Robust Digital Image Cryptosystem Based on Nonlinear Dynamics of Compound Sine and Cosine Chaotic Maps for Private Data Protection

Sarun Maksuanpan, Tanachard Veerawadtanapong, Wimol San-Um

Intelligent Electronics Systems Research Laboratory

Faculty of Engineering, Thai-Nichi Institute of Technology, Patthanakarn Rd., Suanlaung, Bangkok, Thailand

sarun.maksuanpan@gmail.com, tanachad.p@gmail.com, and wimol@tni.ac.th

***Abstract*—this paper presents a digital image cryptosystem based on nonlinear dynamics of a compound sine and cosine chaotic map. The compound sine and cosine chaotic map is proposed for high-degree of chaos over most regions of parameter spaces in order to increase high-entropy random-bit sources. Image diffusion is performed through pixel shuffling and bit-plane separations prior to XOR operations in order to achieve a fast encryption process. Security key conversions from ASCII code to floating number for use as initial conditions and control parameters are also presented in order to enhance key-space and key-sensitivity performances. Experiments have been performed in MATLAB using standard color images. Nonlinear dynamics of the chaotic maps were initially investigated in terms of Cobweb map, chaotic attractor, Lyapunov exponent spectrum, bifurcation diagram, and 2-dimensional parameter spaces. Encryption qualitative performances are evaluated through pixel density histograms, 2-dimensional power spectral density, key space analysis, key sensitivity, vertical, horizontal, and diagonal correlation plots. Encryption quantitative performances are evaluated through correlation coefficients, NPCR and UACI. Demonstrations of wrong-key decrypted image are also included.**

***Keyword*— Digital Image Processing, Cryptosystem, Chaotic Map, Encryption, Decryption, Nonlinear Dynamics**

Manuscript received March 7, 2013. This work was financially supported by Research and Academic Services Division, Thai-Nichi Institute of Technology.

Sarun Maksuanpan is with computer engineering program, Faculty of Engineering, Thai-Nichi Institute of technology, Bangkok, Thailand. (E-mail: sarun.maksuanpan@gmail.com).

Tanachard Veerawadtanapong is with Computer Engineering Program, Faculty of Engineering, Thai-Nichi Institute of technology, Thailand. (E-mail: tanachad.pong@gmail.com).

Wimol San-Um is with the Intelligent Electronics Systems Research Laboratory, Faculty of Engineering, Thai-Nichi Institute of Technology, Bangkok, Thailand, Fax: (+662) 7632700, Tel: (+662) 7632600 Ext. 2926, (E-mail: wimol@tni.ac.th).

I. INTRODUCTION

RECENT advances in communications have led to great demand for secured image transmissions for a variety of applications such as medical, industrial and military imaging systems. The secured image 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 [1]. 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 large computational time and high computing power, especially for the images with large data capacity and high correlation among pixels [2].

Recently, the utilization of chaotic systems has extensively been suggested as one of a potential alternative cryptography in secured image transmissions. As compared to those of conventional encryption algorithms, chaos-based encryptions are sensitive to initial conditions and parameters whilst 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 [3]. 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 1-D, 2-D, and 3-D chaotic maps such as Baker map [4,5], Arnold cat map [6,7], and Standard map [8, 9] for secret key generations. Furthermore, the combinations of two or three different maps have been suggested [10, 11] 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.

This paper therefore presents an alternative chaos-based digital image cryptosystem with three main aspects. First, the compound sine and cosine chaotic maps, which potentially offers high-degree of chaos over most regions of parameter spaces, is proposed through nonlinear dynamics analyses and is consequently exploited as high-entropy random-bit sources for encryption. Second, image confusion and diffusion processes are performed through uncomplicated pixel shuffling and bit-plane separations prior to XOR operations in order to achieve a fast encryption process. Last, security key conversions from ASCII code to floating number for use as initial conditions and control parameters are also presented in order to enhance key-space and key-sensitivity performances.

II. PROPOSED ENCRYPTION ALGORITHMS

A category of trigonometric functions, involving sine and cosine maps, have potentially offered rich dynamic behaviours as described in a simple forms as [12] $x_{n+1}=\sin(ax_n)$ and $x_{n+1}=\cos(bx_n)$ where the constants a and b can be considered as the parameters associated the frequencies of sine and cosine functions, respectively. Although such sine and cosine maps offers relatively high complexity in terms of nonlinear dynamics, the chaotic regions in the bifurcation diagram is still insufficient due to periodic characteristics. This paper therefore considers an enhancement of sine and cosine maps through the combination between sine and cosine maps, i.e.

$$x_{n+1} = \cos(ax_n) + \sin(bx_n) \quad (1)$$

As will be seen later, such a compound sine and cosine map in (1) offers high-degree of chaos over most regions of parameter spaces. As a nature of chaotic maps, the initial conditions and control parameters can be used as internal security keys that entirely set the encryption characteristics. The proposed cryptography technique attempts to achieve simple-but-highly-secured image encryption and decryption algorithms in a category of chaos-based cryptosystems. Fig.1 shows the proposed encryption and detection algorithms using compound sine and cosine maps. Three major procedures are summarized as follows;

First, the original image is prepared for diffusion. The

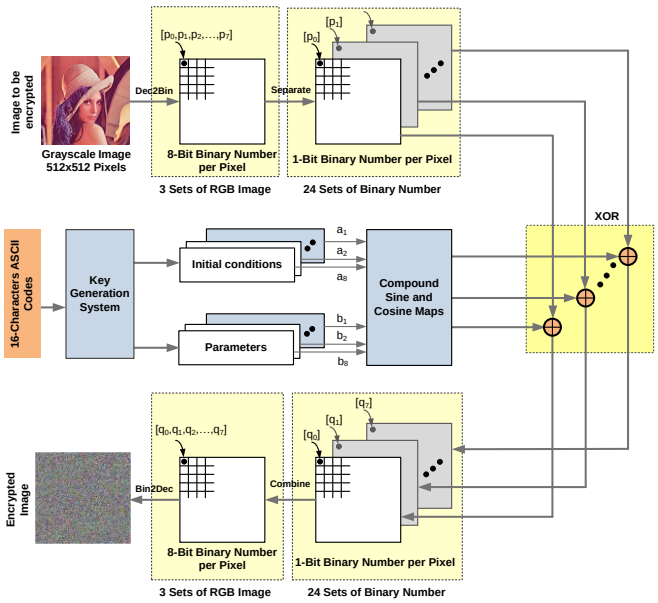


Fig. 1. Proposed pncryption algorithms using compound sine and consine chaotic maps.

TABLE I
SUMMARY OF 16-CHARACTERS INPUT ASCII CODES FOR SETTING INITIAL CONDITIONS AND CONTROL PARAMETERS

ASCII code X_m for Setting initial conditions		**ASCII code Y_m for setting control parameters**	
$\mathbf{X_1}$	: $A_1A_4A_7A_{10}A_{13}A_{16}$	$\mathbf{Y_1}$	: $A_1A_3A_5A_7A_9A_{11}$
$\mathbf{X_2}$	: $A_2A_5A_8A_{11}A_{14}A_1$	$\mathbf{Y_2}$	: $A_2A_4A_6A_8A_{10}A_{12}$
$\mathbf{X_3}$	: $A_3A_6A_9A_{12}A_{15}A_2$	$\mathbf{Y_3}$	: $A_3A_5A_7A_9A_{11}A_{13}$
$\mathbf{X_4}$	: $A_4A_7A_{10}A_{13}A_{16}A_3$	$\mathbf{Y_4}$	: $A_4A_6A_8A_{10}A_{12}A_{14}$
$\mathbf{X_5}$	: $A_5A_8A_{11}A_{14}A_1A_4$	$\mathbf{Y_5}$	: $A5A_7A_9A_{11}A_{13}A_{15}$
$\mathbf{X_6}$	: $A_6A_9A_{12}A_{15}A_2A_5$	$\mathbf{Y_6}$	: $A_6A_8A_{10}A_{12}A_{14}A_{16}$
$\mathbf{X_7}$	: $A_7A_{10}A_{13}A_{16}A_3A_6$	$\mathbf{Y_7}$	: $A_7A_9A_{11}A_{13}A_{15}A_1$
$\mathbf{X_8}$	: $A_8A_{11}A_{14}A_1A_4A_7$	$\mathbf{Y_8}$	: $A_8A_{10}A_{12}A_{14}A_{16}A_2$

original color image with $M\times N$ image size is initially converted into three sets of sub-images with RGB components containing pixels in grey scale levels. Each sub-image will subsequently be converted into binary matrix in which each pixel is represented by 8-bit binary numbers. For example, the pixel $p(1,1)$ contains the binary number p_0-p_7. Each pixel will then be separated into eight planes corresponding to binary bits p_0 to p_7. As a result, there are 24 sets of bit plane images represented in matrix forms with a single binary number in each pixel, which is ready for further Excusive-OR (XOR) operations.

Second, the input security keys from users which is represented in ASCII code with arbitrary 16 alphanumeric characters defined as $A=A_1A_2A_3,...,A_{16}$ will form two main sets of ASCII codes, i.e X_m and Y_m, for setting the initial conditions and the control parameters, respectively, where m = 1, 2, 3,...,8

as summarized in Table 1. Such two sets X_m and Y_m will be converted into 48-bit binary representations denoted by B_{X1} to B_{X48} and B_{Y1} to B_{Y48}, respectively. The real numbers are subsequently formed by converting the binary representation as follows;

$$R_{Xm} = (\mathrm{B}_{\mathrm{X1}} \times 2^0 + \mathrm{B}_{\mathrm{X1}} \times 2^1 + ... + \mathrm{B}_{\mathrm{X48}} \times 2^{47}) / 2^{48} \quad (2)$$

$$R_{Ym} = (\mathrm{B}_{\mathrm{Y1}} \times 2^0 + \mathrm{B}_{\mathrm{Y1}} \times 2^1 + ... + \mathrm{B}_{\mathrm{Y48}} \times 2^{47}) / 2^{48} \quad (3)$$

As a result, the initial conditions and the control parameters can be achieved by

$$a_m = (R_{Xm} \times R_{Ym}) \bmod 1 \quad (4)$$

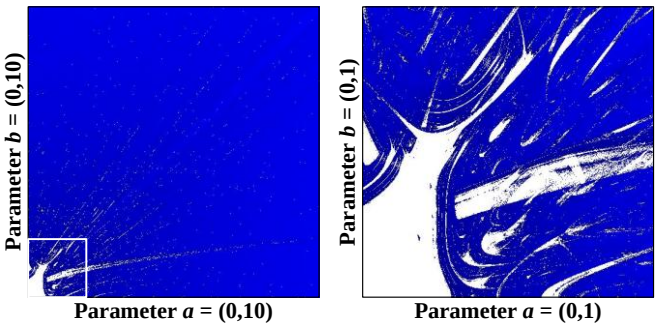
$$b_m = (R_{Ym} \times R_{Ym+1}) \bmod 1 \quad (5)$$

It is apparent that the values of a_{m} and b_{m} are in the region of (0,1) and are ready for use as internal security keys in the encryption algorithms. The design algorithm realizes eight chaotic maps based on (1) as follows;

$$x_{\mathrm{m,n+1}} = \cos(b_m 10\pi x_{\mathrm{n}}) + \sin(b_{m+1} 10\pi x_{\mathrm{n}}) \quad (6)$$

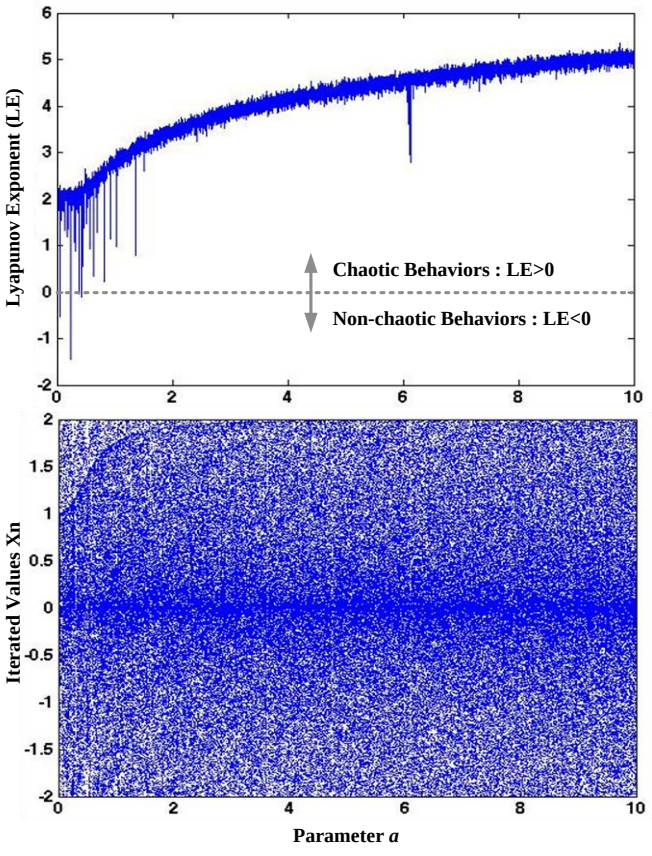
It is seen in (4) that the constant 10π has been include in order to sustain the parameters a and b described in (1) in the region of (0, 10) which is sufficient to acquire chaos. The values of m are circularly shifted with 1 to 8, i.e. if the operation round reaches m+1=8 then the next value is 1. As results, a total 16 keys are employed as security keys in the encryption process. Such keys are used to generate chaotic signal from the compound sine and cosine chaotic maps. The output signals are adjusted to the binary number through the zero thresholds for the subsequent XOR operations.

Last, the XOR operations diffuse the generated chaotic bit and the 24 binary images in parallel process. The XOR operation yields bit "1" if the two input bits are different, but yields bits "0" if the two inputs are similar. The results obtained from such XOR operations are 24 matrices with single binary number in each pixel. All the 24 matrices are combined into three RGB matrices of a single 8-bit matrix in which each pixel is represented by [b_0-b_7]. As a result, the encrypted image can be achieved. The decryption process also follows the encryption process in a backward algorithms as long as the security keys are known. It is seen in (4) that the constant 10π has been include in order to sustain the parameters a and b described in (1) in the region of (0, 10) which is sufficient to acquire chaos. The values of m are circularly shifted with 1 to 8, i.e. if the operation round reaches m+1=8 then the next value is 1. As results, a total 16 keys are employed as security keys in the encryption process. Such keys are used to generate chaotic



(a) (b)

Fig. 2. Plots of 2-D Lyapunov Exponent bifurcation structure between parameters a and b over the parameter space; (a) (0,10) and (b) the zoomed in region (0,1).

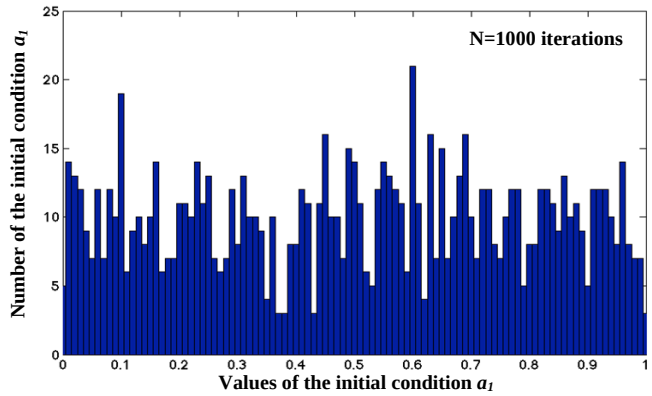


(b) (b)

Fig. 3. Plots of the Lyapunov exponent spectrum and the bifurcation diagram of parameters a over the parameter space (0,10) when the parameter b is fixed at 0.5.

signal from the compound sine and cosine chaotic maps. The output signals are adjusted to the binary number through the zero thresholds for the subsequent XOR operations.

Last, the XOR operations diffuse the generated chaotic bit and the 24 binary images in parallel process. The XOR operation yields bit "1" if the two input bits are different, but yields bits "0" if the two inputs are similar. The results obtained from such XOR operations are 24 matrices with single binary number in each pixel. All the 24 matrices are combined into



(c) (b)

Fig. 4. Histrogram of numbers of initial conditions a_1.

three RGB matrices of a single 8-bit matrix in which each pixel is represented by [b_0-b_7]. As a result, the encrypted image can be achieved. The decryption process also follows the encryption process in a backward algorithms as long as the security keys are known.

III. Experimental Results

Experimental results have been performed in a computer–aid design tool MATLAB. Nonlinear dynamics of a compound sine and cosine map was initially simulated and encryption and decryption security performances were subsequently evaluated.

A. Nonlinear Dynamics of Compound Sine and Cosine Map

Since chaotic behaviors of the compound sine and cosine maps determine overall performance of the cryptosystem, Lyapunov exponent (LE) has been realized as a quantitative measure of chaoticity. The LE is defined as a quantity that characterizes the rate of separation of infinitesimally close trajectories and is given by

$$\mathrm{LE} = \lim_{\mathrm{n}\to\infty} \frac{1}{\mathrm{N}} \sum_{\mathrm{n}=1}^{\mathrm{N}} \log_2 \frac{\mathrm{dX}_{\mathrm{n}+1}}{\mathrm{dX}_{\mathrm{n}}} \tag{7}$$

where N is the number of iterations. Typically, the positive LE indicates chaotic behaviors. The larger value of LE results in higher degree of chaos. Fig.1 shows the plots of 2-imensional Lyapunov Exponent bifurcation structure between parameters *a* and *b* over the parameter space (0, 10) and the zoomed in region (0, 1) where the chaotic region is represented by the dark blue color while the non-chaotic region is represented in the white region. It is shown in Fig.1 that the chaotic behaviors of the compound sine and cosine map occupy most of parameter spaces, leading to a very robust chaos for secret key generations. Nonetheless, the zoomed in region at small values of parameters *a* and *b* contain some non-chaotic regions, which represent quasi-chaotic or periodic behaviors. The proposed key generation system has been designed to potentially generates secret keys potentially since the nonchaotic signals will ultimately be LE spectrum and the bifurcation diagram of parameters *a* over the parameter space (0, 10) when the parameter *b* is fixed at 0.5. It is apparent in Fig.2 that the LE spectrum is greater than zero and growing to infinity. In addition, the bifurcation diagram shows dense area of the maximum values of X_n over the entire range. As for a particular example, Fig.3 shows the histograms of the numbers of the secret key a_1 for 1,000 iterations. It can be seen from Fig.3 that the nonlinear dynamics of the compound sine and cosine maps provide the random secret keys that distribute over the region (0, 1) randomly. Such characteristics have also found in other secret keys. The simulations have been ensured that the proposed compound the nonlinear dynamics of the compound sine and cosine maps and the key generation systems can potentially provide truly random values for diffusion process in the proposed cryptosystem.

B. Key Space Analysis

The encryption and decryption realizes the 16-character ASCII code "ABCDEFG012345678" as an input key and the wrong key changes the last character to 5. The resulting eight initial conditions and eight parameters, i.e. a total of 16 keys, are represented by 8-digit floating-point numbers. Considering each key in the form $S\times2^E$ where *S* is a significand and *E* is an exponent, the keys that represented by 8 digits of a floating-point number (~3.4028×10^{38}) results in 128 uncertain digits, which is greater than the minimum requirement of the 56-bit data (~7.2057×10^{16}) encryption standard (DES) algorithm [23].

C. Histograms and 2D Power Spectral Analysis

The image histogram is a graph that illustrates the number of pixels in an image at different intensity values. In particular, the histogram of a color image can be separated into three sub-images with Red (R), Green (G), and Blue (B) components. Each sub-image has 256 different grey intensity levels, graphically displaying 256 numbers with distribution of pixels amongst these grayscale values. In addition, the 2D power spectrum that shows the power of image intensity can be obtained through a Discrete Fourier Transform (DFT) analysis and the algorithm is given by [24]

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \exp(-j(2\pi/M)ux) \exp(-j(2\pi/N)vy) \tag{8}$$

where *x* and *y* are a coordinates pair of an image, M and N are the size of image, *f*(*x*, *y*) is the image value at the pixel (*x*, *y*). Fig.4 shows the histograms of three R, G, B components and 2D power spectrums of original image, encrypted image, decrypted image, and decrypted image with wrong keys. As for a particular demonstration, the original image is Lena image with 256×256 image size. It can be seen from Figs.4 that the intensities of all original images in the histogram are contributed with different values in a particular shape and the power spectrum is not flat having a peak of intensity in the

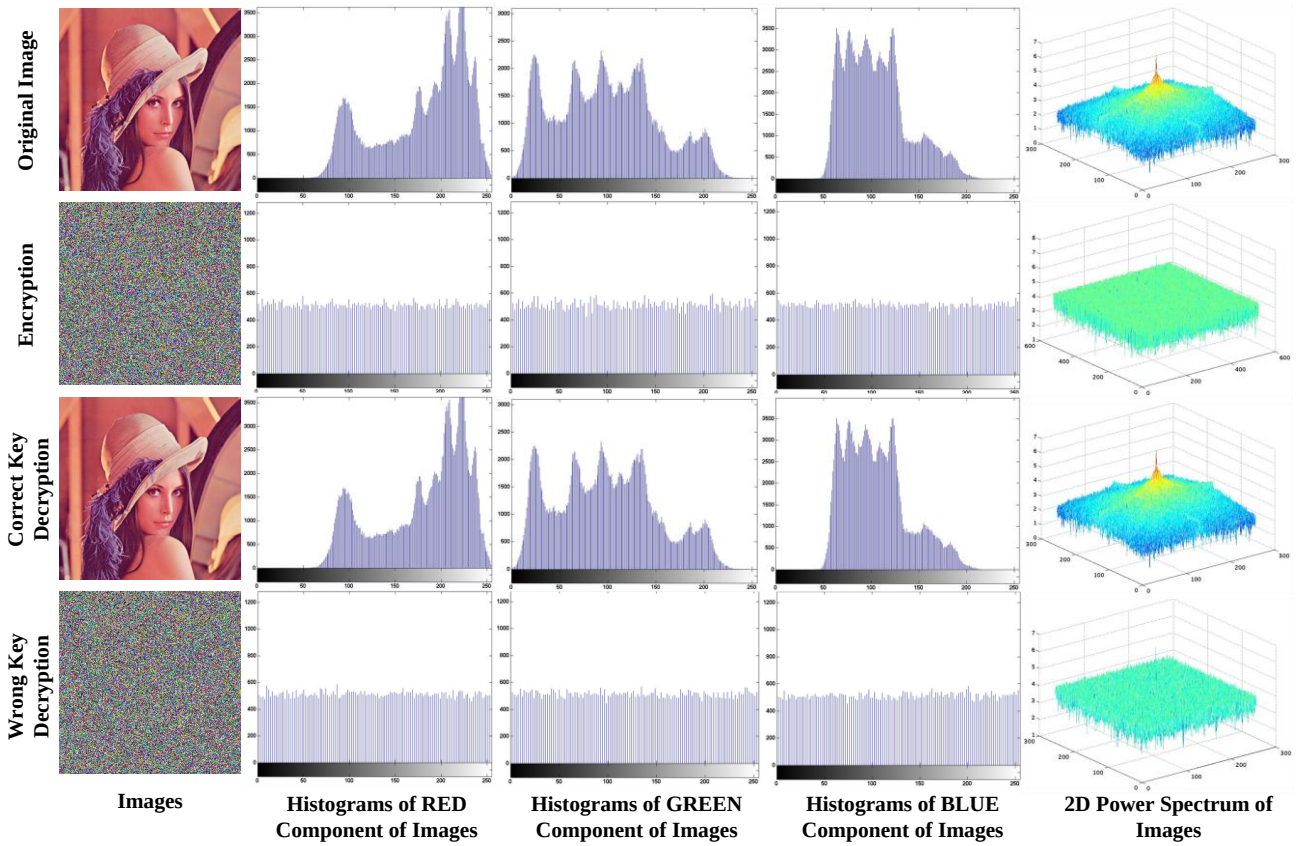


Fig.5. Histograms and 2D power spectrums of original image, encrypted image, decrypted image, and decrypted image with wrong keys.

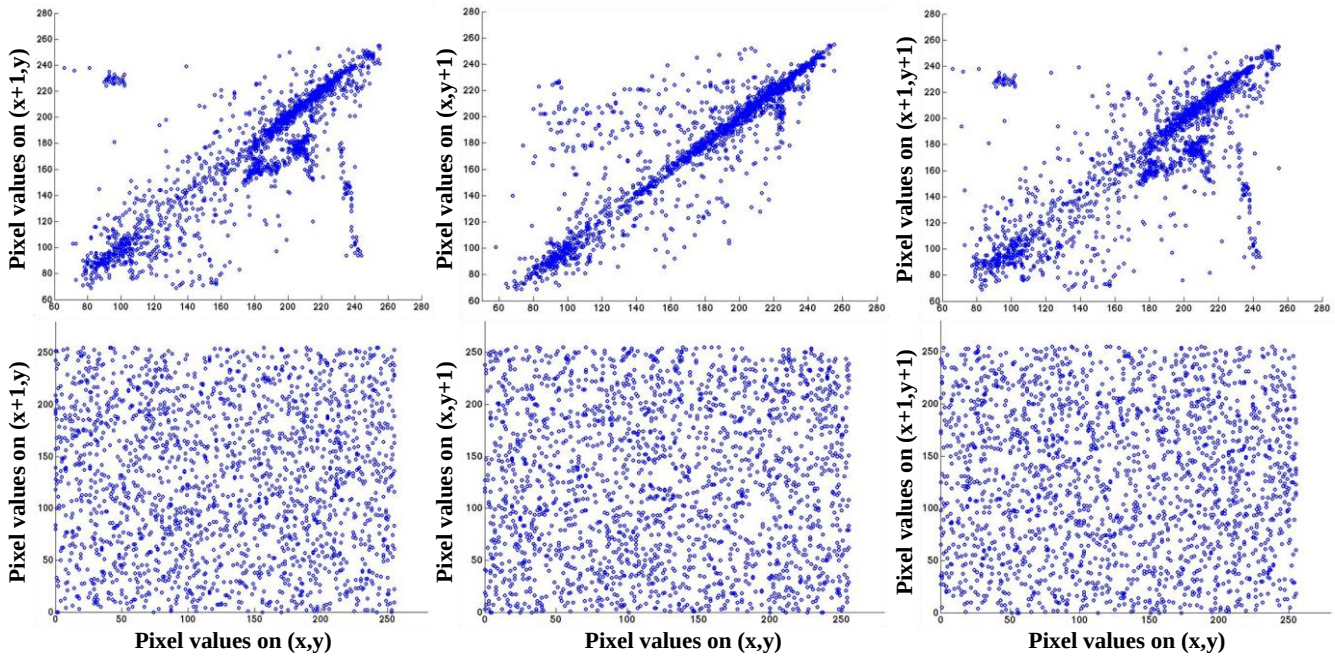
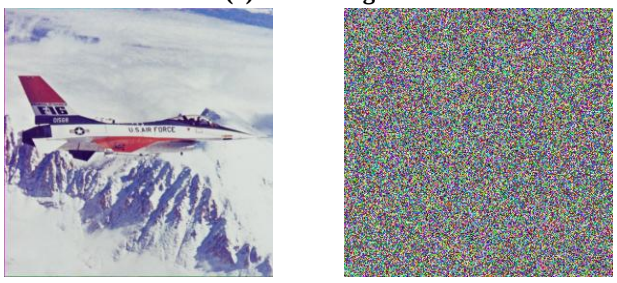


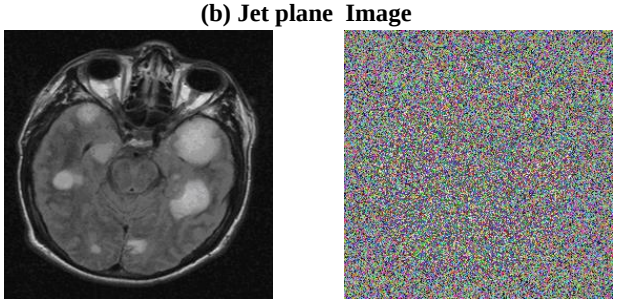
Fig.6. Image correlation tests in original and encrypted images, including horizontally, vertically, and diagonally adjacent pixels.

middle. The encrypted image has a flat histogram and power spectrum, indicating that the intensity values are equally contributed over all the intensity range and the original images are completely diffused and invisible. The decrypted images with right keys provide similar characteristics of the original images while the decrypted images with wrong keys are still diffused and the original images cannot be seen. These results qualitatively guarantee that the image is secured.

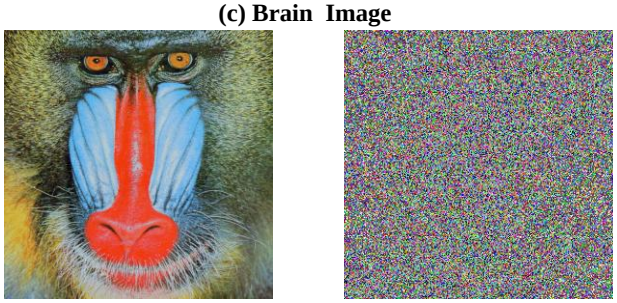
(a) Lena Image



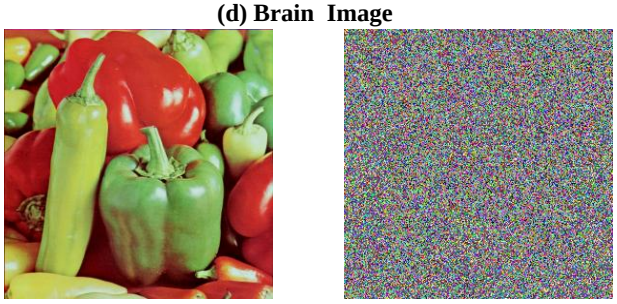
(b) Jet plane Image



(c) Brain Image



(d) Brain Image



(e) Peppers Image

Fig. 7. Original and cipher images of five images for the experiments.

D. Correlation Coefficient Analysis

In order to quantify the encryption performance and key sensitivity analysis, correlation between image pairs, which is a measure of relationships between two pixels intensities of two images, of the three realized images have been analyzed. The covariance C_v and the correlation coefficient γ_{xy} can be obtained as follows [16-17];

$$C_v(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{9}$$

$$\gamma_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \tag{10}$$

where the functions $E(x)$ and $D(x)$ are expressed as

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad \text{and} \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{11}$$

and the variables x and y are grey-scale values of pixels in corresponding pixels in different images or two adjacent pixels in the same image. Typically, the value of γ_{xy} is in the region [-1, 1]. In other words, the values of γ_{xy} in the region (-1,0) and (0,1) respectively indicate positive and negative relationships, while the larger number close to 1 or -1 have stronger relationships. Using a random selection of 2,048 pairs of pixels, Fig.5 shows image correlation tests in original and encrypted images, including horizontally, vertically, and diagonally adjacent pixels. It can qualitatively be considered from Figs.5 that the adjacent pixels of all encrypted images are highly uncorrelated as depicted by scatters plots of correlations.

For the quantitative measures, the correlations between pairs of original images and corresponding encrypted images through the computation of correlation coefficient between RGB components of the original images and corresponding encrypted images have been analyzed. Table 2 summarizes correlation coefficients of 2,048 pixels of each image pair. It can be seen in Table 3 that the correlation coefficients are very small closing to zero, indicating that each pair of images are completely independent of each other. Fig.7 shows the original and cipher images of five images for the experiments, including Lena, Jet plane, Brain, Baboon and Peppers images. As for investigations of other images with different characteristics, comparisons of correlation coefficients of four standard images in MATLAB shown in Fig.7 are also studied. Table 3 summarizes correlation coefficients of 2,048 pixels of each pair of images shown in Fig.7. Apparently, the correlation coefficients are also very small. These results quantitatively guarantee that the image is secured.

E. Original Image Sensitivity Analysis

One minor change in the plain image causes significant changes in the encrypted image then such differential analysis may become inefficient, and therefore much difference between encrypted forms is expected in order to maintain high security level. NPCR (Net Pixel Change Rate) and UACI (Unified Average Changing Intensity) are two most common measures. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired encrypted images

TABLE II
COMPARISONS OF CORRELATION COEFFICIENTS OF LENA IMAGE AT DIFFERENT SIZES.

Image Sizes	C_{RR}	C_{RG}	C_{RB}	C_{GR}	C_{GG}	C_{GB}	C_{BR}	C_{BG}	C_{BB}
256×256	0.00312	0.00298	-0.00406	0.00195	0.00061	-0.00267	0.00052	-0.00061	-0.00419
512×512	-0.00306	-0.00325	-0.00099	-0.00421	-0.00211	-0.00153	-0.00367	-0.00060	-0.00108
1024×1024	0.00181	-0.00081	0.00033	0.00113	-0.00056	-0.00053	0.00077	0.00008	-0.00063

TABLE III
COMPARISONS OF CORRELATION COEFFICIENTS OF DIFFERENT IMAGE WITH 256×256 IMAGE SIZE.

Images	C_{RR}	C_{RG}	C_{RB}	C_{GR}	C_{GG}	C_{GB}	C_{BR}	C_{BG}	C_{BB}
Brain	0.00259	-0.00123	-0.00270	0.00259	-0.00121	-0.00271	0.00261	-0.00128	-0.00269
Mandril	-0.00044	0.00735	-0.00606	0.00265	0.00657	-0.00625	0.00340	0.00194	-0.00613
Peppers	0.00429	-0.00456	-0.00240	0.00524	-0.00076	-0.00152	0.00129	-0.00378	-0.00152
Jet Plane	-0.00111	-0.00588	-0.00644	-0.00087	-0.00347	-0.00601	-0.00126	-0.00362	-0.00488

TABLE IV
SUMMARY OF NPCR AND UACI OF DIFFERENT IMAGE WITH 256×256 IMAGE SIZE.

Images	$NPCR_R$	$NPCR_G$	$NPCR_B$	$UACI_R$	$UACI_G$	$UACI_B$
Lena	99.2020	98.4085	99.2020	33.4107	33.4309	33.5449
Brain	99.2048	98.4956	99.3125	33.4488	33.3952	33.3707
Mandril	99.5102	99.0132	99.4123	33.5100	33.3507	33.4846
Peppers	99.4262	99.2144	99.2314	33.4387	33.3085	33.5637
Jet Plane	99.2436	98.9485	99.3345	33.4456	33.3845	33.4562

[17]. For the two encrypted images in which the corresponding original images have only one pixel difference are denoted by C^1 and C^2. Label the greyscale values of the pixels at pixel (i,j) in C^1 and C^2 by C^1(i,j) and C^2(i,j), respectively. Define a bipolar array D, with the same size as images C^1 and C^2. Consequently, D(i,j) is determined by C^1(i,j) and C^2(i,j), if C^1(i,j) =C^2(i,j) then D(i,j)=1, otherwise, D(i,j)=0. The NPCR [21] is defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{T} \times 100\% \quad (12)$$

$$UACI = \left(\frac{\sum_{i,j} D(i,j)}{T} \right) \times 100\% \quad (13)$$

where T denotes the total number pixels in the encrypted image, F denotes the largest supported pixel value compatible with the cipher image format, and |.| denotes the absolute value function. Table 4 summarizes the values of NPCR and UACI for different image with the sizes of 256×256. It can be seen that the NPCR are relatively close to 100% and the UACI are also in the acceptable region of approximately 33%.

F. Information Entropy Analysis

The entropy $H(s)$ is one of important characteristics of the randomness and can be found by

$$H(s) = \sum_{i=0}^{2^M-1} P(S_i) \log_2 \frac{1}{P(S_i)} \quad (12)$$

where $P(S_i)$ represents the probability of symbols i. In the case where a purely random source producing $2M$ symbols, the entropy is given by $H(s)=M$. If the output of a cipher image produces the number of symbols with the entropy value of less than M, there is a certain degree of predictability which intimidates its security. Table 5 summarizes the results of information entropy of those five standard images in Fig.7. The values obtained are very close to the theoretical value of M=8, indicating that information leakage during encryption process is negligible and the encryption system is secure against the entropy attack.

TABLE V
RESULTS OF INFORMATION ENTROPY OF FIVE STANDARD IMAGES

Images	Entropy H(s)
Lena	7.99915
Brain	7.99924
Mandril	7.99910
Peppers	7.99896
Jet Plane	7.99923

CONCLUSION

A robust digital image cryptosystem based on nonlinear dynamics of a compound sine and cosine chaotic map has been presented. The compound sine and cosine chaotic map has been proposed for high-degree of chaos over most regions of parameter spaces in order to increase high-entropy random-bit sources. Image diffusion has been performed through pixel shuffling and bit-plane separations prior to XOR operations in order to achieve a fast encryption process. Security key conversions from ASCII code to floating number for use as initial conditions and control parameters were also presented to enhance key-space and key-sensitivity performances. Nonlinear dynamics of the chaotic maps have been investigated in terms of chaotic attractor, Lyapunov exponent spectrum, bifurcation diagram, and 2-dimensional parameter spaces. Encryption qualitative performances were evaluated through pixel density

histograms, 2-dimensional power spectral density, key space analysis, key sensitivity, vertical, horizontal, and diagonal correlation plots. Encryption quantitative performances were evaluated through correlation coefficients, NPCR and UACI. Demonstrations of wrong-key decrypted image are also included. The proposed cryptosystem offers a potential alternative to private data protection systems.

REFERENCES

[1] M. Philip, "An Enhanced Chaotic Image Encryption" International Journal of Computer Science, Vol. 1, No. 5, 2011.

[2] 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, 2012.

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

[4] X. Tong, M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator", Signal Processing, Vol. 89, pp. 480-491, 2009.

[5] J.W. Yoon, H. Kim,"An image encryption scheme with a pseudorandom permutation based on chaotic maps", Commun Nonlinear Sci Number Simulation, Vol. 15, pp. 3998–4006, 2010.

[6] X. Ma, C. Fu, W. Lei, 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, 2011.

[7] K. Wang, W. Pei, L. Zou, A. Song, Z. He, "On the security of 3D Cat map based symmetric image encryption scheme", Physics Letters A, Vol. 343, pp. 432–439, 2005.

[8] K. Wong, B. Kwok, and W. Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", Physics Letters A, Vol. 372, pp. 2645-2652, 2008.

[9] S. Lian, J. Sun, Z. Wang, "A block cipher based on a suitable use of the chaotic standard map", Chaos, Solitons and Fractals, Vol. 26, pp. 117–129, 2005.

[10] K. Gupta, S. Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Jour. of Information Security, pp. 139-150, 2011

[11] F. Huang, Y. Feng, "Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm", Front. Electr. Electron. Eng. China, Vol. 4, No. 1, pp. 5-9, 2009.

[12] G.Lee and N. H. Farhat , "Parametrically Coupled Sine Map Networks" ,Electrical Engineering Department, University of Pennsylvania, Philadelphia, PA, USA,15 December 2000

[13] F.Sun, S. Liu , Z. Li , Z. Lu , "A novel image encryption scheme based on spatial chaos map",College of Control Science and Engineering, Shandong University, Jinan , PR China , pp. 631–640 , 2008

[14] Q. Gong-bin, J. Qing-feng,Q. Shui-sheng, "A new image encryption scheme based on DES algorithm and Chua's circuit", Imaging Systems and Techniques, pp. 168 – 172, 2009.

[15] Z. Peng, T.B. Kirk, "Two-dimensional fast Fourier transform and power spectrum for wear particle analysis", Tribology International, Vol. 30, Issue. 8, pp. 583-590, 1997.

[16] A. Yahya and A. Abdalla, "A Shuffle Image-Encryption Algorithm", J. Comput. Sci,pp.999-1002

[17] Y.Wu, Joseph P. Noonan, S.Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Department of Electrical and Computer Engineering Tufts UniversityMedford, MA ,USA

Sarun Maksuanpan was born in Samutsakorn Province, Thailand in 1991. He received B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory. His research interests include information security systems, cryptosystems, artificial neural networks, and digital image processing.

Tanachard Veerawadtanapong was born in Bangkok, Thailand in 1992. He received B.Eng. in Computer Engineering from Computer Engineering Department, Faculty of Engineering, Thai-Nichi Institute of Technology (TNI). Currently, he is also a research assistant at Intelligent Electronic Research Laboratory. His research interests include Ad Hoc mobile network, cryptosystems, and chaos theory.

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 Computer Engineering Department, 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.