IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 5 Issue 6, June 2018
ISSN (Online) 2348 – 7968
www.ijiset.com

A Hybrid Image Encryption and Decryption Using Logistic Map & Block Based Encryption

Shruti Garg[1] and Er. Jasdeep Singh Mann[2]

P.G. Student, Department of Computer Engineering, BMS Engineering College,
Sri Muktsar Sahib, India[1]
Associate Professor, Department of Computer Engineering, BMS Engineering College,
Sri Muktsar Sahib, India[2]

Abstract

In this paper, a novel image encryption algorithm is proposed. The Chaotic Logistic Map in bits of pixels and the block based encryption system are employed for the encryption of the proposed scheme. For Logistic Map operations, random key use to generate the logistic map with the same size of the original image, to scramble the image. The scrambled image is encrypted into the ciphered image by the block based encryption with the help of private key. Then again apply logistic mapping on encrypted image to enhance the image complexity. The simulation experiments and theoretical analyses indicate that the proposed scheme is superior and able to resist exhaustive attack and statistical attack

Keywords: *Image encryption, Chaos, block structure, logistic map.*

1. Introduction

Nowadays more and more images and videos are transmitted through Internet. This brings great convenience to people in daily life as they can obtain what they want on the Internet conveniently. But there are some problems: the information transmitted on the Internet can be intercepted, tampered and destroyed illegally. So the secure transmission of images has become urgent. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption[2,3] are not suitable for image encryption. Since chaos has the characters of non-periodicity, non-convergence, ergodicity and sensitive dependence on initial conditions, chaos-based image encryption system attracts more and more people's attentions. Therefore, Chaotic Logistic Map[4,5] is a suitable technology for scrambling images because this technology contains many features such as simplicity, efficiency, size flexibility of images, randomness. And Block cipher[6] are deterministic algorithms operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. Block ciphers are important elementary components in the design of many cryptographic protocols, and are widely used to implement encryption of bulk data. So, the combination of Logistic Mapping for scrambling of image and Block-based encryption[7,8] of image can increase the security of the encryption scheme and resist common attacks. The theoretical analyses and experimental results in the rest of the paper indicate the security of proposed image encryption scheme

2. PROPOSED WORK

Chaotic system has been widely used in encryption algorithms for its good characteristics. Generally, chaotic systems are applied in both the key generations and data scramble for cryptography design based on its randomness characteristic. Therefore, the chaotic Logistic Map system is applied to efficiently scramble the image with the help of random key[9] which we generate with the help of chaotic system. Furthermore, this operation is reversible and asymmetric for a decryption process.

2.1. Encryption process

The process of the proposed encryption scheme is as follows:

Step 1: Read the real Image and do pre-processes on the image. Pre-processes are

1. Read the image
   Img = imread([p,f]);
2. Resize the image to make it compatible with the block size
   Img = imresize(Img[512,512]);
3. Convert the image in to gray as we are working on gray image
   Img =rgb2gray(Img);

Step 2: Initialize Random Key and Private Key.

1. Generate non-negative integer as Random Key with the help of “twister” function

```
    2.   Select one more non-negative key as private key
    3.   Initialize one wrong key
    4.   Mention the block size, to divide the real image
Step 3: Divide the Real Image in to equal size of blocks $S_b$
Step 4: Set the Mode on for encryption
Step 5: We use FOR LOOP here
    1.   For Block $S_b$ in All Blocks
          For Row r in Block $S_b$
           For Column c in Block $S_b$
         1.1  Use Logistic Map to shuffle image block $S_b$
         1.2  Generate a key matrix of 5 more Private Keys
              k1,k2,k3,k4,k5 with the help of Private Key
         1.3  Use Block Based Encryption to encrypt all
              image blocks $S_b$ with the help of 5 generated
              keys
         1.4  Combine all the Encrypted sub blocks $S_b$ and
              get the encrypted image
         1.5  Using Logistic Map Shuffle the encrypted
              image again to increase the complexity of
              pixel relation
    2.   Get the final Encrypted image
Step 6: Stop
```

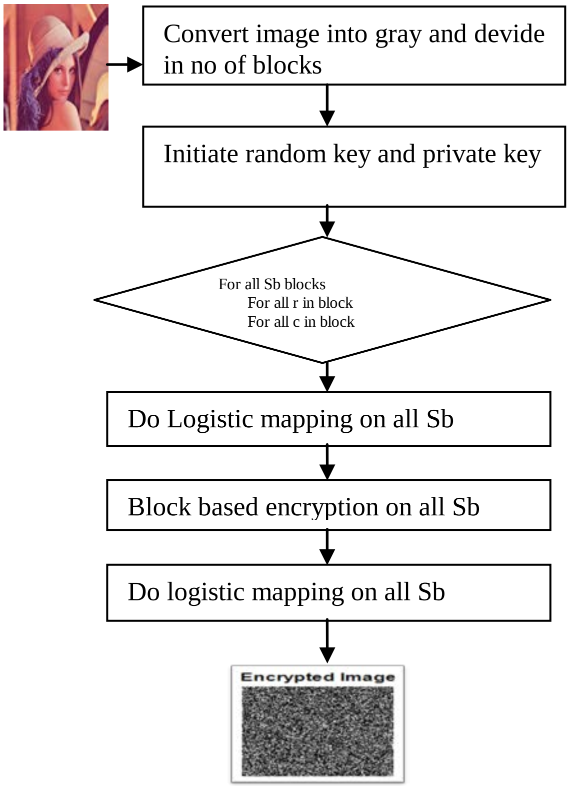
Convert image into gray and devide in no of blocks
Initiate random key and private key
For all Sb blocks
For all r in block
For all c in block
Do Logistic mapping on all Sb
Block based encryption on all Sb
Do logistic mapping on all Sb
Encrypted Image

Fig 1 Block diagram of encryption

2.2 Image Decryption Algorithm

The decryption process is the inverse process of the corresponding encryption scheme

```
Step 1: Get the encrypted image
Step 2: Also get the Private Key and Random Key
Step 3: Set the Mode as Decryption
    1.   Mention the block size to divide the encrypted
         image
Step 4: Divide the image in to equal size of blocks
Step 5: Use FOR LOOP
    1.   For Block $S_b$ in All Blocks
          For Row r in Block $S_b$
           For Column c in Block $S_b$
         1.1  Use Logistic Map to reshuffle the image
              Block Sb
         1.2  Generate a key matrix of 5 more Private Keys
              k1,k2,k3,k4,k5 with the help of Private Key
         1.3  Use Block Based Decryption to decrypt all
              image blocks $S_b$ with the help of 5 generated
              keys
         1.4  Combine all the Decrypted sub blocks $S_b$ and
              get the semi encrypted image
         1.5  Use Logistic Map to reshuffle the semi-
              encrypted image again to get the real image
    2.   Get the real image in grey colors
Step 6: Stop
```

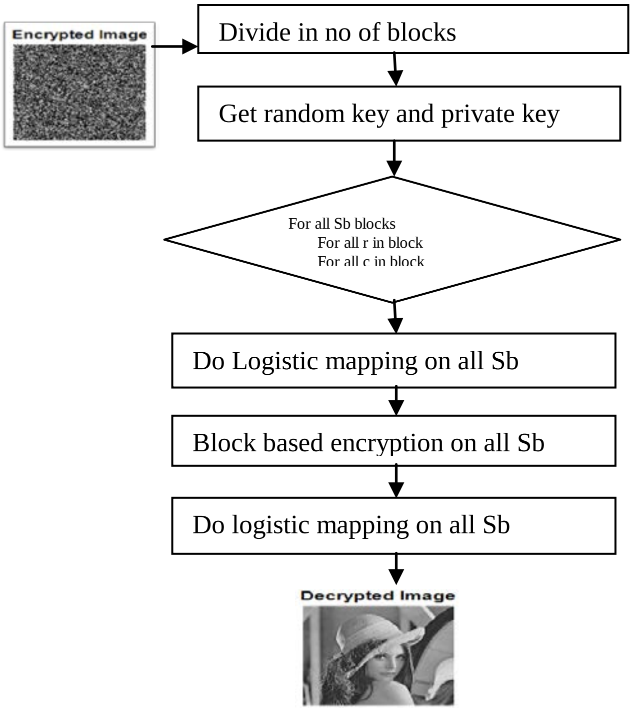
Encrypted Image
Divide in no of blocks
Get random key and private key
For all Sb blocks
For all r in block
For all c in block
Do Logistic mapping on all Sb
Block based encryption on all Sb
Do logistic mapping on all Sb
Decrypted Image

Fig 2 Block Diagram of Decryption

3. Experimental results and analysis

Simulation results and performance analysis for the proposed scheme are reported in this section. The software Matlab is used to demonstrate, validate and evaluate the algorithm by simulation experiments. The images of Lena and Lion, the 256 _ 256 images with 256 grey levels, are encrypted individually. Figures below shows the experimental results of Lena and Lion images. The original Leena image is Fig 3 while Fig 4 is the Gray image image. Fig 5 is the encrypted image and Fig 6 is the decrypted image using the correct keys. Fig 7,8,9 shows the experimental result of the image Lion. The original image is Fig 7 while Fig 8 is the Encrypted image. Fig 9 is the decrypted image by using the correct keys. The experimental results indicate that the proposed scheme is secure.

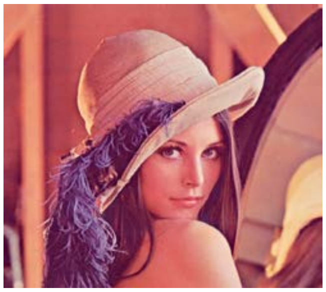

Fig 3 The Standard Lena Image 512x512

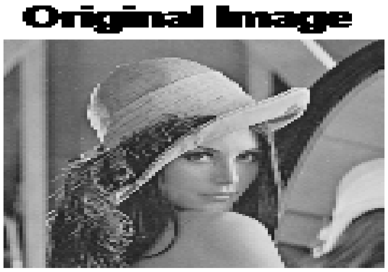

Fig 4 The grayscale image of Leena

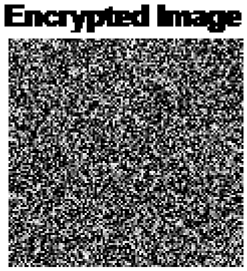

Fig 5 The encrypted image of Leena

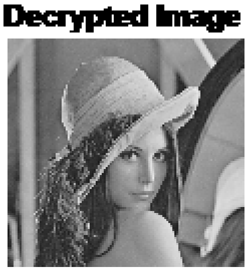

Fig 6 The decrypted image of Leena

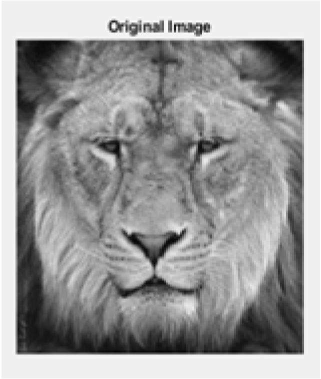

Fig 7 The orignal gary image of Lion, as taken it from base paper

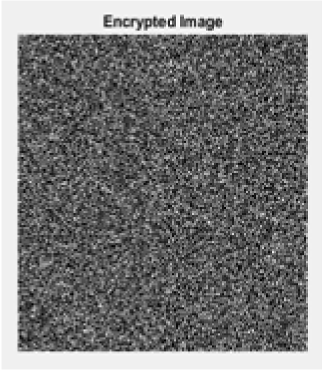

Fig 8 The encrypted image of Lion

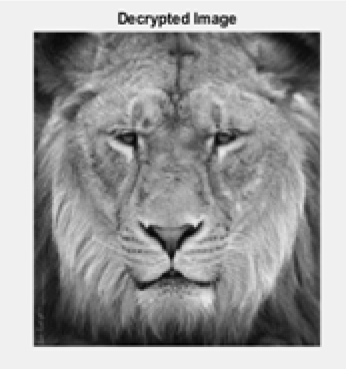

Fig 9 The decrypted image of Lion

3.1 Performance analysis

3.1.1 Secret key's space

In this, We have two secret keys[10] one is Random key which include the initial values of logistic map and other is Private Key which is use by internal coding to generate five more keys which are used in Block Based encryption. Each pixel of the gray image is 8 bit. Therefore, if the attackers want to recover the random key in Logistic Map operations, they have to cost $8^{256*256}$ times calculations and for Block Based encryption Key they have to try further for 2^{15} time more calculations. Obviously, Random key is large enough for the key space to resist force-brute-attack, but as we are using the secret key matrix here which provide more complex system for attacker to crack the system.

3.1.2. Information Entropy

Information entropy[11] analysis is carried out to show the distribution of the gray values. This entropy is defined as follows:

$$H(S) = \sum_{s} \left(P(si)_{log2} \quad \frac{1}{P(si)} bit \right)$$

where P(si) refers to the probability of each symbol appearance. The ideal entropy value for a ciphered image should be 8, which means that the more the distribution of a gray value is uniform, the greater the information entropy. Therefore, a value below 8 would give a possibility of broken the image security of the ciphered image. The entropy of experimental results in the proposed scheme is 7.99954378. The obtained result is close to the ideal value 8. This indicates that the rate of information leakage in the proposed scheme is negligible and the ciphered image using the proposed scheme is secure against any kind of entropy attack.

3.1.3 Sensitivity Analysis

Generally, an attacker may make a slight change (e.g. only one pixel changed) of the original image, and then observes the change of encryption results. In this way, the attacker may be able to find out a meaningful relationship between two ciphered images and the original image. In order to test the influences of this attack, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used. Eqs. For calculating NPCR and UACI are as follows:

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} D(i,j)}{M \times N} \times 100$$

$$UACI = \frac{1}{M \times N} \left[\frac{\sum_{i=1}^{M} \sum_{j=1}^{M} |m_1(i,j) - m_2(i,j)|}{256} \right] \times 100$$

where m1 and m2 are two different ciphered images.

For the image of Lena, the values of NPCR and UACI are 99.88% and 33.32%, respectively. For image of Lion, the values of NPCR and UACI are 99.90% and 33.37%, respectively. For all cryptographic systems, the idea results of NPCR and UACI are100% and 33.33%, respectively. Therefore, experimental results of the proposed scheme are close to the idea results.

3.1.4 Correlation Coefficient Analysis

As a good encryption scheme, the correlation between adjacent pixels should be significantly reduced in the ciphered image. Here, correlation coefficient is applied to analyze the proposed scheme for resisting statistical attack. In order to analyze correlations of the original image and the ciphered image, 1000 pairs of two adjacent pixels from original image and ciphered image in horizontal, vertical, and diagonal direction respectively are selected. Eq. is used to calculate the correlation coefficient as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Direction	Horizontally	Vertically	Diagonal (lower left to top right)	Diagonal (lower right to top left)

Orignal image of leena pixel values	0.9352	0.9456	0.9255	0.9565
Orignal image of lion pixel values	0.9722	0.9601	0.9823	0.9211
Ciphered image of leena	0.00089	0.0029355	0.00185	0.08710
Ciphered image of lion	0.00066	0.0002404	0.00134	0.00892

Table 1: Correlation Coefficient comparison of real image of Leena and Lion with the Ciphered image of Leena and Lion

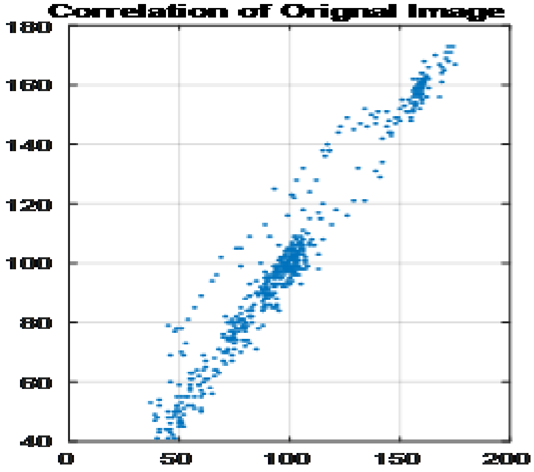

Fig 10 Correlation among pixels of orignal image Leena

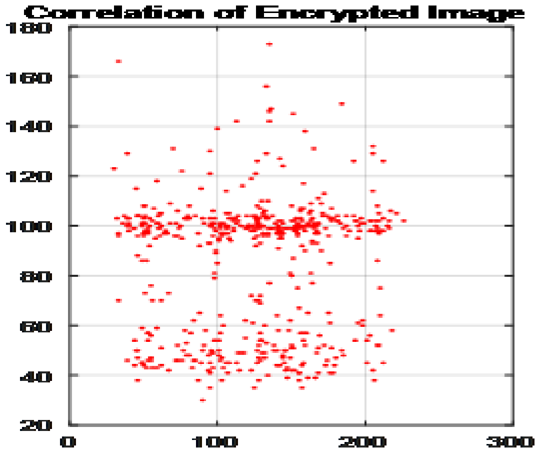

Fig 11 Correlation among pixels of encrypted image of leena

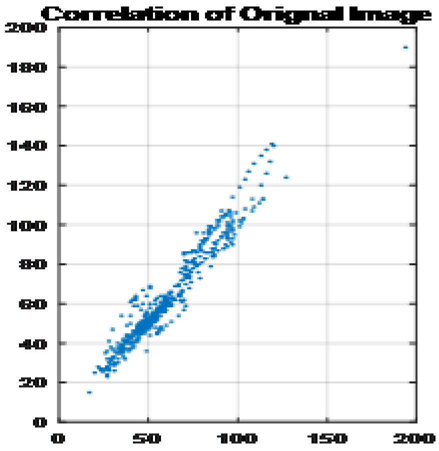

Fig 11 Correlation among the pixels of orignal iamgeof lion

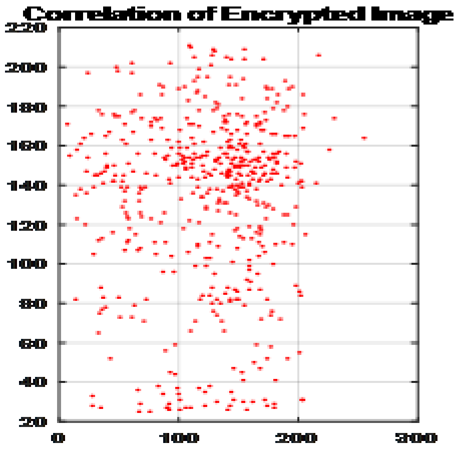

Fig 12 Correlation among the pixels of encrypted image of lion

3.1.5 Distribution

The histogram of an image reveals the distribution information of pixel values and statistical characteristics of images. An ideal encrypted image should have a uniform and completely different histogram against the plain-image. The experimental results of histograms are shown in Figs 13,14,15 and 16.

The results indicate that each histogram has a specific pattern that depends on the corresponding image before encryptions. After the encryption process, pixel values are distributed uniformly. Thus, it is difficult for attackers to recover the original image from statistical characteristics of ciphered images.

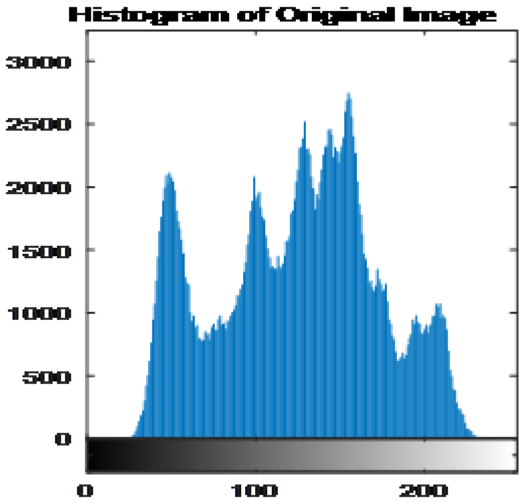

Fig 13 The histogram graph of orignal image of leena

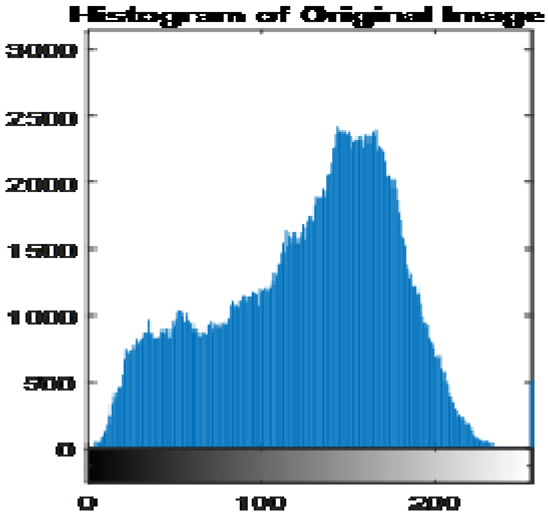

Fig 15 The histogram graph of original image of lion

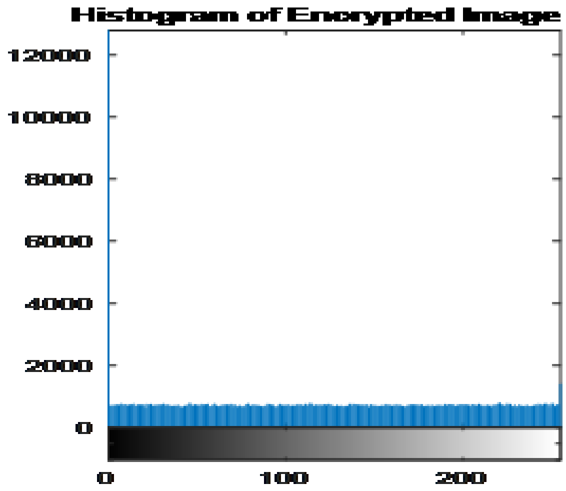

Fig 14 The histogram graph of encrypted image of leena

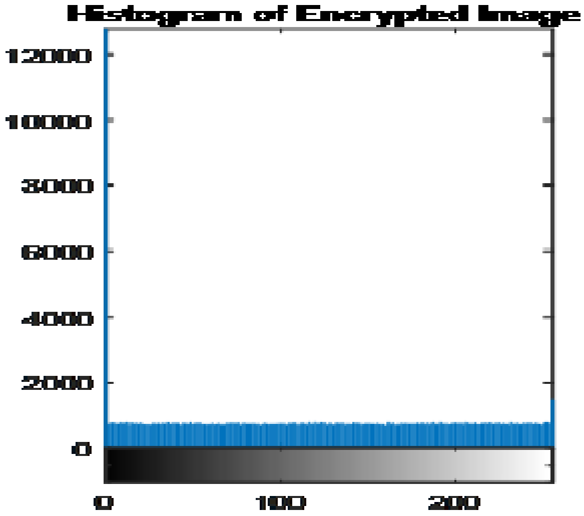

Fig 16 The historam graph of Encrypted image of lion

4 Conclusions

In this paper, a new image encryption algorithm based on the Logistic mapping and block based encryption is proposed. The arithmetic designs a method of key generation and utilizes the map to shuffle the position of image pixels and block based encryption to encrypt the image. The experimental tests have been carried out and the results show the efficiency of the arithmetic. A technique for image encryption using number theoretic paradigm is developed. The block based encoding operation performed by the proposed method is shown to be simple in terms of computational complexity. The amount of encryption achieved for different images using the proposed method is comparable with that of the conventional methods and also high level of security is provided to the transmitted images. The results obtained illustrate that the proposed algorithm provides a new encryption technique which has the features of coding benefits depending on the statistics of the image, inbuilt encryption module to enable secure transmission and less system complexity. However, one must be aware of the fact that although the algorithm is safe against passive eavesdropping and other attacks, it is protected from the active attacks.

References

[1]. Wang, X. Y., Gu, S. X., & Zhang, Y. Q. (2015). Novel image encryption algorithm based on cycle shift and chaotic system. *Optics and Lasers in Engineering*, *68*, 126-134.

[2]. Cheng, H., & Li, X. (2000). Partial encryption of compressed images and videos. *IEEE Transactions on signal processing*, *48*(8), 2439-2451.

[3]. Yekkala, A. K., Udupa, N., Bussa, N., & Madhavan, C. V. (2007, January). Lightweight encryption for images. In *Consumer Electronics, 2007. ICCE 2007. Digest of Technical Papers. International Conference on* (pp. 1-2). IEEE.

[4]. Li, C., Xie, T., Liu, Q., & Cheng, G. (2014). Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dynamics*, *78*(2), 1545-1551.

[5]. Nayak, M., Dash, D., & Sa, K. D. (2017, December). An improved image encryption technique using diffusion method associated with hill cipher and chaotic logistic map. In *Man and Machine Interfacing (MAMI), 2017 2nd International Conference on* (pp. 1-6). IEEE.

[6]. Dworkin, M. J. (2016). *Recommendation for block cipher modes of operation: The CMAC mode for authentication* (No. Special Publication (NIST SP)-800-38B).

[7]. Shaw, N., Dey, B., Mazumder, S., & Laskar, F. M. (2017). ENHANCE THE DATA SECURITY BY CHANGINGTHE ENCRYPTION TECHNIQUE BASED ON DATA PATTERN IN BLOCK BASED PRIVATE KEY DATA ENCRYPTION. *International Journal of Advanced Research in Computer Science*, *8*(7).

[8]. Mohamed, F. K. (2014). A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology, an International Journal*, *17*(2), 85-94.

[9]. Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2016). Hash key-based image encryption using crossover operator and chaos. *Multimedia tools and applications*, *75*(8), 4753-4769.

[10]. Chou, R. A., Bloch, M. R., & Abbe, E. (2015). Polar coding for secret-key generation. *IEEE Transactions on Information Theory*, *61*(11), 6213-6237.

[11]. Li, C., Feng, B., & Lü, J. (2018). Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *arXiv preprint arXiv:1803.10024*.

[12]. Teodoro, G., Kurç, T. M., Taveira, L. F., Melo, A. C., Gao, Y., Kong, J., & Saltz, J. H. (2016). Algorithm sensitivity analysis and parameter tuning for tissue image segmentation pipelines. *Bioinformatics*, *33*(7), 1064-1072.

[13]. Gu, W., Lv, Z., & Hao, M. (2017). Change detection method for remote sensing images based on an improved Markov random field. *Multimedia Tools and Applications*, *76*(17), 17719-17734.

[14]. Jain, A., & Rajpal, N. (2016). A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimedia Tools and Applications*, *75*(10), 5455-5472.

[15]. Blaber, J., Adair, B., & Antoniou, A. (2015). Ncorr: open-source 2D digital image correlation matlab software. *Experimental Mechanics*, *55*(6), 1105-1122.

[16]. van den Oord, A., Kalchbrenner, N., Espeholt, L., Vinyals, O., & Graves, A. (2016). Conditional image generation with pixelcnn decoders. In *Advances in Neural Information Processing Systems* (pp. 4790-4798).

[17]. Lim, S. H., Isa, N. A. M., Ooi, C. H., & Toh, K. K. V. (2015). A new histogram equalization method for digital image enhancement and brightness preservation. *Signal, Image and Video Processing*, *9*(3), 675-689.

[18]. Bagheri, M., Mohammadi, K., Taheri, M., & Mosavi, M. R. (2010, December). "Evolution of mapping functions for image encryption using Evolvable Hardware". In *Telecommunications (IST), 2010 5th International Symposium on* (pp. 852-857). IEEE.

[19]. Chai, X., Chen, Y., & Broyde, L. (2017). "A novel chaos-based image encryption algorithm using DNA sequence operations". *Optics and Lasers in engineering*, *88*, 197-213.

[20]. Cheepchol, S., San-Um, W., Kiattisin, S., & Leelasantitham, A. (2014, March). "Digital biometric facial image encryption using chaotic cellular automata for secure image storages". In *Information and Communication Technology, Electronic and Electrical Engineering (JICTEE), 2014 4th Joint International Conference on* (pp. 1-5). IEEE.

[21]. Delei, J., Sen, B., & Wenming, D. (2008, December). "An image encryption algorithm based on knight's tour and slip encryption-filter". In *Computer Science and Software Engineering, 2008 International Conference on* (Vol. 1, pp. 251-255). IEEE.

[22]. Delfs, H., & Knebl, H. (2007). "Symmetric-key encryption". In *Introduction to Cryptography* (pp. 11-31). Springer, Berlin, Heidelberg.

[23]. Devi, M. U., Preeti, M., & Rani, M. N. (2017). "Network Security using Cryptography".

[24]. Diffie, W., & Hellman, M. (1976). “New directions in cryptography”. *IEEE transactions on Information Theory*, *22*(6), 644-654.

[25]. Diffie, W., & Hellman, M. E. (1976, June). “Multiuser cryptographic techniques”. In *Proceedings of the June 7-10, 1976, national computer conference and exposition* (pp. 109-112). ACM.