2017 14th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico City, Mexico. September 20-22, 2017

Information Security Analysis of Deterministic Encryption and Chaotic Encryption in Spatial Domain and Frequency Domain

Zhengmao Ye, Hang Yin
College of Engineering, Southern University
Baton Rouge, LA70813, USA
zhengmao_ye@subr.edu,hang_yin@subr.edu

Yongmao Ye
Liaoning Radio and Television Station
ShenYang, Liaoning, China
yeyongmao@hotmail.com

***Abstract* — Information security is crucial to data storage and transmission, which is necessary to protect information under various hostile environments. Cryptography serves as a major element to ensure confidentiality in both communication and information technology, where the encryption and decryption schemes are implemented to scramble the pure plaintext and descramble the secret ciphertext using security keys. There are two dominating types of encryption schemes: deterministic encryption and chaotic encryption. Encryption and decryption can be conducted in either spatial domain or frequency domain. To ensure secure transmission of digital information, comparisons on merits and drawbacks of two practical encryption schemes are conducted, where case studies on the true color digital image encryption are presented. Both deterministic encryption in spatial domain and chaotic encryption in frequency domain are analyzed in context, as well as the information integrity after decryption.**

***Index Terms* — Deterministic Encryption, Chaotic Encryption, Information Security, Entropy, Mutual Information, Correlation**

I. INTRODUCTION

In cryptography, encryption and decryption are used to protect privacy and confidentiality of transmitted data via the process of encoding and decoding, so that the authorized parties are able to access it exclusively. Encryption keys are also introduced in order to make the ciphertext more difficult to decipher against tampering. In the meanwhile, authorized recipients can simply decrypt the ciphertext with the keys. Symmetric key encryption contains a single private key to protect integrity and authenticity. Generally asymmetric encryption schemes are more secure which contain both a public key for authorized group and a private key. However an asymmetric key must be much longer than a symmetric key to be secure, because the former is generated based on large prime numbers and the latter is generated based on random numbers. For the same key length (e.g. 256 bits), a symmetric key could be more secure than a much longer asymmetric key.

There are a variety of technical applications of encryption algorithms. For permutation-only image ciphering, entries of the image matrix are scrambled using a mapping matrix built by the pseudo-random number generator. It is assumed permutation-only ciphering is insecure against both ciphertext attacks and plaintext attacks. Contrary to incomplete plaintexts retrieval in previous studies, the work has made cryptanalysis on chosen plaintext attacks complete and efficient using a deterministic method regardless of cipher structure [3]. A novel compression and encryption combined scheme using variable model arithmetic coding and coupled chaotic system can encrypt and compress plaintexts synchronously. The new scheme is secure since a key bit-stream generated by deterministic randomness can counteract with previous attacks against chaotic encryption which can also achieve high compression efficiency [4]. It has been also documented that most lossy compression schemes will provide perfect visual perception under an exceptional compression ratio, among which discrete Fourier transform and statistical schemes are dominant approaches for compression and reconstruction. Comparative study on schemes has been made using a well-defined set of quantitative metrics from Information Theory [5]. An image encryption is conducted via two dimensional chaotic sequence obtained from multi-scroll chaotic attractors. Initial values of chaotic attractors are served as the private key. With the elaborately designed 2D chaotic sequence, encrypted images contain balanced ratio and ideal nonlinearity. The 2D discrete Fourier transform can validate the chaotic encryption approach [6]. Fractional order analysis of chaotic systems has also been conducted. Qualitative analysis of fractional orders on chaotic system characteristics is made which provides a solid basis for applying fractional order control to either generate or suppress chaotic behaviors [7]. A new approach is proposed for image encryption based on chaotic logistic maps for secure transmission. A secret key of 80 bit and two chaotic logistic maps are employed. To make ciphering more robust against attack, the secret key is modified after encrypting each block of sixteen pixels of the image. The statistical analysis and key sensitivity tests demonstrated that proposed encryption provides an efficient and secure way for real-time image encryption and transmission [8]. Similarly a physical layer security-enhanced transmission scheme is successfully implemented via Discrete Fourier Transform spread orthogonal frequency division multiplexing signals in a passive optical network [9]. The new chaos-based cryptographic algorithm is proposed for image encryption based on multiple-parameter discrete fractional Fourier transform and chaotic logistic maps. The digital image has been encrypted by multiple parameter discrete fractional Fourier transform while the alignment is determined by chaotic logistic maps. Without introduction of keys, it is comparable or robustness to blind decryption [10].

A double image encryption method is proposed by utilizing the discrete multiple parameter fractional Fourier transform and chaotic maps. One image scrambled by one chaotic map is encoded into the amplitude of complex signals. The complex signal multiplied by another chaotic random phase mask is then encrypted by discrete multiple parameter fractional Fourier transform. Parameters in chaotic map serve as the keys of this

978-1-5386-3406-6/17/$31.00 ©2017 IEEE

encryption scheme [11]. In this research, two major schemes on information security are presented using deterministic encryption and chaotic encryption in the spatial domain and frequency domain [1-11], respectively. Comparative studies are also made via numerical simulations in order to determine the best scheme for secure digital data transmission.

II. RGB True Color Model

At the true color space, every color is represented by a mixture of three primary spectral components (Red, Green and Blue) at the Cartesian coordinate system. Color composition gives rise to the appearance of the actual scene. The RGB image can be depicted by a matrix (M×N×3) of intensity levels independent from each other. In the RGB color model, 3 primary color components are mapped into a cube in which the Red, Green and Blue values are set to be three corners; black is set to be the origin and white is set to be the opposite corner. Cyan, magenta and yellow are instead set to be the rest three corners of the cube. An arbitrary composite color is a vector on or inside the cube. The projection of true color intensity components to the diagonal will lead to the grayscale image of the size (M×N).

III. Deterministic Encryption in Spatial Domain

Deterministic encryption represents the cryptosystem that produces exactly the same ciphertext for the given plaintext and key across all executions of encryption. Pseudorandom key generators are used in the deterministic algorithm at a fixed length to generate the symmetric cipher keys for permutation. The block cipher is selected for symmetric key encryption which comprises of 64 bits as a single unit of encryption. It could be further repeatedly applied in a loop. The spatial domain encryption of the digital image is thus implemented on the 64 bit block with 64 bit key to encrypt 64 bit of data each time step by step. In particular, for a grayscale digital image or each component (R, G, B) of the true color digital image, the intensity of each pixel (0 to 255) is converted to an 8 bit binary plaintext. Given a source image of size of M × N, the matrix of M × 8N is thus generated whose 8*M*N elements are equal to either zero or one. Collating plaintexts of 8 consecutive pixels in the sequence will give rise to the 64 bit plaintext input subject to encryption with the 64 bit pseudorandom key. For decryption process, the same 64 bit pseudorandom key is applied once again to block ciphers step by step so as to retrieve the source image completely.

Scrambling is then applied to all pixels of the digital image using the predetermined pseudorandom keys. Specifically, the XOR (modulo 2 addition, exclusive OR) binary operation ($A \oplus B$) is conducted between the 64 bit plaintext and 64 bit key as well as between the 64 bit ciphertext and the 64 bit key for scrambling and descrambling. The purpose is simply to create confusion and diffusion across deterministic encryption and decryption schemes, respectively.

IV. 2D Discrete Fourier Transform (DFT)

2D Discrete Fourier Transform (DFT) should be employed to implement digital image encryption in the frequency domain. DFT operates at a finite number of discrete data points. Using DFT, a digital image in the spatial domain is transformed into an equally spaced set of values in frequency domain with real and imaginary components. 2D DFT from spatial f(x,y) to frequency domain F(u, v) is shown in (1).

$$F(u, v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-2\pi i(xu/M+yv/N)} \quad (1)$$

where x and y are coordinate pair of the digital image pixel; M and N are the size of image; f(x, y) is the actual intensity level corresponding to the pixel (x, y).

DFT decomposes a digital image into its real and imaginary components to represent digital image information in the frequency domain. DFT operates on cosine and sine functions. The number of discrete frequencies in the frequency domain is equivalent to the number of pixels in the spatial domain. In the frequency domain, real parts of the DFT complex exponentials are subject to encryption. To decrypt the digital image from the frequency domain back to the spatial domain, inverse DFT can be applied which is shown in (2). In this way, the source image will be recovered by decryption.

$$f(x, y)=\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u, v)e^{+2\pi i(xu/M+yv/N)} \quad (2)$$

V. Chaotic Encryption In Frequency Domain

To keep transmitted ciphertexts secure in both spatial and frequency domains, inexpensive chaotic encryption can be introduced which is relatively simple to implement with ease to protect data transmission. The 64 bit symmetric chaotic cipher key is generated by a typical chaotic logistic map. The logistic difference equation is formulated as (3).

$$x_{n+1}=\mu x_n(1- x_n) \quad (3)$$

where x_n is between 0 and 1; $0<\mu\leq 4$ is the driving parameter that could exhibit bifurcation behaviors when $\mu = 3.0$. With a small constant value of the driving parameter μ, the sequence $\{x_0, x_1, x_2, \ldots, x_n\}$ eventually converges recursively to a single number x_n. An initial value must be set and the parameter value of μ has been selected as 3.75 which has the chaotic behavior.

For a gray level digital image or each component (R, G, B) of the true color digital image in the frequency domain, the real part of the DFT complex exponentials expressed in the decimal plaintext is converted to an 8 bit binary plaintext. Again given a source image of size of M × N in the frequency domain, the matrix of M × 8N is thus generated whose 8*M*N entries are equal to either zero or one. Collating the plaintexts with 8 consecutive pixels in the sequence will give rise to the 64 bit plaintext subject to encryption. Chaotic scrambling is thus made between the 64 bit plaintext and the 64 bit generated chaotic sequence in binary formulation. For each block cipher, an initial x_0 in the logistic iterative sequence is selected one by one individually to enhance the security.

Scrambling is then applied to all frequency levels of the digital image using chaotic keys. XOR (modulo-2 addition, exclusive or) binary operation ($A \oplus B$) is conducted between the 64 bit plaintext and 64 bit key as well as between the 64 bit secure ciphertext and 64 bit key once again for scrambling and descrambling. In this case, confusion and diffusion is created across chaotic scrambling and descrambling for encryption and decryption schemes, respectively.

VI. Numerical Simulation and Histogram Analysis

Fig. 1. Diverse Types of True Color Source Images

Numerical simulations on diverse types of digital true color images are conducted. Each source image is composed of three primary color components of red, blue and green. Each primary color component is subject to either deterministic or chaotic types of encryption and decryption. Without loss of generality, two major types of digital images are selected with a couple of examples. Two sparse-distributed source digital images are shown in the upper row and two dense-distributed digital source images are shown in the lower row of Fig. 1. Encryption and decryption outcomes of 2 sparse-distributed digital images are shown in Fig. 2 while encryption and decryption outcomes of 2 dense-distributed digital images are shown in Fig. 5. In both Fig. 2 and Fig. 5, outcomes from deterministic permutation based encryption and decryption are placed to the left while outcomes from chaotic substitution based encryption and decryption are placed to the right. Histogram analysis is conducted, which is able to reveal detail information about the source image, encrypted image and decrypted image. Histogram is a graphical representation of the distribution of the total count of each intensity level in digital images, indicating discrete frequency distributions across all potential intensity levels. It manifests how often each different intensity level in a set of all possible intensity levels occurs. Histogram (Red, Green and Blue) analysis of 4 diverse digital images is also made whose results are shown in Fig. 3, Fig. 4, Fig. 6 and Fig. 7 respectively. Histograms of the source image, deterministic encryption and decryption images, chaotic encryption and decryption images are listed in order from the 1st to 5th row, while RGB components are listed from the 1st to 3rd column.

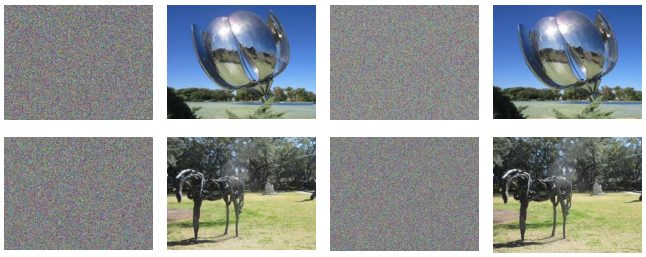

Fig. 2. Deterministic and Chaotic Encryption and Decryption Case 1 & 2

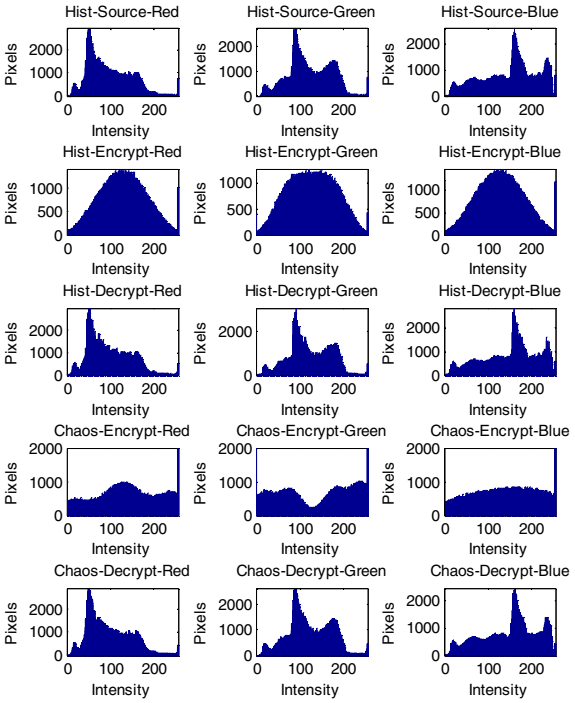

Fig. 3. Histogram (R, G, B) Analysis of Digital Image 1

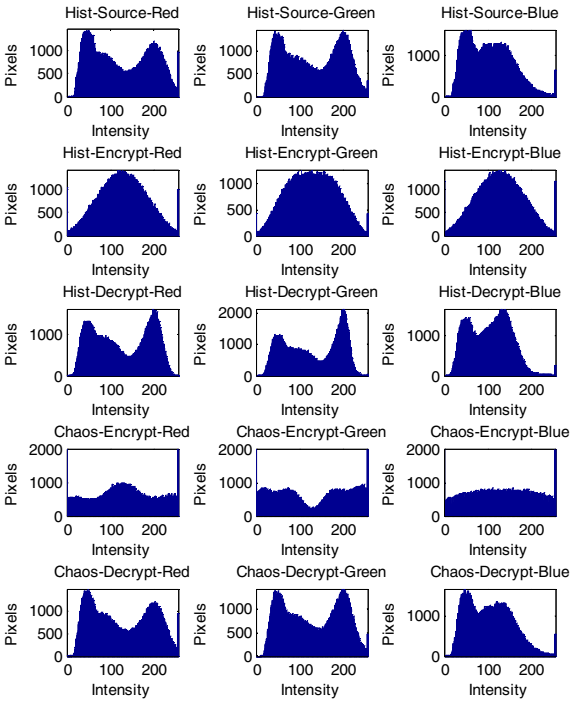

Fig. 4. Histogram (R, G, B) Analysis of Digital Image 2

When the encrypted image histogram reaches nearly uniform distribution, the encryption scheme is regarded as secure since it is robust against ciphertext attack. In contrast, when the encrypted image histogram has distribution somehow similar to that of source image, the encryption scheme is considered as weak since it is vulnerable against ciphertext attack. From Fig. 3 and Fig. 4, for sparse-distributed digital images, histograms of the source images, decrypted images via the deterministic scheme, and decrypted images via the chaotic scheme depict remarkable similarities upon information recovery. The minor mismatch is due to the quantization error in number conversion among binary, decimal and hexadecimal codes. On the other hand, deterministic permutation based encryption merely rearrange the pixels which does not change total counts of different intensity levels. Chaotic substitution based encryption however is based on discrete chaotic generator, which is able to vary the total counts of different intensity levels. The former will relocate the histogram distribution while the latter flattens histograms instead. The chaotic scheme is more confidential. The histograms in the 3rd and 5th column of Fig. 3 and Fig. 4 simply verify this conclusion.

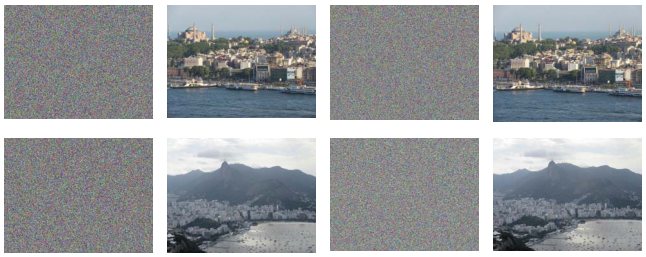

Fig. 5. Deterministic and Chaotic Encryption and Decryption Case 3 & 4

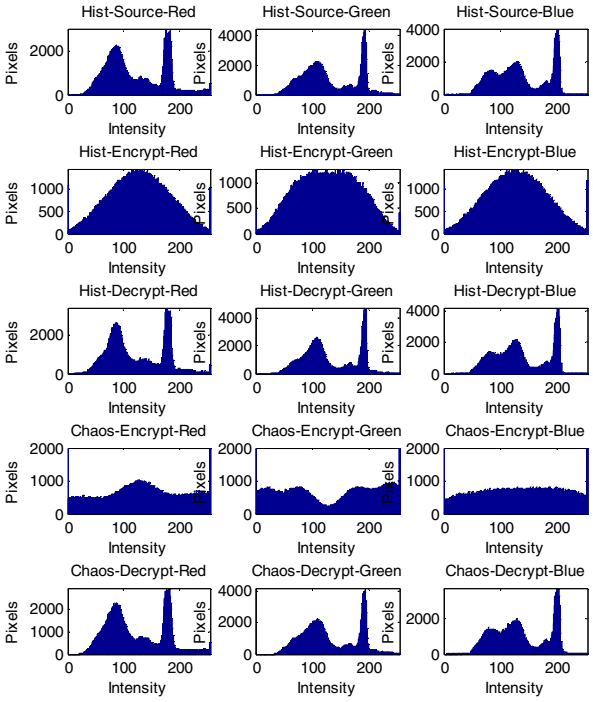

Fig. 6. Histogram (R, G, B) Analysis of Digital Image 3

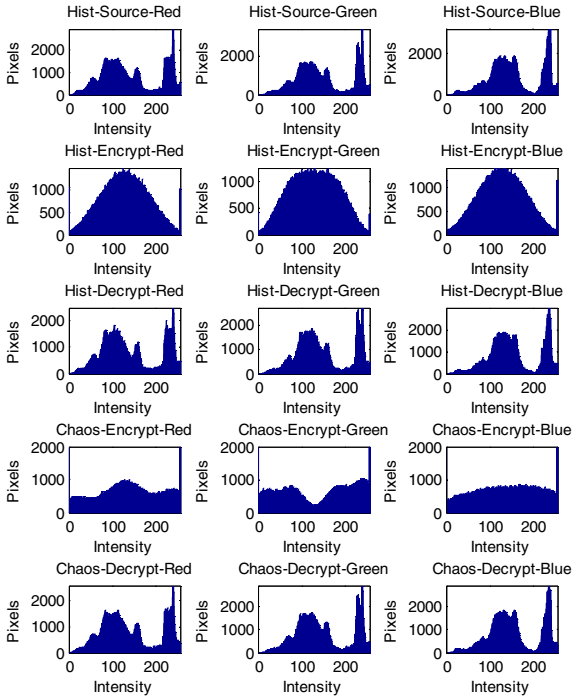

Fig. 7. Histogram (R, G, B) Analysis of Digital Image 4

Alternatively from Fig. 6 and Fig. 7, for dense-distributed digital images, histograms of source images, decrypted images via the deterministic scheme, and decrypted images via the chaotic scheme again depict significant similarities on information recovery. The minor mismatch is still due to the quantization error in the number system conversion. Similarly deterministic permutation based encryption only rearrange pixels which won't change total counts of different intensity levels. Chaotic substitution based encryption instead is based on discrete chaotic generator, which is able to change total counts of different intensity levels. The former rearranges the histograms while the latter actually flattens the histograms. From visual appearances of histograms of deterministic and chaotic encryption schemes in Figs (3, 4, 6, 7), the chaotic encryption scheme outperforms the deterministic encryption scheme against ciphertext attack. To further analyze the impact of two encryption and decryption schemes, some quantitative metrics will be introduced for objective evaluation.

VII. Quantitative Comparisons

A. Discrete Entropy

The average amount of information conveyed from a digital image is described by the discrete entropy, formulated as the sum of products between the probability of outcome and logarithm of the inverse of the probability (4), considering all potential outcomes in the event $\{x_1, x_2, \ldots, x_k\}$, where k is a count of the intensity levels; p(i) is the probability distribution. For encrypted images, the larger the discrete entropy is, the more secure the encryption scheme is.

$$H(x)=\sum_{i=1}^{k} p(i)\log_2 \frac{1}{p(i)} = -\sum_{i=1}^{k} p(i)\log_2 p(i) \quad (4)$$

B. Discrete Energy

In order to show how intensity level of each primary color channel is distributed, another metric discrete energy is used to indicate the randomness which is defined as (5), where E(x) represents the discrete energy with 256 bins; p(i) represents the probability distribution for a channel (R, G, B) based on the total histogram counts. For an image of constant intensity, the discrete energy has the maximal value of one. In contrast to the discrete entropy, for encrypted images, the larger the discrete energy is, the less secure the encryption scheme is.

$$E(x)=\sum_{i=1}^{k} p(i)^2 \tag{5}$$

C. Correlation

Correlation is defined as (6) which reflects linear dependency of the intensity levels among neighboring pixels. It shows the amount of local intensity variations across the entire digital image. It produces non-contact measurement for digital image processing. In (6), i and j are the coordinate pair of the co-occurrence matrix; g(i, j) represents an intensity element of the co-occurrence matrix at the coordinates i and j; μ_i and μ_j represent the horizontal mean and vertical mean; σ_i and σ_j represent the horizontal variance and vertical variance. The correlation represents a statistical relationship. The higher degree the dependency is, the more vulnerable the scheme is.

$$R=\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{(i-\mu_i)(j-\mu_j)}{\sigma_i\sigma_j}g(i,j) \tag{6}$$

D. Mutual Information

Mutual information depicts that the information that Y can tell about X is equal to the uncertainty reduction of X due to the existence of Y. It is defined in (7), which acts as a symmetric function, where I(X; Y) is the mutual information; H(X) and H(X|Y) are discrete entropy and conditional entropy values. Zero mutual information means two images are independent.

$$I(X;Y)=H(X)-H(X|Y)=\sum_{X,Y} p_{XY}(X,Y)\log_2\frac{p_{XY}(X,Y)}{p_X(X)p_Y(Y)} \tag{7}$$

Quantitative metrics based on both deterministic and chaotic encryption and decryption schemes are computed and listed in Table 1 to Table 8. Tables (1, 3, 5, 7) provide the numerical results on discrete entropy, discrete energy and correlation for 4 digital images. Metrics of the source image, deterministic encrypted and decrypted images, chaotic encrypted and decrypted images are shown from the 1st to 5th column. Tables (2, 4, 6, 8) provide the numerical results on mutual information based on 4 digital images. Meanwhile, analysis on all 3 components of Red, Green and Blue has been conducted. Mutual information of deterministic encryption and decryption images, chaotic encryption and decryption images associated to source images are shown from the 1st to 4th column.

The encryption algorithm aims to mix extra information by scrambling plaintexts so that generated ciphertexts become too complicated for potential intruders to differentiate and predict. Simultaneously deciphered results after descrambling should match original plaintexts as close as possible. The secure encryption must produce large disorder ciphertexts exhibiting high level of randomness to avoid the cryptographic attack. From Tables (1, 3, 5, 7), for deterministic encryption in the spatial domain and the chaotic encryption in the frequency domain, corresponding decryption could retrieve information with high degree of similarity. However, better matches in the discrete entropy and discrete energy occur in the latter chaotic scheme than the former deterministic scheme. With respect to the encrypted ciphertexts, the chaotic encryption outcomes in the frequency domain are corresponding to the larger discrete entropy and smaller discrete energy than the deterministic encryption outcomes in the spatial domain, no matter which source image is selected and which color component is applied. Therefore the security performance of chaotic scheme is stronger than the deterministic scheme from entropy attack point of view. The encrypted image is supposed to have the low correlation value which is lack of periodicity, dependency and repeatability, so that little information on plaintexts can be extracted from ciphertexts. On the other hand, the decrypted image is supposed to possess similar or exact correlation value to the source image. From Tables (1, 3, 5, 7), better matches in the correlation value occur in the latter chaotic scheme than the former deterministic scheme regardless of which source image is selected. The encrypted ciphertexts always retain much smaller correlation values than either plaintexts or decrypted texts. However, no conclusion could be made to distinguish between two encryption schemes on a basis of correlation analysis because results vary case by case when different color components are evaluated. From Tables (2, 4, 6, 8), mutual information between encrypted and source images is much greater than that between decrypted images and source images, it shows that decrypted images are nearly independent of source images using two encryption schemes.

For the sensitivity issue, NPCR (Number of Pixels Change Rate) can be applied to evaluate to the impact of changing a single pixel in a source image on an encrypted image. For each case above, using 2 encryption schemes, NPCR always ranges from 98% to 99% between any two relevant images, indicating that both schemes are sensitive to small changes. However NPCR must be applied to a large quantity of images for comparisons, no convincing conclusion is thus reached here between two schemes.

TABLE 1 QUANTITATIVE METRICS OF SPARSE-DISTRIBUTED IMAGE 1

	Source	Encryption1	Decryption1	Encryption2	Decryption2
Entropy_R	2.063163	3.620904	2.18746	4.089945	2.060176
Entropy_G	2.044416	3.624417	2.156932	4.053372	2.04156
Entropy_B	2.288587	3.611781	2.418556	4.127156	2.287058
Energy_R	0.175716	0.033621	0.161858	0.017945	0.176215
Energy_G	0.175694	0.031895	0.164436	0.019042	0.176217
Energy_B	0.133572	0.034115	0.124997	0.016604	0.134169
Correlation_R	0.973127	0.070369	0.957482	0.084636	0.973248
Correlation_G	0.97295	0.07582	0.95662	0.07357	0.973238
Correlation_B	0.982826	0.06952	0.971366	0.075759	0.982865

TABLE 2 MUTUAL INFORMATION OF SPARSE -DISTRIBUTED IMAGE 1

Mutual Information	Red	Green	Blue
Encryption 1	0.314957	0.279684	0.023057
Decryption1	0.007252	0.02385	0.00082
Encryption 2	0.076662	0.05806	0.260993
Decryption2	0.006828	0.003629	0.01034

TABLE 3 QUANTITATIVE METRICS OF SPARSE-DISTRIBUTED IMAGE 2

	Source	Encryption1	Decryption1	Encryption2	Decryption2
Entropy_R	2.677226	3.626924	2.671111	4.106952	2.686039
Entropy_G	2.653247	3.631184	2.660375	4.077646	2.662088
Entropy_B	2.535186	3.618953	2.515005	4.141567	2.534722
Energy_R	0.096161	0.033415	0.093634	0.017298	0.09468
Energy_G	0.094928	0.031644	0.092854	0.018082	0.093704
Energy_B	0.112243	0.033764	0.111019	0.016142	0.110931
Correlation_R	0.945148	0.067398	0.937182	0.072132	0.945418
Correlation_G	0.942212	0.074848	0.932093	0.094352	0.942639
Correlation_B	0.901305	0.068882	0.880142	0.06429	0.901977

TABLE 4 MUTUAL INFORMATION OF SPARSE -DISTRIBUTED IMAGE 2

Mutual Information	Red	Green	Blue
Encryption 1	0.53367	0.142901	0.168077
Decryption1	0.085949	0.008031	0.096976
Encryption 2	0.42065	0.23901	0.54135
Decryption2	0.002333	0.002344	0.003892

TABLE 5 QUANTITATIVE METRICS OF DENSE-DISTRIBUTED IMAGE 3

	Source	Encryption1	Decryption1	Encryption2	Decryption2
Entropy_R	2.099928	3.629542	2.274678	4.10367	2.107068
Entropy_G	1.946185	3.630357	2.086513	4.078179	1.957705
Entropy_B	2.116983	3.614853	2.298975	4.139424	2.133832
Energy_R	0.180114	0.033325	0.160377	0.017424	0.178905
Energy_G	0.209264	0.031668	0.19587	0.018123	0.207787
Energy_B	0.155004	0.033939	0.131466	0.016213	0.152755
Correlation_R	0.964016	0.070733	0.928797	0.064947	0.963312
Correlation_G	0.956157	0.075704	0.91648	0.085804	0.955378
Correlation_B	0.957095	0.068837	0.925148	0.057828	0.956186

TABLE 6 MUTUAL INFORMATION OF DENSE-DISTRIBUTED IMAGE 3

Mutual Information	Red	Green	Blue
Encryption 1	0.423208	0.601181	0.593411
Decryption1	0.065435	0.05918	0.001459
Encryption 2	0.057009	0.361277	0.374055
Decryption2	0.008696	0.015202	0.029297

TABLE 7 QUANTITATIVE METRICS OF DENSE-DISTRIBUTED IMAGE 4

	Source	Encryption1	Decryption1	Encryption2	Decryption2
Entropy_R	2.125326	3.626212	2.248209	4.0887	2.133224
Entropy_G	2.054836	3.631202	2.18555	4.051366	2.064141
Entropy_B	2.005959	3.614189	2.136557	4.123401	2.020455
Energy_R	0.153045	0.033378	0.143309	0.018007	0.152485
Energy_G	0.167361	0.031627	0.155212	0.019162	0.16656
Energy_B	0.178523	0.033996	0.165741	0.016732	0.177135
Correlation_R	0.988744	0.063542	0.979987	0.084442	0.988374
Correlation_G	0.987167	0.071708	0.977004	0.106342	0.986692
Correlation_B	0.985655	0.063271	0.974662	0.076815	0.984925

TABLE 8 MUTUAL INFORMATION OF DENSE-DISTRIBUTED IMAGE 4

Mutual Information	Red	Green	Blue
Encryption 1	0.157604	0.309072	0.375831
Decryption1	0.018075	0.005377	0.001042
Encryption 2	0.236649	0.029434	0.123322
Decryption2	0.00186	0.006982	0.007831

CONCLUSIONS

Applications of both deterministic and chaotic digital image cryptosystems in the spatial domain and frequency domain are conducted in this research. The corresponding outcomes are compared from both qualitative and quantitative points of view, utilizing symmetric deterministic and chaotic encryption schemes. 64 bit block ciphers are implemented in both cases of secret key cryptography. The deterministic encryption scheme implemented in spatial domain is based on the permutation encryption algorithm by reallocating pixels. It could speed up source data retrieval via efficient encryption database searching but security is not fully guaranteed. On the other hand, to ensure secure encoding and decoding of digital images, chaotic encryption is implemented in frequency domain via scrambling with the generated chaotic logistic map. In particular, 2D Discrete Fourier Transform and Inverse Fourier Transform are applied in the process of frequency domain encryption and decryption. It is based on substitution encryption via chaotic sequence in order to revise correlation, flatten histograms and enhance key sensitivity. The differential scrambling is applied in both cases where exclusive OR operations between the plaintext and either deterministic key or chaotic key are made. Numerical simulations on several cases of true color digital images are conducted. The outcomes are evaluated using both qualitative and quantitative analysis. The chaotic scheme is shown to be better than deterministic scheme against entropy attack and ciphertext attack.

REFERENCES

[1] R. Schilling, S. Harris, “Fundamental of Digital Signal Processing using Matlab”, Cengage Learning. 2005

[2] B. Lathi, “Modern Digital and Analog Communication Systems”, Latest Edition, Oxford University Press, 2009

[3] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "On the Security of Permutation-Only Image Encryption Schemes", IEEE Transactions on Information Forensics and Security, Volume 11, Issue 2, Feb 2016

[4] J. Tang, X. Zhang, L. Zhao, C. Zou, "A Novel Arithmetic Coding On Data Compression And Encryption With Asymptotic Deterministic Randomness", 2010 International Conference on Computer Application and System Modeling, Taiyuan, China

[5] Z. Ye, H. Mohamadian and Y. Ye, "Information Loss Determination on Digital Image Compression and Reconstruction Using Qualitative and Quantitative Analysis", Journal of Multimedia, Academy Publisher, Vol. 6, No. 6, pp. 486-493, December, 2011

[6] F. Han, J. Hu, X. Yu, Y. Wang, "Fingerprint Images Encryption Via Multi-Scroll Chaotic Attractors", Applied Mathematics and Computation 185 (2007) 931–939

[7] Z. Ye, H. Mohamadian, H. Yin, "Impact of Fractional Orders on Characteristics of Chaotic Dynamical Systems", 2016 International Conference on Science and Innovative Engineering (ICSIE), DEC. 12-13, 2016, Buenos Aires, Argentina

[8] N. Pareeka, V. Patidara, and K. Suda, "Image Encryption Using Chaotic Logistic Map", Image and Vision Computing, Volume 24, Issue 9, September 2006, Pages 926–934

[9] Z. Shen, X. Yang, H. He, W. Hu, "Secure Transmission of Optical DFT-S-OFDM Data Encrypted by Digital Chaos", IEEE Photonics Journal, Volume 8, Issue 3, June 2016

[10] J. Lang, R. Tao, Y. Wang, "Image Encryption Based On The Multiple-Parameter Discrete Fractional Fourier Transform And Chaos Function", Vol 283, Issue 10, 15 May 2010, pp. 2092–2096, Optics Communications

[11] M. Shan, J. Chang, Z. Zhong, B. Hao,"Double Image Encryption Based On Discrete Multiple-Parameter Fractional Fourier Transform And Chaotic Maps", Volume 285, Issues 21–22, 1 October 2012, Pages 4227–4234, Optics Communications