LE spectrum in the range p=[0,2]

3 Proposed Data Encryption Using Chaotic Map and Cellular Automata

The whole structure of the proposed digital image encryption scheme using chaotic map and cellular automata is shown in Figure 8. The procedures for this encryption are described as follows:

1) The keys of the proposed scheme include parameters, involving initial conditions and system constants.

2) The original image is decomposed into red, green and blue components and each component is converted into binary format.

3) $W \times H$ iterations are required for the absolute chaotic map in order to generate the chaotic matrix X, where W and H are the width and height of original image in binary format. The $n{+}1^{th}$ element of the chaotic matrix can be calculated as in Equation (1) where

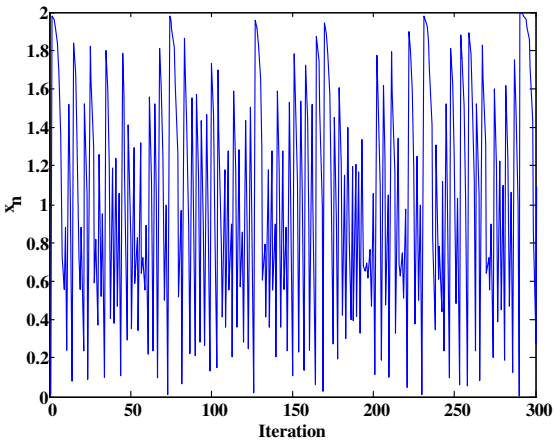


Figure 4: The apparently chaotic waveforms in time-domain

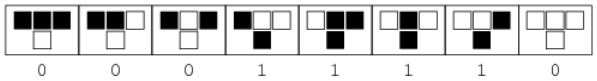


Figure 5: The outcome for every possible neighborhoods for rule 30

n=1, 2, ..., $W \times H$ and the value of p is given by

$$p = p_0 + \frac{\sum_{i,j,k} O(i,j,k)}{W \times H \times 255 \times 3 \times 10^6} \quad (5)$$

where the value p_0 is in a range of 1.999998 to 1.999999. Let $O(i,j,1)$, $O(i,j,2)$ and $O(i,j,3)$ be the intensity level of $(i,j)^{th}$ pixel of red, green and blue components, respectively.

4) X is transformed into a chaotic matrix with 2-dimension of $W \times H$.

5) The red, green and blue components and the chaotic matrix are combined through bitwise XOR operations.

6) The CA rule number and the bit sequence of the first row of CA matrix are chosen. Then the CA matrix is generated.

7) The encrypted red, green, and blue components are obtained by operating bitwise XOR on the two dimensional cellular automata matrix and the outcome of Step 5.

8) Finally, the encrypted red, green, and blue components are combined to form the encrypted image.

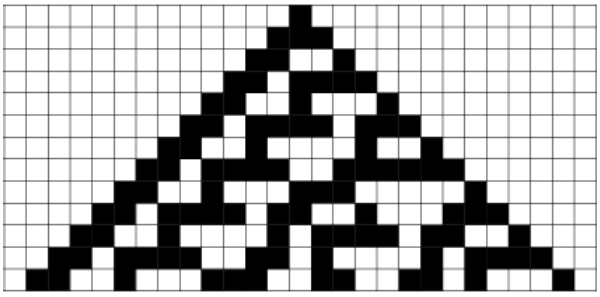


Figure 6: The first 12 steps of the evolution for rule 30

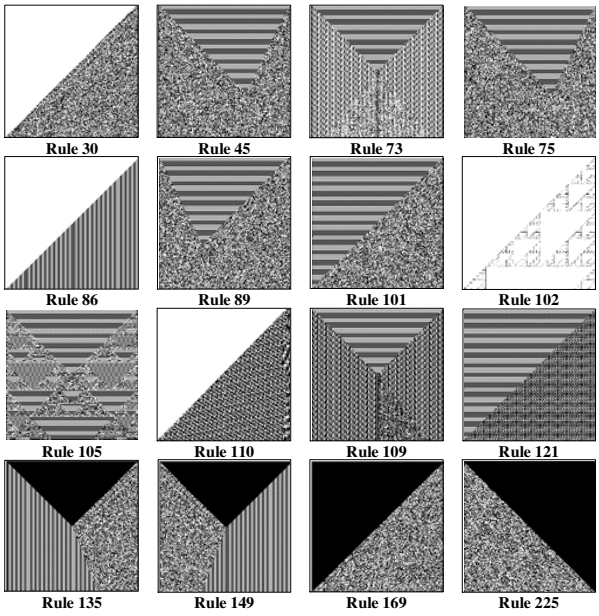


Figure 7: The produced patterns of CA rules

The decryption procedure is similar to that of encryption demonstrated above with reverse of encrypted image as input instead of original image in the encryption procedure.

The proposed encryption scheme can also be applied to any other data type such as plaintext as shown in Figure 9. The plaintexts in excel file and text file are illustrated in Figures 10 and 12. After encryption, the encrypted data in excel and text files can be shown in Figures 11 and 13.

4 Security Analysis

In order to evaluate the security of the proposed scheme, the key space analysis, histogram analysis, the correlation coefficient analysis of two adjacent pixels and differential attack analysis are performed.

4.1 Sensitivity Analysis

An ideal image encryption procedure should be sensitive with respect to the secret key, i.e., the change of a single bit in the secret key should produce a completely different encrypted image. The following experiments and results show key sensitivity of the presented scheme. An original image illustrated in Figure 14 is encrypted by using the correct key and the encrypted image is shown in Figure 15. Figure 16 illustrates the decrypted image using the right key. If there is only one bit difference between the encryption and decryption keys, an unexpected image

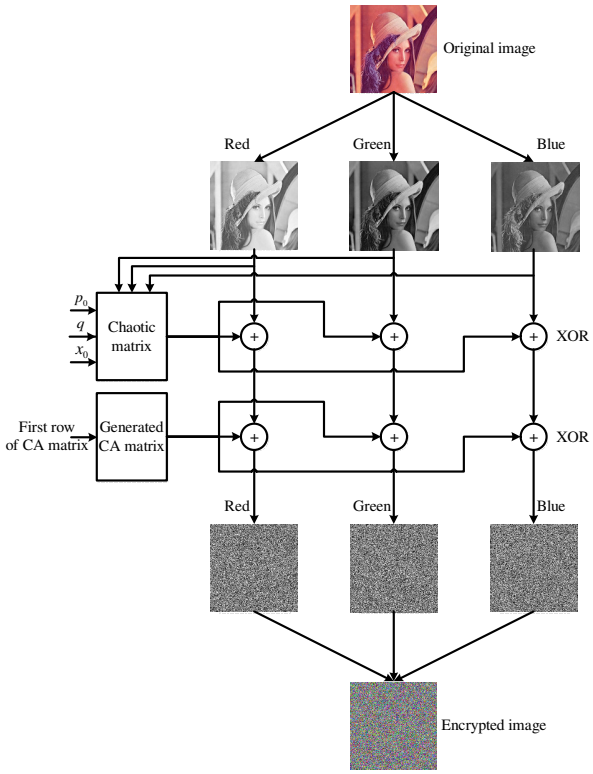


Figure 8: Proposed digital image encryption

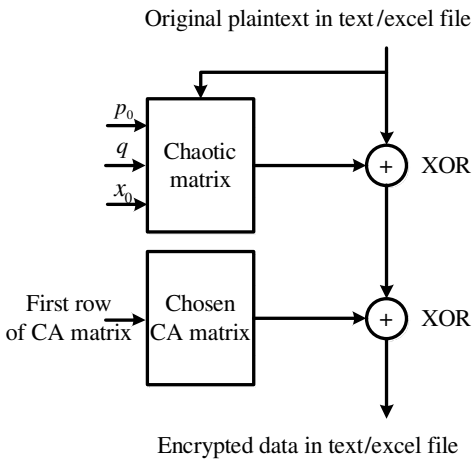


Figure 9: Proposed plaintext encryption in text/excel file

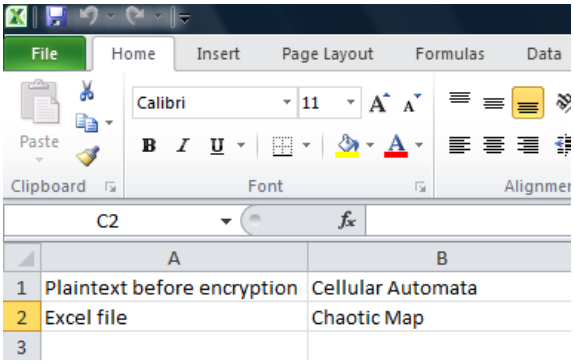


Figure 10: Plaintext before encryption in excel file

will be obtained as illustrated in Figure 17. So it can be concluded that the proposed encryption scheme is highly sensitive to the keys.

4.2 Key Space Analysis

Key space for the scheme means the number of all possible keys that can be adopted to encrypt data. Key space size ought to be sufficiently large, making brute-force attacks infeasible. For the proposed scheme, the initial conditions such as values of p_0, q and x_0, CA rule number and the bit sequence of the first row of CA matrix are used as keys. If the precision is 10^{-12} and as described before there are 8 possible CA rules that can be used for encryption such that the key space contains $10^{12}\times10^{12}\times10^{12}\times8\times2^{w}$ or $2^{w+3}\times10^{36}$ possible keys, where w, the length of the bit sequence of the first row of CA matrix, is equal to the width of original image in binary format W. As can be seen, the key space size is large enough to withstand the brute-force attacks.

4.3 Histogram Analysis (Histograms of Encrypted Image)

Histogram is a useful tool that displays the tonal distribution of a digital image. It illustrates the number of pixels at each intensity level. The histograms of red, green, and blue components of original and encrypted images are demonstrated in Figure 18. It can be noticed that particular intensity levels are dominant in the original images whereas the intensity levels of the encrypted image are uniformly distributed on [0, 255]. Consequently, it does not provide any information to perform any statistical analysis attack on the encrypted image.

4.4 3D Power Spectral Analysis

Discrete Fourier Transform (DFT) analysis can be used to attained the 3D power spectrum and the power spectral density is given by [18].

$$P(u,v)=\sum_{x=0}^{W-1}\sum_{y=0}^{H-1} I(x,y)\cdot\exp(-j(2\pi/W)ux)\cdot\exp(-j(2\pi/H)vy) \quad (6)$$

where (x,y) represents the coordinate of pixels in the image, W and H are width and height of the image, $I(x,y)$ is intensity value of image at (x,y). The power spectral densities of the original and encrypted images are demonstrated in Figure 19. The original image has a peak power spectral density at the center while the power spectral density of the encrypted image is flat. The results indicate that the intensity values of the encrypted image are uniformly distributed all over the intensity range. This means that the encryption scheme is secure, as there is no information leakage.

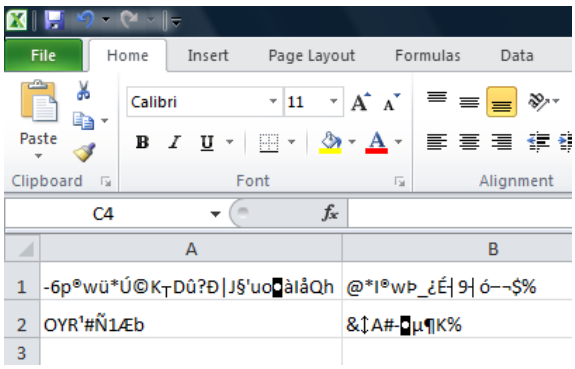


Figure 11: Encrypted data in excel file

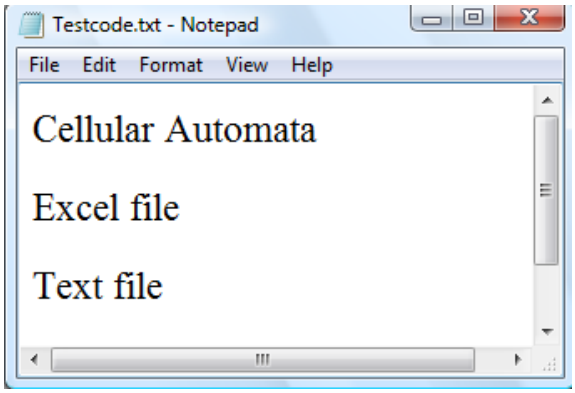


Figure 12: Plaintext before encryption in text file

4.5 Correlation Coefficient Analysis of Two Adjacent Pixels

A correlation is a statistical method that is used to measure degree of similarity between pairs of variables. In order to illustrate the relationship between two adjacent pixels in the digital image, correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in the original and encrypted images are analyzed.

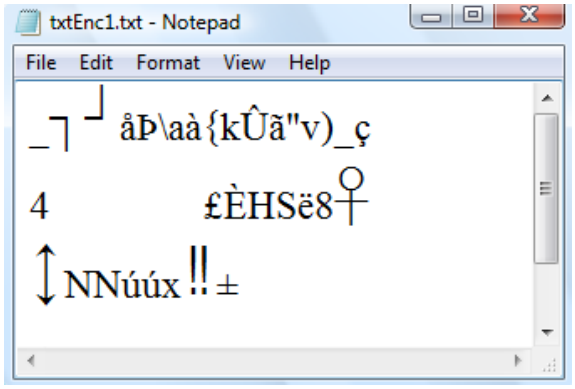


Figure 13: Encrypted data in text file

Figure 14: Original image

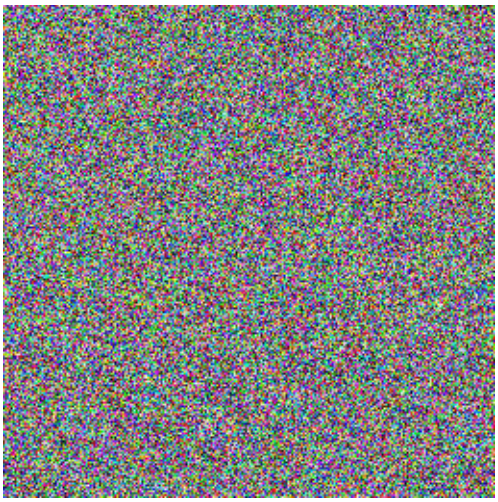


Figure 15: Encrypted image

The correlation coefficient is computed as follows:

$$C_r = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N} x_i \times \sum_{i=1}^{N} y_i}{\sqrt{\left(N\sum_{i=1}^{N} x_i^2 - \left(\sum_{i=1}^{N} x_i\right)^2\right)\left(N\sum_{i=1}^{N} y_i^2 - \left(\sum_{i=1}^{N} y_i\right)^2\right)}} \quad (7)$$

where x_i and y_i are the intensity level of two adjacent pixels and N is overall number of pixels in the digital image. Figure 20 illustrates the correlation distribution of two horizontally adjacent pixels in the original image and encrypted image. It can be noticed that the adjacent pixels of all encrypted images are highly unrelated demonstrated by scatter graphs. The correlation coefficients are illustrated in Table 2. As can be seen, the value of correlation coefficient of the encrypted image is nearly zero. This reveals that two adjacent pixels are extremely unrelated.

Table 2: Simulated correlation coefficient of the original and encrypted images

Correlation of Images	Correlation Coefficient Values
C_{RR}	-0.0020
C_{RG}	0.0050
C_{RB}	-0.0006
C_{GR}	-0.0015
C_{GG}	0.0009
C_{GB}	0.0009
C_{BR}	-0.0020
C_{BG}	0.0002
C_{BB}	0.0006

Table 3: Summary of NPCR and UACI tests

Measures	Proposed scheme	2D Baker map	DES
NPCR (red)	99.6155	99.5132	0.0045
NPCR (green)	99.6124	99.5407	0.0045
NPCR (blue)	99.6094	99.5849	0.0030
UACI (red)	33.3399	32.1693	0.0012
UACI (green)	33.3458	32.1788	0.0026
UACI (blue)	33.2698	32.3173	0.0089

Figure 16: Decrypted image using the right key

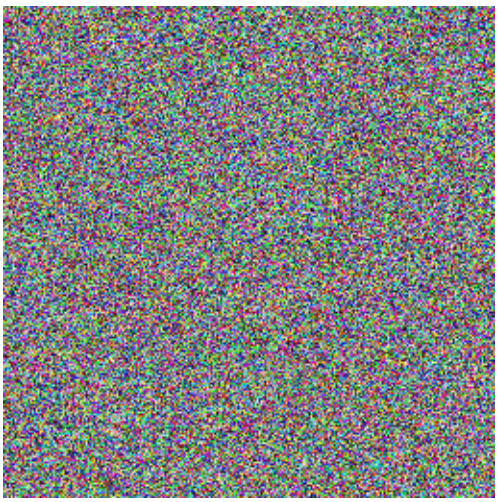


Figure 17: Decrypted image using the wrong key

4.6 Analysis of Differential Attack

In order to observe a relationship between the original image and the encrypted image, the rival may alter only one pixel of the original image, and then notices the difference of the outcome. A substantial change of the outcome is expected to make this differential attack infeasible. To see the impact of altering one pixel in plaintext image on the encrypted image. Two most common standards, Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI), are used to evaluate the resistance against the differential attack. The NPCR determines the percentage of changed pixels between two encrypted images. The UACI measures the mean intensity of distinctions between two encrypted images. These two standards can be calculated as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (8)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\left|\frac{C_1(i,j) - C_2(i,j)}{255}\right|\right] \times 100\% \quad (9)$$

Let $C_1(i,j)$ and $C_2(i,j)$ be $(i,j)^{th}$ pixel of two differ-

Table 4: Information entropy test

Test item	Proposed scheme	2D Baker map	DES
Information entropy	7.999223	7.999158	7.999096

Table 5: NIST statistical test suite results for one hundred 1 M-bit sequences generated using randomly initial condition

Statistical test	p-value	Pass rate
Frequency	0.537894	1.00
Block frequency	0.919617	0.99
Runs	0.747165	0.98
Long runs of ones	0.061725	0.99
Rank	0.490471	0.97
Discrete Fourier Transform (Spectral)	0.912314	1.00
Non overlapping templates	0.113991	0.96
Overlapping templates	0.022266	0.99
Universal	0.666870	0.98
Linear complexity	0.232466	0.98
Serial 1	0.741995	1.00
Serial 2	0.677427	1.00
Approximate entropy	0.444053	0.96
Cumulative sums (forward)	0.642075	0.96
Cumulative sums (reward)	0.493507	0.96
Random excursions	0.465971	0.97
Random excursions variant	0.307470	0.97

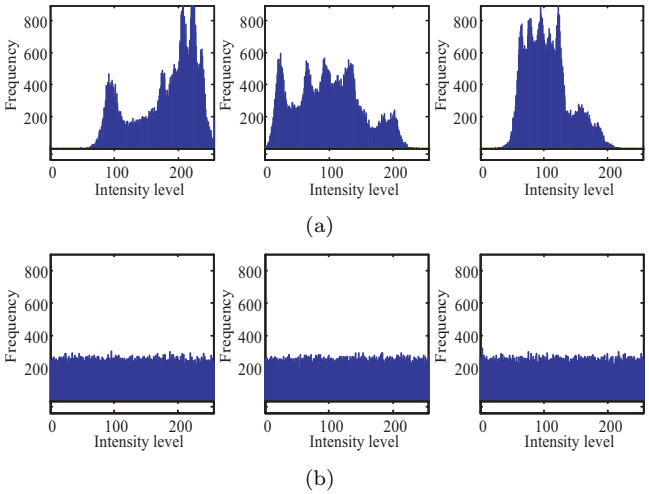


Figure 18: Histograms of RGB components: (a) Original image, (b) Encrypted image

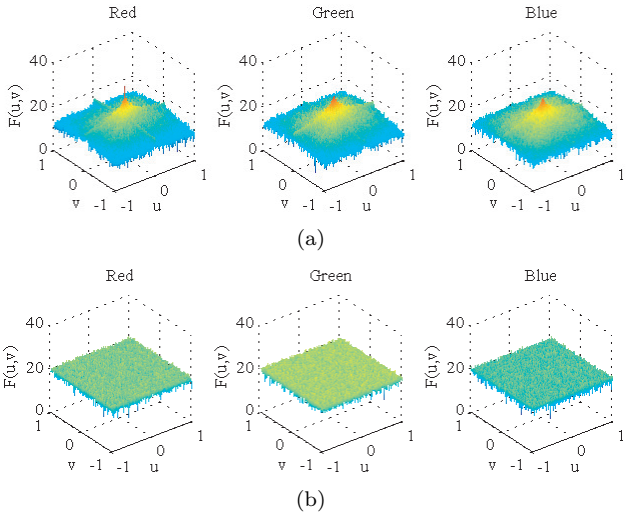


Figure 19: 3D power spectral density: (a) Original image, (b) Encrypted image

ent encrypted-images. The parameters W and H are the width and height of encrypted-images and $D(i,j)$ is defined as follows:

$$D(i,j) = \begin{cases} 1, & if C_1(i,j) \neq C_2(i,j) \\ 0, & if C_1(i,j) = C_2(i,j) \end{cases} \quad (10)$$

The experimental results comparison with 2D Baker map and DES schemes are illustrated in Table 3. The obtained values obviously demonstrate that changing of one pixel in the original image leads to a substantial change in the encrypted image, therefore the proposed scheme is secure against differential attacks.

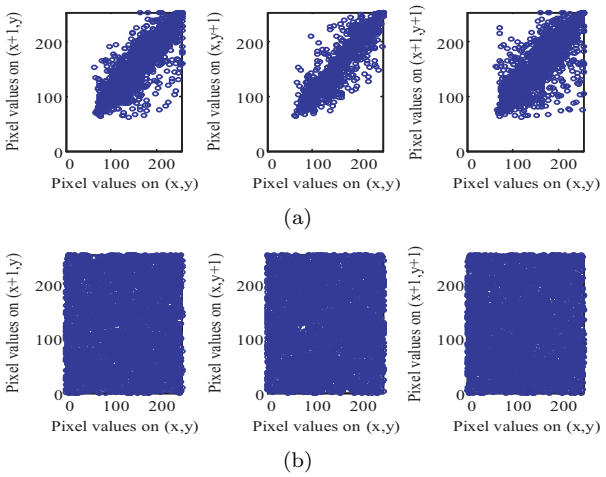


Figure 20: Image correlation experiments comprising horizontally, vertically, and diagonally adjacent pixels: (a) Original image, (b) Encrypted image

4.7 Information Entropy Analysis

Information entropy can be determined as a probabilistic measure of uncertainty associated with a random variable. It can be calculated as follows:

$$H(S) = \sum_{S} P(s_i) \log_2 \frac{1}{P(s_i)} \tag{11}$$

$P(s_i)$ denotes the probability of symbol s_i. The test results comparison with 2D Baker map and DES schemes are demonstrated in Table 4. The entropy value acquired approaches the theoretical value of 8, demonstrating that the proposed scheme is secure against the attacks.

4.8 NIST Statistical Tests

NIST statistical tests [16] are employed for examining the random sequences. The NIST test suite is a statistical package composing of 16 tests that are used to test the randomness of binary sequences generated by software or hardware. These tests concentrate on a various types of non-randomness that may appear anywhere in a sequence. For each of these tests, one hundred sequences of length 10^6 bits are tested. In accordance with NIST document, a pass rate of 96% is satisfactory. A test results are shown in Table 5. The achieved results illustrate the supreme statistical properties of the generated random sequences.

4.9 Flexibility and Speed Analysis

The proposed encryption scheme is flexible since there is no restriction on the size of the original data and it can encrypt many different types of data, such as plaintext, binary data and digital image. The running speed of the encryption scheme, on a 3.20 GHz Intel(R) Xenon(R) computer with 16 GB of RAM running Windows 7 (64-bit) is about 9.3 Mb/s (Megabits per second).

5 Comparison of Proposed Scheme with Other Existing Techniques

The proposed scheme is analyzed and compared with the existing (a) chaotic map and (b) chaotic flow in terms of numbers of terms in equation, calculation time, text encryption and decryption, type of characters, key space, the positive LE value (LE $>$ 0), key sensitivity, robust chaos and power spectrum, as illustrated in Table 6. From Table 6, it can be concluded that the proposed scheme offers better aspects and performances than other chaotic schemes. For instance, the computational time of the proposed scheme is relatively fast due to low-dimension of system order comparing to the 3rd-order chaotic flows that require particular algorithms to solve for ordinary differential equations. The proposed scheme can be applied to text encryption and decryption based on Unicode system and ASCII. Key space is equal to $2^{w+3}\times10^{36}$ digits, where w is the length of the bit sequence of the first row of CA matrix. The key space is large enough to make the attack infeasible. The system is truly chaotic (LE $>$ 0) with robust chaos and sensitive to keys. Moreover, the power spectral density of the encrypted data is uniformly distributed.

6 Security Implementation

As for illustration, the proposed image encryption scheme will be implemented on an Android device in order to protect the important and confidential data. Figure 21 demonstrates Android application user interface for the encryption. The procedures for the image encryption are described as follows:

1) Input the system parameters (p_0, q and x_0).
2) Locate the image file (.PNG) of the initial bit sequence of the first row of CA matrix. This bit sequence is saved in PNG format for the convenience of both sender and receiver.
3) Choose and import the image to be encrypted.
4) Click on "ENCRYPT" button.
5) The results of the encryption are displayed on the screen.

The initial conditions and the image file (.PNG) of the initial bit sequence of the first row of CA matrix are shared between sender and receiver. The sender uses the shared key for encryption and the receiver uses the same shared key for decryption.

Android application user interface for the decryption is illustrated in Figure 22. The procedures for the image decryption are described as follows:

1) Input the system parameters (p_0, q and x_0).

Table 6: Performance comparison between the proposed scheme and other chaotic schemes, "/" is "Yes", "x" is "No" and "-" is "not presented in the paper".

Comparisons	Chaotic types					
	Chaotic maps		Chaotic flows			
	Proposed scheme	Logistic [3]	Jerk [21]	Lu [13]	Lorenz [9]	Rossler [19]
Terms in equation	2	2	5	6	7	7
Computational time	Fast	Fast	Low	Low	Low	Low
Text encryption/decryption	/	/	x	x	/	x
Type of characters	Unicode and ASCII	ASCII	x	x	ASCII	x
Key space	$2^{w+3}\times10^{36}$ digits	-	-	-	-	-
LE > 0	/	/	/	/	/	/
Robust chaos	/	x	x	x	x	x
Power spectrum	/	x	x	x	x	x
Key sensitivity	High	x	x	x	x	x

2) Locate the image file (.PNG) of the initial bit sequence of the first row of CA matrix.

3) Choose and import the encrypted image to be decrypted.

4) Click on "DECRYPT" button.

5) The results of the decryption are displayed on the screen.

These results confirm that the proposed encryption scheme can protect the important and confidential data on Android device.

7 Conclusions

The data encryption scheme based on rules of Cellular Automata and chaotic map function has been proposed. The proposed chaotic map exploits absolute-value piecewise-linear nonlinearity that offers robust chaotic regions over broad parameter spaces with high degree of randomness. Cellular Automata has also been used to generate pseudo-random number sequences with a very high randomness. A combination of cellular automata sequences and chaotic system has been realized in order to achieve a high level of security and adequately large key space. The proposed scheme is flexible since it can take the original data of any length and encrypt many types of data, such as plaintext, binary data and digital image. Experimental results reveal that the proposed scheme has many important features including: (i) high sensitive to the key and original message, (ii) large key space, (iii) resistant to various attacks such as the brute-force, statistical and differential attacks, and (iv) high data encryption speed. These properties make the proposed data encryption scheme to be suitable for real-time implementation as demonstrated in smart phone with Android operating system.

Acknowledgments

The authors are grateful to Thai-Nichi Institute of Technology for financial supports. The authors would also like to thank Mr. Sivapong Nilwong for his useful suggestions.

References

[1] C. C. Chang, Y. Liu, G. Song, Y. Liu and D. Wang, "Digital image scrambling algorithm based on Chaotic sequence and decomposition and recombination of pixel values," *International Journal of Network Security*, vol. 17, no. 3, pp. 322–327, 2015.

[2] G. Chen, Y. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, pp. 749–761, 2004.

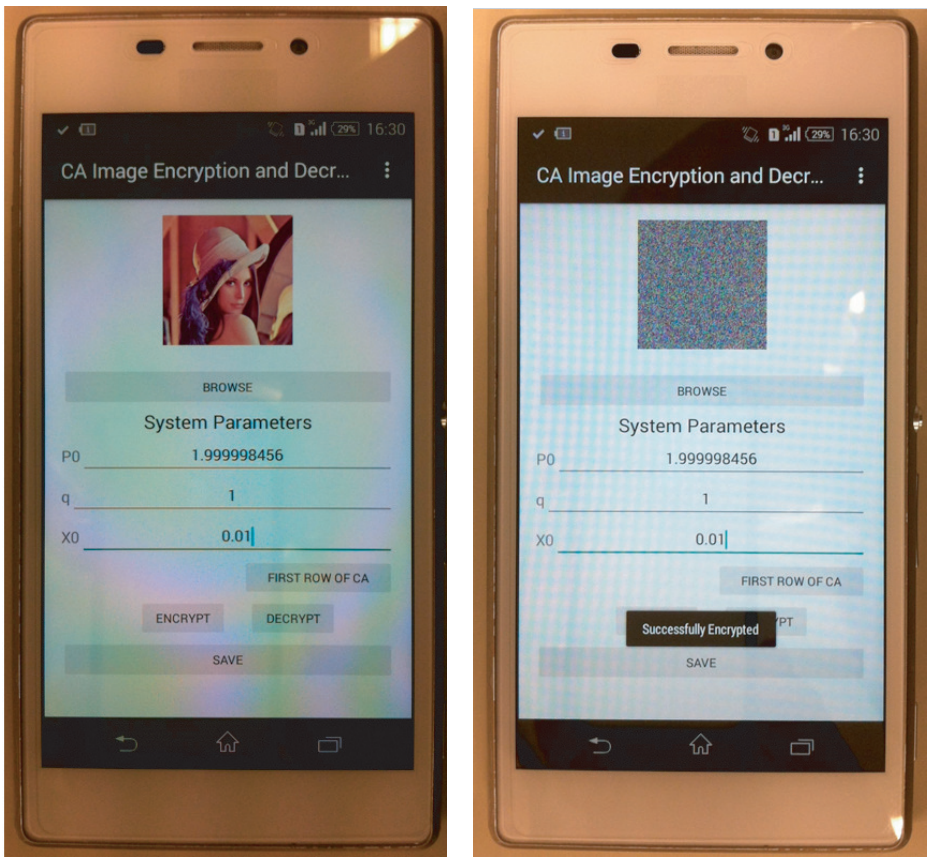
[3] C. K. Chen, C. L. Lin and Y. M. Chiu, "Text encryption using ECG signals with chaotic Logistic map," *IEEE International Conference on Industrial Technology*, pp. 1741–1746, 2010.

[4] K. Gupta and S. Silakari, "New approach for fast color image encryption using chaotic map," *Journal of Information Security*, vol. 2, no. 4, pp. 139–150, 2011

[5] S. U. Guan, S. Zhang, and M. Quieta, "2-D CA variation with asymmetric neighborship for pseudo-random number generation," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 3, pp. 378–388, 2004.

[6] F. Huang and Y. Feng, "Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm," *Frontiers of Electrical and Electronic Engineering in China*, vol. 4, no. 1, pp. 5–9, 2009.

[7] H. F. Huang, P. H. Lin and M. H. Tsai, "Convertible multi-authenticated encryption scheme for data communication," *International Journal of Network Security*, vol. 17, no. 1, pp. 40–48, 2015.



(a) (b)

Figure 21: Android application user interface: (a) Original image for the encryption process, (b) The encrypted image

[8] I. A. Ismail, M. Amin and H. Diab, "A digital image encryption algorithm based a composition of two chaotic Logistic maps," *International Journal of Network Security*, vol. 11, no. 1, pp. 1–10, 2010.

[9] Y. Ji, C. Wen and Z. G. Li, "A practical chaotic secure communication scheme based on Lorenz model," *Proceedings of the 4th International IEEE Conference on Industrial Informatics (INDIN'06)*, pp. 576–580, 2006.

[10] G. H. Karimian, B. Rashidi and A. Farmani, "A high speed and low power image encryption with 128-bit AES algorithm," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 3, pp. 367, 2012.

[11] C. C. Lee, S. T. Chiu and C. T. Li, "Improving security of a communication-efficient three-party password authentication key exchange protocol," *International Journal of Network Security*, vol. 17, no. 1, pp. 1–6, 2015.

[12] 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.

[13] J. Lu, G. Chen and S. Zhang, "The compound structure of a new chaotic attractor," *Chaos, Solitons and Fractals*, vol. 14, no. 5, pp. 669–672, 2002.

[14] X. Ma, C. Fu, W. Lei and S. Li, "A novel chaos-based image encryption scheme with an improved permutation process," *International Journal of Advancements in Computing Technology*, vol. 3, no. 5, pp. 223–233, 2011.

[15] S. Nandi, B. K. Kar and P. P. Chaudhuri., "Theory and applications of cellular automata in cryptography," *IEEE Transactions on Computers*, vol. 43, no. 12, pp. 1346–1357, 1994.

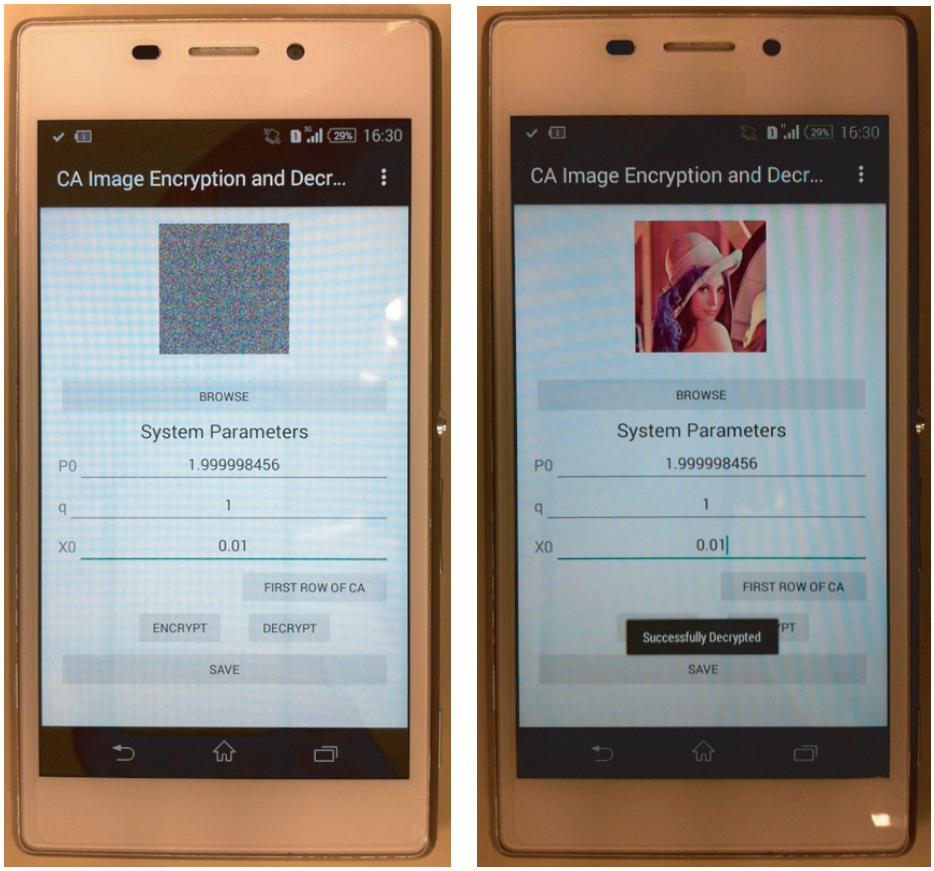
[16] NIST Special Publication 800-22 rev1, A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications, online document, 2008. (<http://www.csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html>)

[17] M. Philip, "An enhanced chaotic image encryption," *International Journal of Computer Science*, vol. 1, no. 5, pp. 201, 2011.

[18] Z. Peng, T. B. Kirk, "Two-dimensional fast Fourier transform and power spectrum for wear particle analysis," *Tribology International*, vol. 30, no. 8, pp. 583–590, 1997.

[19] O. E. Rössler, "An equation for continuous chaos," *Physics Letters A*, vol. 57, no. 5, pp. 397–398, 1976.

[20] F. Seredynski, P. Bouvry and A. Y. Zomaya, "Cellular programming and symmetric key cryptography



(a) (b)

Figure 22: Android application user interface: (a) Original image for the decryption process, (b) The decrypted image

systems," *Genetic and Evolutionary Computation*, pp. 1369–1381, 2003.

[21] B. Srisuchinwong, "Chaos in a fractional-order Jerk model using tanh nonlinearity," *Proceedings of the 2nd Chaotic Modeling and Simulation International Conference*, pp. 1–8, 2009.

[22] F. Seredynski, P. Bouvry and Albert Y. Zomaya, "Cellular automata computations and secret key cryptography," *Parallel Computing*, vol. 30, no. 5, pp. 753–766, 2004.

[23] X. Tong and M. Cui, "Image encryption scheme based on 3D Baker with dynamical compound chaotic sequence cipher generator," *Signal Processing*, vol. 89, pp. 480–491, 2009.

[24] K. Wang, W. Pei, L. Zou, A. Song and Z. He, "On the security of 3D Cat map based symmetric image encryption scheme," *Physics Letters A*, vol. 343, no. 6, pp. 432–439, 2005.

[25] K. Wong, B. Kwok, and W. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters A*, vol. 372, no. 15, pp. 2645–2652, 2008.

[26] S. Wolfram, "Cryptography with cellular automata," *Advances in Cryptology*, LNCS 218, pp. 429–432, Springer, 1985.

[27] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.

Warakorn Srichavengsup obtained the B.Eng., M.Eng. and Ph.D. degree in Electrical Engineering from Chulalongkorn University, Bangkok, Thailand, in 1998, 2003 and 2009, respectively. He is currently a lecturer with the Department of Computer Engineering at Faculty of Engineering, Thai-Nichi Institute of Technology (TNI), Bangkok, Thailand. Prior to joining TNI, he was a visiting research student during 2008 with the Laboratory for Information and Decision Systems (LIDS) at the Massachusetts Institute of Technology (MIT). His main research interests are MAC protocol for high speed wireless local area networks, computer cryptography and information security.

Wimol San-Um was born in Nan Province, Thailand in 1981. He received B.Eng. Degree in Electrical Engineering and M.Sc. Degree in Telecommunications in 2003 and 2006, respectively, from Sirindhorn International Institute of Technology (SIIT), Thammasat University in Thailand. In 2007, he was a research student at

University of Applied Science Ravensburg-Weingarten in Germany. He received Ph.D. in mixed-signal very large-scaled integrated circuit designs in 2010 from the Department of Electronic and Photonic System Engineering, Kochi University of Technology (KUT) in Japan. He is currently with Master of Engineering Technology program, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). He is also the head of Intelligent Electronic Systems (IES) Research Laboratory. His areas of research interests are chaos theory, artificial neural networks, control automations, digital image processing, secure communications, and nonlinear dynamics of chaotic circuits and systems.