EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Fast selective encryption algorithms based on moments and chaos theory

Abdelhalim Kamrani[1,*], Khalid Zenkouar[1] and Said Najah[1]

[1]Laboratory of Intelligent Systems and Application (LSIA), Faculty of Sciences and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco

Abstract

In this work, we propose a novel selective encryption scheme based on chaos theory and moments' transforms, two moments families were considered, namely Tchebichef and Hahn. The goal is to propose an ecryption scheme that's fast and can be deployed in real world scenarios. The proposed algorithms operate in the transform domains of Tchebichef and Hahn moments. We encrypt only the most significant coefficients of the moments transforms. First, we down-sample the computed moments' matrices coefficients, then we use two logistic maps for confusion and diffusion of the down-sampled Tchebichef's and Hahn's coefficients, the resulting matrix is the encrypted image. This approach improves drastically the speed of the encryption algorithm while keeping a "good" security level. In order to prove the capabilities of our algorithms, we run different experiments and we test the algorithms on different criteria: MSE, correlation coefficient, differential analysis, entropy and time performance. The obtained results prove that the encryption scheme proposed is secure and outperform state-of-the-art algorithms.

Keywords: Image encryption, Tchebichef moments, Hahn moments, Selective encryption, Chaos encryption

Received on 27 July 2022, accepted on 20 July 2023, published on 24 July 2023

doi: 10.4108/eetiot.v9i2.2193

1. Introduction

Information security plays a huge role in securing and authenticating digital images. One of the main techniques to secure data is through encryption [1]. The goal is to obscure the data in such a way that it is only available to authorized users. Encryption algorithms are continually developed and are in wide use for almost every online application. Traditional schemes such as IDEA, RSA and DES are particularly used for text-based encryption. As for image encryption, these algorithms were reported to be insufficient [2]. In fact, as a consequence of intrinsic properties of images like high correlation among pixels and bulk data capacity; the text based encryption algorithms cannot be extended to image encryption. For that regard, specific encryption algorithms intended to be used particularly with images were developed [3–5].

Image encryption algorithms are categorized into two main categories, namely algorithms dealing with space domain and algorithms using frequency domain. The former operate directly on the pixels of the image and thus tend to be more time efficient. Meanwhile these algorithms can cause un-correlation between pixels, which makes the compression process infeasible [6]. The latter operate on the coefficients obtained in the domain of transform, these algorithms are more efficient, they can make lossless image recovery and are robust against operations of image processing [7]. In the literature, several transform domains for encryption were proposed, DCT [8], IWT [9] and FrDCT [10] to cite a few. In recent years, an attempt was made to use image moments' as a transform domain for encryption [11]. The results showed a great encryption performance for these algorithms and even outperformed the latest algorithms.

The main concern that arises when it comes to image encryption -or multimedia encryption in general- is the speed vs. the security dilemma [12]. While the security is the main purpose of image encryption, the algorithm should be fast enough to be deployed in real world applications. In fact the more we work on enhancing the security aspect of an algorithm the slower it gets [13]. Multiple works were introduced with the goal of reducing the time complexity of encryption algorithms while keeping an acceptable level of security [14–17]. In this paper, we introduce two encryption algorithms that are fast and secure using selective encryption

*Corresponding author. Email: abdelhalim.kamrani@usmba.ac.ma

and image moments. Two encryption algorithms were proposed based on Tchebichef and Hahn moments. The conducted experiments prove that the proposed scheme is secure against all attacks and is fast enough to be deployed in day-to-day applications. This paper is organized as follows: in the second section, the essential knowledge to understand our algorithms is proposed. The third section presents the proposed scheme in details. In section four, we present the results of our experiments, and finally a conclusion is presented in section 5.

2. preliminary knowledge

Here we present the necessary background to comprehend the proposed approach. Two main concepts are explained: chaos theory and moments transforms particularly Tchebichef and Hahn moments:

2.1. Moments theory

The first introduction of moments theory into image analysis was by Hu[18] in 1961. He proposed invariant moments that found several applications [19, 20] due to there capabilities of representing global features. The main disadvantage of these moments is that they are not orthogonal and thus the reconstruction of the image is not a trivial task.

Zernike and Legendre moments were the second next category of moments that was proposed by Teague [21] in 1980. These moments are orthogonal and represent information with minimal redundancy. Nevertheless, these moments had several disadvantages such as coordinate space transformation,large variation in the dynamic range of values and numerical approximation of continuous integrals.

New set of orthogonal discrete moments have been proposed over the recent years, these moments use discrete orthogonal polynomials as the basis set. Thus they have a superior image representation [22].

Tchebichef moments. Tchebichef moments first introduced by Mukundan et al. [22] and are defined as:

$$T_{pq} = \frac{1}{\rho(p,N)\rho(q,N)} \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} t_p(x)t_q(y)f(x,y) \quad (1)$$

And the inverse moment transform to construct the original image given a set of moments T_{pq} :

$$f(x,y) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} T_{mn}t_m(x)t_n(y) \quad (2)$$

Where $t_n(x)$ are the scaled Tchebichef polynomials expressed as

$$t_n(x) = \frac{t_n(x)}{\beta(n,N)} \quad (3)$$

$t_n(x)$ is the discrete Tchebichef polynomials of degree n, given by:

$$t_n(x) = (1-N)_{x3}F_2(-n,-x,1+n;1,1-N;1) \quad (4)$$

Where $(a)_n$ is the pochhammer symbol given by:

$$(a)_k = a(a+1)(a+2)...(a+k-1) \quad (5)$$

and ${}_3F_2$ is defined as:

$${}_3F_2(a_1,a_2,a_3;b_1,b_2;z) = \sum_{k=0}^{\infty} \frac{(a_1)_k(a_2)_k(a_3)_k}{(b_1)_k(b_2)_k}\frac{z^k}{k!} \quad (6)$$

Hahn moments. In 2005, Zhou [23] proposed a new set of discrete orthogonal moment functions based on Hahn polynomials. The Hahn moments for an image $f(x,y)$ are described as follows:

$$H_{mn} = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(x,y)\tilde{h}_m^{\mu,\nu}(x,N)\tilde{h}_n^{\mu,\nu}(y,N) \quad (7)$$

Where $\tilde{h}$ is the scaled Hahn polynomial described as:

$$\tilde{h}_n^{\mu,\nu}(x,N) = h_n^{\mu,\nu}(x,N)\sqrt{\frac{\rho(x)}{d_n^2}} \quad (8)$$

and d_n^2 is the square norm which has the following expression:

$$d_n^2 = \frac{\Gamma(2N+\mu+\nu-n)}{(2N+\mu+\nu-2n-1)\Gamma(N+\mu+\nu-n)} \times \frac{1}{\Gamma(N+\mu-n)\Gamma(N+\nu-n)\Gamma(n+1)\Gamma(N-n)}$$

and $\rho(x)$ is the weighting function which is given by:

$$\rho(x) = \frac{1}{\Gamma(x+1)\Gamma(x+\mu+1)\Gamma(N+\nu-x)\Gamma(N-n-x)} \quad (9)$$

$h_n^{\mu,\nu}(x,N)$ are the Hahn polynomials defined as:

$$h_n^{\mu,\nu}(x,N) = (N+\nu-1)_n(N-1)_n \times \sum_{k=0}^{n}(-1)^k \frac{(-n)_k(-x)_k(2N+\mu+\nu-n-1)_k}{(N-\nu-1)_k(N-1)_k} \times \frac{1}{k!} \quad (10)$$

Where $(a)_k$ is the pochhammer symbol.

2.2. Chaos encryption

The chaos encryption process is typically divided into two main stages: The first stage is called confusion, the pixels are transposed with a random sequence generated by a chaotic map without changing the values of the pixels. This operation obscures the image but it is not enough to make it secure. The second stage is called diffusion; the pixels' values are changed using a random sequence. The confusion and the diffusion are repeated until a required level of security is achieved.

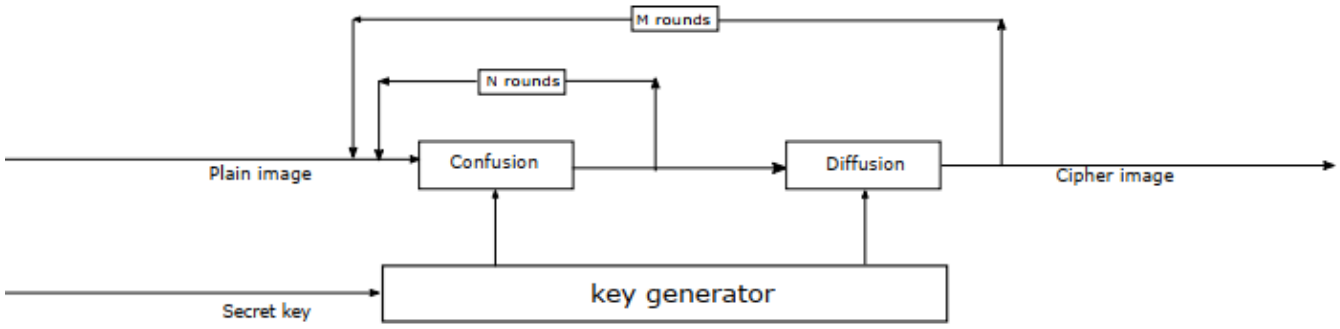

Figure 1. General scheme for chaos based encryption

3. The proposed algorithm

In this work, a new encryption scheme is introduced based on chaos and moments transforms. The proposed scheme is based on selective encryption, which makes it extremely fast without compromising the security aspect. We propose two encryption algorithms based on the same scheme, the difference between the two algorithms is the family of moments used; namely Tchebichef and Hahn moments. In this section, we explain in details the encryption algorithms.

3.1. Encryption

1. **Segmentation and Down Sampling**: First the image is segmented into blocks of 8*8, then we compute the moments' coefficients for each block. In order to speed the encryption process, we down sample the matrix coefficients into a matrix of 3*3. These coefficients encompass most of the information and thus the image can be represented by this down sample without much loss.

2. **Key generation**: K is a key of length 128 bits, which is divided into 2 segments: K_1 and K_2.The logistic map used for encryption has as input a value between 1 and 0. We apply some operations on the key segments in order to adopt them to the logistic map entry. Each segment K_i is presented by its binary form which can be noted as: $K_1 = K_{11}, K_{12}...K_{164}.K_2 = K_{21}, K_{22}...K_{264}$. The input values for the logistic maps are calculated as: $X_0 = (K_{11}2^0 + K_{12}2^1 + ... + K_{164}2^{63})/2^{64}$. $Y_0 = (K_{21}2^0 + K_{22}2^1 + ... + K_{264}2^{63})/2^{64}$ Where X_0 and Y_0 are the inputs for the logistic maps X and Y.

3. **Confusion**: We use the logisitic map X with the input X_0 to generate an array of size 96*96. The matrix derived from step 1 is converted to an array of size 9216 (96*96). This array is permuted according to the map generated by X.

4. **Diffusion**: Another random sequence is generated from Y with initial condition Y_0. Then this sequence is XORed with the array generated from step 3. The result is the encrypted image E.

3.2. Decryption

Decryption is the inverse process of encryption, the goal is to reconstruct the original image from the encrypted image. First we convert the encrypted image E to an array of size 96*96. This array is then XORed with sequence generated by Y with initial condition Y_0. We permute the resulted array according to the sequence generated by X with intial condition X_0. this array is transformed to a 256*256 matrix by sampling, i.e. the remaining pixels are put to zero. Then we compute the inverse tchebichef and Hahn moments. Thus we end up with the decrypted image I'.

4. Experimental study

We present the results of our experiments in this section. Our proposed scheme is compared to state-of-the-art algorithms to prove their efficiency. The results of these experiments are given below.

4.1. Space key analysis

For a secure encryption scheme, the key-space must be larger than 2^{100} [24]. The proposed algorithms has 2^{128} possible combinations of encryption key.

4.2. Image similarity

The proposed scheme is a "Lossy" image encryption since it only considers the most significant bits in the encryption process. To measure the "loss" during the image reconstruction / decryption we use the Mean Squared Error (MSE), which is defined as:

$$MSE = \frac{1}{NM}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}[f(x,y) - g(x,y)]^2 \qquad (11)$$

$f(x,y)$ is the original image $g(x,y)$ is the decrypted image size $M * N$

The algorithms in Refs [25–27], are lossless algorithms which explains the value 0 of the MSE. i.e. the decrypted image perfectly matches the original image. However, the proposed algorithms have some information lost due to the selective encryption process. Meanwhile the values of the MSE for the proposed algorithms are close to 0, this means that the original image and the decrypted image are similar and the difference is unnoticeable to the naked eye.

4.3. correlation coefficient

As a security measure, we should minimize the similarity between the encrypted image and the original one. The correlation coefficient is a metric used just for that, it takes a value between -1 and 1. A value of 0 indicates no correlation between the compared image while a value of 1 is an indicator that the two images are perfectly correlated. The correlation coefficient is defined as:

$$C.C = \frac{Cov(x,y)}{\sigma_x \times \sigma_y} \tag{12}$$

$$\sigma_x = \sqrt{VAR(x)} \tag{13}$$

$$\sigma_y = \sqrt{VAR(y)} \tag{14}$$

$$VAR(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{15}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{16}$$

y and x are positions of the pixels in the encrypted image and plain image respectively, $VAR(x)$ is the variance for pixel x, $Cov(x;y)$ is covariance, σ_x is the standard deviation while N is the number of pixels.

The results are presented in Table 2. We compute the correlation coefficient for vertical, horizontal and diagonal pixels. It is clear from the results that the correlation coefficient is close to 0 for all the algorithms including the proposed algorithms, this shows that the algorithms are secure against statistical attacks.

4.4. Differential analysis : NPCR & UACI

To demonstrate resistance to differential attacks, two quantitative descriptors are used: NPCR and UACI, they provide a security proof against chosen plaintext attacks. The encryption scheme should show a good image sensitivity.

The encrypted image should show a qualitative transformation if one pixel value is altered in the original image. NPCR and UACI can be described mathematically as:

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100 \tag{17}$$

$D(i,j)$ can be expressed as:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100 \tag{19}$$

When UACI is around 33.4 and the NPCR is approximately about 99.6, the encryption is considered resistant to differential attacks. We encrypt Lena, Baboon and Cameraman pictures using the proposed scheme and compare the results to state-of-the-art algorithms. From the tables 3 and 4, the NPCR values for the proposed algorithms are all higher than 99.8 and the UACI values are around to 31, which implies that the proposed algorithms are secure against differential attacks. Furthermor,e compared to other algorithms the proposed algorithms exhibit good security performance.

4.5. Entropy

Entropy measures the randomness in a system. It is used for evaluating the security of an image encryption scheme. A secure algorithm should increase the entropy by decreasing the mutual information among pixels. For a message m The entropy $H(m)$ can be measured by the formula:

$$H(m) = \sum_{i=0}^{M-1} p(m_i) log \frac{1}{m_i} \tag{20}$$

$p(m_i)$ is probability of occurrence for the symbol m_i and M denotes the number of all possible symbols. Ideally, an entropy value of 8 means the source is completely random, but realistically we can only reach values close to 8.

The results are depicted in Table 5, the entropy values for the encrypted images are all above 7.99 which means all the algorithms pass the entropy test. Moreover we see that our algorithms exhibit good results compared to other algorithms.

4.6. Speed Analysis

Our main contribution is developing a lightweight encryption algorithm, which is fast and secure at the same time. In order to validate the time performance aspect of our proposed scheme, we analyze the time performance with different image sizes, i.e. 256×256, 512×512 and 1024×1024 and compare the results

Table 1. MSE results

MSE	Tchebichef	Hahn	Ref[25]	Ref[26]	Ref[27]
Lena	2.1 x 10-3	1.9 x 10-3	0	0	0
Baboon	1.6 x 10-4	2.6 x 10-3	0	0	0
Cameraman	7.3 x 10-4	2.4 x 10-4	0	0	0

Table 2. Correlation coefficient results

C.C	Plain image	Tchebichef	Hahn	Ref[25]	Ref[26]	Ref[27]
Horizontal	0.8263	0.039	0.0015	-0.0025	-0.088	0.0039
Vertical	0.9273	-0.0078	0.0092	0.00126	0.079	0.002
Diagonal	0.867	0.046	-0.0084	-0.006	0.096	0.076

Table 3. NPCR results

NPCR	Tchebichef	Hahn	Ref[25]	Ref[26]	Ref[27]
Lena	99.8731	99.9807	99.9961	99.9961	99.9955
Baboon	99.9289	99.9304	99.9953	99.996	99.9958
Cameraman	99.8149	99.9712	99.9959	99.996	99.9956

Table 4. UACI results

UACI	Tchebichef	Hahn	Ref[25]	Ref[26]	Ref[27]
Lena	31.712	31.144	33.232	33.198	33.174
Baboon	31.039	32.162	33.161	33.166	33.255
Cameraman	26.140	31.702	33.332	33.212	33.26

Table 5. Entropy results

Entropy	Tchebichef	Hahn	Ref[25]	Ref[26]	Ref[27]
Lena	7.9924	7.9968	7.9964	7.9967	7.996
Baboon	7.996	7.9944	7.9959	7.9963	7.9961
Cameraman	7.9926	7.9940	7.9961	7.996	7.9952

with other algorithms. The results are shown in table 6. The proposed encryption scheme is based on selective encryption, which makes it extremely fast compared to other algorithms. The table 6 shows clearly that our proposed algorithms outperform state-of-the-art algorithms when it comes to time performance.

5. Conclusion

In this work, we introduce a novel selective chaotic encryption scheme based on Tchebichef and Hahn moments. Our main object was to propose a fast encryption algorithm that can be deployed in real world applications without harming the security aspect. We achieved that by encrypting only the most significant bits in the transform domain of Tchebichef and Hahn moments. The encryption scheme is a "Lossy" one, which means that the decrypted image is not similar at a 100% to the original image, but the similarity measure shows that it's close enough not to be noticed by naked eye. The experimental results showed that our encryption scheme is secure against all known attacks, furthermore the speed analysis proved that the proposed algorithms outperformed state-of-the-art algorithms. Given the presented results of the proposed algorithms, we are confident about their ability to be deployed in real world applications. Our future works will be focused on implementing these algorithms for video encryption.

References

[1] Kaur, M. and Kumar, V. (2020) A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering* **27**(1): 15–43.

Table 6. Speed analysis results

Speed Analysis	Tchebichef	Hahn	Ref[25]	Ref[26]	Ref[27]
256 * 256	0.138	0.188	0.46	0.442	0.11794
512 * 512	0.330	0.285	0.979	0.466	0.27444
1024 * 1024	0.480	0.459	1.1361	0.975	0.78902

[2] Li, S., Chen, G., Cheung, A., Bhargava, B. and Lo, K.T. (2007) On the design of perceptual mpeg-video encryption algorithms. *IEEE Transactions on Circuits and Systems for Video Technology* **17**(2): 214–223.

[3] Zolfaghari, B. and Koshiba, T. (2022) Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap. *Applied System Innovation* **5**(3): 57.

[4] Zhao, R., Zhang, Y., Nan, Y., Wen, W., Chai, X. and Lan, R. (2022) Primitively visually meaningful image encryption: A new paradigm. *Information Sciences* **613**: 628–648.

[5] Wang, M.m., Zhou, N.r., Li, L. and Xu, M.t. (2022) A novel image encryption scheme based on chaotic apertured fractional mellin transform and its filter bank. *Expert Systems with Applications* **207**: 118067.

[6] Zheng, N., Jiang, X. and Lan, X. (2006) *Advances in Machine Vision, Image Processing, and Pattern Analysis: International Workshop on Intelligent Computing in Pattern Analysis/Synthesis, IWICPAS 2006, Xi'an, China, August 26-27, 2006, Proceedings*, **4153** (Springer).

[7] Guan, M., Yang, X. and Hu, W. (2019) Chaotic image encryption algorithm using frequency-domain dna encoding. *IET image processing* **13**(9): 1535–1539.

[8] Xin, G., Fen-lin, L., Bin, L., Wei, W. and Juan, C. (2010) An image encryption algorithm based on spatiotemporal chaos in dct domain. In *2010 2nd IEEE international conference on information management and engineering* (IEEE): 267–270.

[9] Luo, Y., Du, M. and Liu, J. (2015) A symmetrical image encryption scheme in wavelet and time domain. *Communications in Nonlinear Science and Numerical Simulation* **20**(2): 447–460.

[10] Wu, J., Guo, F., Zeng, P. and Zhou, N. (2013) Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence. *Journal of Modern Optics* **60**(20): 1760–1771.

[11] Kamrani, A., Zenkouar, K. and Najah, S. (2020) A new set of image encryption algorithms based on discrete orthogonal moments and chaos theory. *Multimedia Tools and Applications* **79**(27): 20263–20279.

[12] Wang, X., Feng, L. and Zhao, H. (2019) Fast image encryption algorithm based on parallel computing system. *Information Sciences* **486**: 340–358.

[13] Zhu, S., Wang, G. and Zhu, C. (2019) A secure and fast image encryption scheme based on double chaotic s-boxes. *Entropy* **21**(8): 790.

[14] Kang, S.W., Choi, U.S. and Cho, S.J. (2022) Fast image encryption algorithm based on (n, m, k)-pcmlca. *Multimedia Tools and Applications* **81**(1): 1209–1235.

[15] Eyebe Fouda, J. and Koepf, W. (2022) An 8-bit precision cipher for fast image encryption. *Multimedia Tools and Applications* : 1–20.

[16] Gao, X., Mou, J., Xiong, L., Sha, Y., Yan, H. and Cao, Y. (2022) A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. *Nonlinear Dynamics* **108**(1): 613–636.

[17] Song, W., Fu, C., Tie, M., Sham, C.W., Liu, J. and Ma, H.f. (2022) A fast parallel batch image encryption algorithm using intrinsic properties of chaos. *Signal Processing: Image Communication* **102**: 116628.

[18] Hu, M.K. (1962) Visual pattern recognition by moment invariants. *IRE transactions on information theory* **8**(2): 179–187.

[19] Dudani, S.A., Breeding, K.J. and McGhee, R.B. (1977) Aircraft identification by moment invariants. *IEEE transactions on computers* **100**(1): 39–46.

[20] Casasent, D. and Cheatham, R.L. (1984) Image segmentation and real-image tests for an optical moment-based feature extractor. *Optics communications* **51**(4): 227–230.

[21] Teague, M.R. (1980) Image analysis via the general theory of moments. *Josa* **70**(8): 920–930.

[22] Mukundan, R., Ong, S. and Lee, P.A. (2001) Image analysis by tchebichef moments. *IEEE Transactions on image Processing* **10**(9): 1357–1364.

[23] Zhou, J., Shu, H., Zhu, H., Toumoulin, C. and Luo, L. (2005) Image analysis by discrete orthogonal hahn moments. In *International Conference Image Analysis and Recognition* (Springer): 524–531.

[24] Alvarez, G. and Li, S. (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos* **16**(08): 2129–2151.

[25] Wang, Y., Wong, K.W., Liao, X. and Chen, G. (2011) A new chaos-based fast image encryption algorithm. *Applied soft computing* **11**(1): 514–522.

[26] Wang, X. and Gao, S. (2020) Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Information sciences* **507**: 16–36.

[27] Song, W., Zheng, Y., Fu, C. and Shan, P. (2020) A novel batch image encryption algorithm using parallel computing. *Information Sciences* **518**: 211–224.