Image Encryption Technique based on the Entropy Value of a Random Block

Dr. Mohammed A. F. Al-Husainy
Department of Computer Science
Faculty of Information Technology,
Middle East University
Amman, Jordan

Dr. Diaa Mohammed Uliyan
Department of Computer Science
Faculty of Information Technology,
Middle East University
Amman, Jordan

***Abstract*—The use of digital images in most fields of information technology systems makes these images usually contain confidential information. When these images transmitted via the Internet especially in the Cloud, it becomes necessary to protect these images in a way that ensure putting the confidential information that are contained far away from the attackers. A proposed image encryption technique has been presented in this work. This technique used a secret key that is extracted from the image content itself. Therefore, there is no need to find a secret channel to exchange any key where, sender and receiver authenticate each other with regards to a shared secret key extracted from the image. The technique constructs its secret key that is used to encrypt the image, based on the entropy values of a set of randomly selected blocks from the image itself. Vairous experiments have been conducted to evaluate the strength and performance of the technique. The experimental results shows that the proposed technique can be used effectively in the field of image security to protect and authenticate images.**

Keywords—Image security; image encryption; secret key; image authentication

I. INTRODUCTION

With the rapid expansion of modern network technology such as Cloud computing, many of current applications such as Facebook employed cloud storage services to store multimedia data (e.g., Images and videos). Due to the fact, that images may contain private information that may be related to personal interests or financial affairs, the deliberate disclosure of confidential content becomes a critical issue for people and organizations [1]-[4].

Images need to be accessed and shared over the cloud securely. Image encryption is an efficient mechanism to contribute security for these images. Encrypting image is defined as protecting visual image through the Internet from hacker attacks [5]. In recent years, various image encryption algorithms have been proposed using cryptographic techniques by modifying their pixel values or locations [6]-[8]. Cryptographic techniques are categorized into symmetric and asymmetric encryption. Symmetric key encryption algorithm [9] uses one key for encrypting and decrypting image respectively. Obviously, it requires keeping the key secret. If the hacker knows the key, image decryption can be done easily. In contrast, asymmetric key encryption algorithm [10] employed two keys: public and private key. Recent studies mentioned that asymmetric key encryption is slower than symmetric key encryption algorithms [11]. Furthermore, asymmetric encryption algorithm has higher computational complexity which, are most of the time prohibitive for images and mathematical correlation between public and private keys may help attackers to hack the image [12]. This might be solved by using secret keys for image encryption or longer sized keys which are difficult to violate by attackers.

Due to digital images have intrinsic characteristics such as redundancy of data, less sensitive, a correlation between pixels and data capacity, it is difficult to handle these issues by using asymmetric cryptographic techniques [13]. They are not suitable for image encryption, while symmetric key image cryptograpphic algorithms appears to be a promising direction which takes profit from these characteristics to encrypt images [14].

The proposed method assumes that image is encrypted at rest with some secret key which, is not available to the attacker. To achieve this issue, the proposed method is developed based on entropy values of the image itself as secret key. The secret key will differ from one image to another. The fact that the attacker may have the historical secret key no longer matters because all the old keys are meaningless. The proposed method has the ability to resolve security problems caused by large data capacity and high correlation among pixels for color image encryption.

The rest of this paper is organized as follows: Related Works will be covered in Section 2. Section 3 describes the Proposed algorithm in detail. Section 4 presents Experimental results and performance analysis. In Section 5, Conclusions are drawn.

II. RELATED WORKS

The main goal of image encryption techniques is to convert source images into limited formats such as texture based or noise based format encrypted images. The pixel values of encrypted images have been changed to prduce a noise image, which arise the information leakage of image content and hide the visual meaning of these images over the cloud. From the security viewpoint, texture based or noise based format pixel features in the encrypted images would efficiently decrease the risk of an encrypted image being attacked and altered. This interesting issue motivates us to present a novel image encryption technique based on entropy features as secret keys

for transforming image into a nearly uniform distributed pixel values in the image to achieve privacy and confidentiality [15].

In recent years, image encryption techniques have been proposed to provide privacy preserving for digital images stored in cloud storage. Image encryption has become the hot topic of exhaustive research as its potential to transmit images more securely. Image encryption techniques can be categorized into: 1) Frequency based image encryption and 2) Spatial based image encryption. Hence, using secret key, the frequency based image encryption algorithms are developed to transform image content in the frequency domain such as the Discrete Cosine Transform (DCT) [16], Discrete fractional Fourier Transform (DFFRT) [17], [18], Quantum Fourier Transform (QFT) [19], Fresnel transform [20], Hartley Transform [21] and Gyrator Transform [22].

The spatial based image encryption techniques are based on two common operations: Substitution and Permutation, where substitution is used to change pixel values and a permutation process is used to shuffle pixel positions in the image. The permutation and substitution processes can be used in spatial based image encryption algorithms like Data Encryption Standard (DES) [15], Advanced Encryption Standard (AES) [23], Rivest, Shamir and Adleman (RSA) [24], P-Fibonacci transform [25], wave transmission [26], elliptic curve ElGamal [27], gray code [28], random grids [29], Latin squares [30] and chaotic mapping [31].

In the first category, the digital image is divided into blocks and transformed into the frequency domain to extract features. These features are disordered to make the original image is invisible. For instance, Phalavan et al. [16] proposed an image encryption method based on DCT coefficients, where the image is divided into 8×8 blocks and then extract high frequency DCT coefficients from these blocks. The main advantage of high frequencies DCT is representing more details in the image content. The secret key for their technique is generated based on cellular automata. Finally, the image blocks were encrypted using a secret key with XOR operation to disorder the values in each block.

Guo et al. [17] used Double Random Phased Encryption technique (DRPE) to encrypt the image where, binary image is used as secret key. Their method is robust of noise addition and the errors in the secret keys, which employed through decryption steps. Similarly, Lima et al. [18] divided grayscale image into blocks with size 8×8 pixels. The image blocks were encrypted with a secret key based on Galois Field Fractional Fourier Transform (GFFFT). The size of secret key is 140-bit, which makes their method has a large key space resist a brute force attack.

In [19], quantum gray level image representation and image encryption is proposed based on QFT. The correlation between adjacent pixels in the encrypted image and its original image is computed. Their method gives high level of security, where random relation exists in the encrypted image.

Singh et al. [20] proposed a scheme that transform an image into complex image subjected to Fresnel transform to extract frequency coefficients. The Devil's vortex toroidal lens phase mask is applied in the frequency domain to produce an encrypted image. The mean square error is computed for their method to show the robustness of encryption algorithm against Gaussian and speckle noise.

Lin et al. [21] proposed to use image scrambling in frequency domain based on Hartley transform. The input image is converted into Arnold cat map space plane and then, it is divided the image into 3×3 blocks. Later, blocks are encoded by H matrix of Heatley transform.

Liu et al. [22] proposed to use an iterative image encryption structure, in which Henon mapping is applied for the input image. Then, mapped image is transformed through gyrator transform to encode the image.

In the second category, Yun-Peng et al. [15] proposed a conventional encryption technique by combining DES algorithm with chaotic sequence to encode the image. The key size for encryption method is 264 bits, which is much larger than the traditional DES algorithm to resist against brute force attacks.

In [23], an image encryption algorithm with a framework of combining diffusion and permutation is proposed. The input image is divided into blocks with size 8×8 pixels. Each block is encoded based on pseudo random numbers which extracted from spatiotemporal chaos. Finally, the permutation of each block is computed using AES. Their method achieved a high speed by avoiding some time consuming operations.

Zhao et al. [24] used RSA encryption algorithm to scramble grayscale image. This algorithm is limited and not suitable for practical images due to large number of permutation rounds. It may not be the most desirable algorithms for digital image encryption, especially for real time systems.

Zhou et al. [25] introduced a new method for encrypting images by combining bit plane decomposition and image permutation. They used Fibonacci P-code transformation to scramble image. Their method is robust to various common attacks like noise, data loss, brute force and plaintext attacks.

Chen et al. [31] developed an encryption method based on Henon chaotic function and Logistic map for encrypting image and the secret key respectively.

Both the frequency based and spatial based image encryption techniques have the ability to increase the level of security to protect images. They are evaluated based on four factors: Security, Speed, Key space analysis and Correlation.

III. PROPOSED MODEL

One most concern of the proposed method is how to generate a secret key from the image properties itself. The image is encrypted and shared through some secret means between sender and receiver. So, the attacker struggles to know the secret key unless he has the same image and the algorithm used for the decryption of the image. The strength of the proposed method comes from the key where it is not dependent on algorithm steps being secret. This leads that, it is difficult to obtain the secret key value out of the possible key space. Therefore, a set of main objectives has been established to be

achieved within the proposed technique :

A. No need to exchange any secret key via a secure channel between sender and receiver.

B. A secret key used in encryption operation is extracted from the image itself.

C. The size of the secret key varied based on the nature of the image.

D. Trying to use a secret key that contains as more as possible of random values.

E. Apply substitution and transposition operations on the image within two different levels of implementation (on block of bytes and on a single byte).

The main stages that the proposed image encryption technique involves are depicted in Fig. 1.

To give readers a clear understanding of the implementation details of each stage of the proposed technique, we give below some necessary definitions and terminologies:

1) ***Source Image (I)*** is a bitmap color image of size (Width×Height×Palette). Where: Width is the width of the image, Height is the height of the image and Palette equal 3 which represents the three colors (R: Red, G: Green and B: Blue).

2) ***Encrypted Image (E)*** is a bitmap color image of size (Width×Height×Palette). Where: Width is the width of the image, Height is the height of the image and Palette equal 3 which represents the three colors (R: Red, G: Green and B: Blue). The image (E) is produced from the technique after encrypting the source image I.

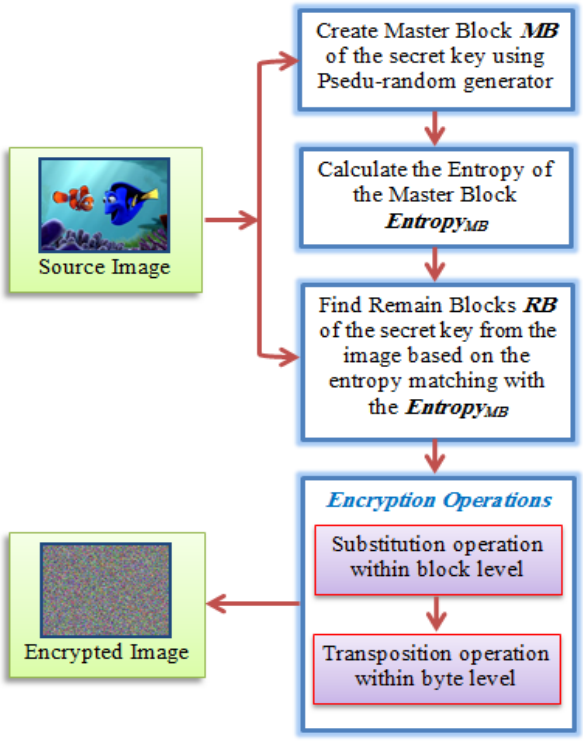

Fig. 1. Stages of the proposed image encryption technique.

3) ***Secret Key (K)*** Consists of a set of 2D blocks, it is divided into two parts: Master Block MB and the Remaining Blocks RB. All blocks are of the same size. The size of each block (i.e., number of rows and columns) is based on the image size and is calculated using the equations (1) and (2).

$$\text{NumberOfRows (R)} = \text{MaxDigitOf(Height)} \quad (1)$$

$$\text{NumberOfColumns (C)} = \text{MaxDigitOf(Width)} \quad (2)$$

4) ***Entropy*** is simply the average (expected) amount of the information from the data [32]. Information entropy is an important feature of randomness. Here, the entropy value is calculated by the equation (3).

$$\text{Entropy} = -\sum_{i=1}^{n} p_i \log_2(p_i) \quad (3)$$

Where n = number of different data values, pi is probability of occurring the data value i.

The main stages that follow in the encryption phase of the proposed image encryption technique are given below:

Stage 1: From the source image size (i.e., its Width and Height), calculate the dimensions of the secret key blocks (R and C) using the equations (1) and (2).

Stage 2: Build the Master Block MB of the secret key K by using a pseudo random generator with a seed value $(R \times C)$. Random values of bytes are filled in MB. The value of each byte is between $(0 \ldots 255)$. This part of the secret key K (i.e., MB) will be used later to construct the second part of the secret key K (i.e., RB). An example of the MB is shown in Fig. 2.

Stage 3: Calculate the entropy value of the MB EntropyMB using the equation (3).

Stage 4: Represent the bytes of the source image I bytes as a set of blocks of dimensions (R×C). The number of blocks in the source image I is calculated using the equation (4).

$$\text{NoOfBlocks} = (\text{Width x Height x Palette})/(\text{R x C}) \quad (4)$$

Stage 5: Search in the source image blocks that are created in Stage 4 to find all the blocks that have entropy values equal to the entropy value EntropyMB. These blocks are represented the remaining blocks RB of the secret key as shown in Fig.3. The number of remaining blocks RB found depends mainly on the image data. And these blocks are excluded from the implementation of the encryption operations that are applied in the next stages. The second part of the secret key K becomes ready to be used in the implementation of the encryption operations on the source image blocks.

C	0	1	2	3
R				
0	14	206	120	37
1	211	30	75	149
2	20	0	55	234

Fig. 2. Content of master block.

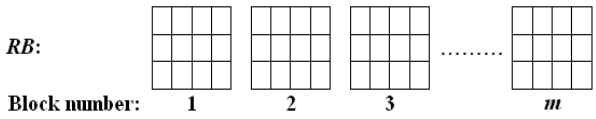

Fig. 3. Remaining blocks in the image.

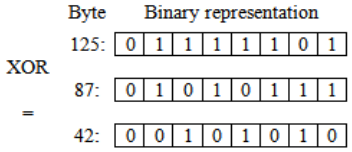

Fig. 4. XOR operation between blocks.

Stage 6: Perform the substitution operation of the encryption technique by doing the XOR logic operation between each block of the image with the one of the blocks in the RB set of blocks sequentially. When reach the block index m in the RB set of blocks, the next block index is 1. Example of XOR operation between two byte values is shown in Fig. 4 above.

Stage 7: Perform the transposition operation of the encryption technique by doing the randomly change the locations of all the bytes of the image including the bytes of the RM blocks. By using a pseudo random generator with a seed value (R×C), a new random location for each byte in the image be found.

Stage 8: Construct the encrypted image E from the collection of bytes that are produced in the Stage 7. As a result, the encrypted image is produced.

The same scenario has been implemented in the decryption phase to recover the original image from the encrypted one E, except the receiver should perform the transposition operation first.

In the proposed image encryption technique, we can note that there is no need to exchange any key between sender and receiver. The key size used (i.e., number of RM blocks used) and the values of bytes in each block vary based on the image data itself. This makes the technique easy to use by the users and more difficult against the attackers. Furthermore, the proposed method leads to the uniformization of the histogram of the encrypted images, which makes it more secure against statistical hacks as shown in Section 4.

IV. Experimental Results and Discussions

In order to evaluate the performance of the proposed technique, the necessary programming codes using C# language are written. Different images used in the experiments to test the technique. Some of these images are listed in Fig. 5.

Fig. 5. Some of the images use in the experiments.

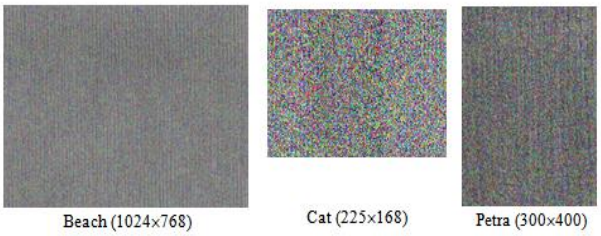

Fig. 6. The encrypted image from the images in Fig. 5.

The encrypted images that are produced from the source images in figure 1 are depicted in Fig. 6.

To make a performance comparison between the proposed image encryption technique and the well-known encryption techniques such as Data Encryption Standard (DES) [15] and Advanced Encryption Standard (AES) [23]. A set of measures (visually and numerically) has been used: Image histogram, Peak Signal to Noise Ratio (PSNR), encryption time, the key size, the complexity of the key and the sensitivity of the key.

1) ***Image histogram:*** good image encryption technique is the one that is able to achieve a high distortion in the distribution of color values of the encrypted image compared with the distribution of color values of the source image. Fig. 7 shows the histogram of the source image (Beach) and its encrypted image using the proposed technique and the DES and AES techniques.

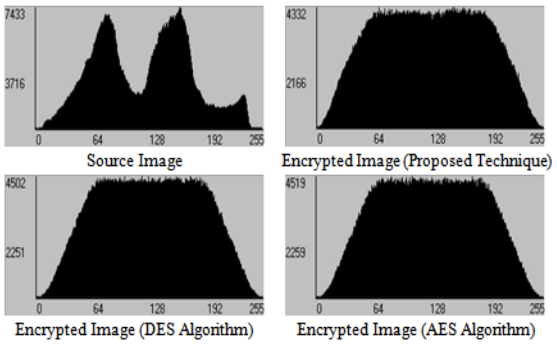

Fig. 7. Histogram of the source image and its encrypted images (Beach image in Fig. 5).

2) ***Peak Signal to Noise Ratio (PSNR):*** a numerical measure that is used to calculate the ratio of noise that is occurring in the encrypted image and it is caused by the implementation of the encryption technique on the source image. Good image encryption technique is the one that is producing high ratio of noise in the encrypted image with a low PSNR value [33], [34]. The PSNR is calculated using the equation (5) and (6), where MAX represents the maximum byte value in the image and I and E are the source image and the encrypted image respectively. Table 1 records the PSNR of the encrypted image in the proposed technique and DES and AES techniques.

$$NMAE = \frac{\sum_{k=0}^{(Width \times Hieght \times Palette)-1} |I(k)-E(k)|}{Width \times Hieght \times Palette} \times 100 \quad (5)$$

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{NMAE}\right) \quad (6)$$

3) ***Encryption time:*** the time needed to complete the encryption phase is one of the common factors that is used to evaluate the performance of the encryption technique. A good image encryption technique is the one that is conducting its encryption operations in a short time. Table 2 summarizes the encryption time of the proposed technique and DES and AES techniques.

TABLE. I. PSNR OF THE ENCRYPTED IMAGE

mage	Algorithm	PSNR (db)
Beach	**Proposed**	8.42
	DES	6.56
	AES	6.56
Cat	**Proposed**	8.25
	DES	7.38
	AES	7.37
Petra	**Proposed**	8.71
	DES	7.81
	AES	7.82

TABLE. II. ENCRYPTION TIME

Image	Algorithm	Time (sec)
Beach	**Proposed**	3.15
	DES	3.70
	AES	3.37
Cat	**Proposed**	0.17
	DES	0.16
	AES	0.18
Petra	**Proposed**	0.52
	DES	0.59
	AES	0.53

4) ***Key size:*** the encryption technique becomes strong whenever it can be used a proportionally large key. The key used in the proposed technique is actually large because it consists of a set of blocks (i.e., RB) and each block consists of a number of bytes. This makes the bits that represent the secret key used by the proposed technique is large. To illustrate this, we assume that the block dimension is (R=4 and C=4). This means that each block of the RB has 16 bytes. And if there are 5 blocks in RB, this means that the number of bits that represent the key is 640, where it calculated using the equation (7). While the DES algorithm uses a key contains 64 bits and the AES algorithm uses a key contains 128 to 256 bits.

$$\text{NumberOfBits} = \sum_{i=1}^{m}[(R \text{ x } C) \text{ x } 8] \quad (7)$$

5) ***Complexity of key:*** is the ratio of randomness and the composite use of the key in the implementation of the operations of the encryption technique. The proposed technique uses a key that is extracted from the image itself and it contains really random bytes. In addition, it uses key in two levels of implementation of the operations (block and byte level).

6) ***Sensitivity of key:*** it means that if we change only one bit in the key used, the technique produces, from the encrypted image, an image that is a completely different from the source image. This forces the attacker to know all the bits of the key to be able to recover the source image from the encrypted image. To prove that, in the proposed technique, we changed one bit in the key used to encrypt one of the images in Fig. 5 and try to decrypt the encrypted image. The produced image is completely different from the source image as shown in Fig. 8.

7) ***Correlation Analysis:*** is the value that depicts the relationship between the adjacent pixels values in the encrypted image. Whenever the correlation value is small this means that the encryption technique achieved high randomness between the adjacent pixels in the encrypted image. The calculated correlation values for the proposed technique and DES and AES techniques are listed in Table 3.

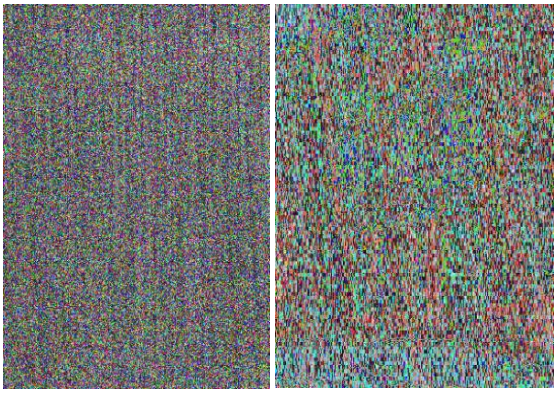

Fig. 8. The source image resulting from the encrypted image using the wrong key (Perta image in Fig. 5).

TABLE. III. CORRELATION BETWEEN ADJACENT PIXELS VALUES

Image	Algorithm	Correlation Value
Beach	Proposed	0.123
	DES	0.107
	AES	0.106
Cat	Proposed	0.120
	DES	0.089
	AES	0.089
Petra	Proposed	0.090
	DES	0.094
	AES	0.093

V. CONCLUSION

This paper introduced a novel image encryption scheme based on Entropy values of selected blocks and perform XOR permutation at the block level with the transposition operation at the byte level. The Entropy is computed from the selected block in the image whose size is based on the image size. The rest of blocks are selected which they have the same entropy to be as candidates used for generating large enough secret key space to encrypt the image later. High level of security is achieved by using a random secret key. This leads that different image should have a different random key for encryption. Experimental results show that the scrambled image has approximately uniform histogram pattern and can be considered as a nearly random image. The security analyses also demonstrate that the proposed method is sensitive to the nature of source image and the encryption key. Therefore, the proposed method has high security and can resist against most common attacks. However, we have found from the experimental results that the secret key values may be different from one image to another which adds more ambiguity at the side of attackers about the key itself. The future work is to investigate the common malicious attacks that can be applied to images such as copy move forgery and image splicing in the field of image forensics.

ACKNOWLEDGMENT

The authors are grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

REFERENCES

[1] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," Information Sciences, vol. 273, pp. 329-351, 2014.

[2] D. M. Uliyan, H. A. Jalab, and A. W. A. Wahab, "Copy move image forgery detection using Hessian and center symmetric local binary pattern," in Open Systems (ICOS), 2015 IEEE Confernece on, 2015, pp. 7-11.

[3] D. M. Uliyan, H. A. Jalab, A. W. Abdul Wahab, and S. Sadeghi, "Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points," Symmetry, vol. 8, p. 62, 2016.

[4] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, P. Shivakumara, and S. Sadeghi, "A novel forged blurred region detection system for image forensic applications," Expert Systems with Applications, vol. 64, pp. 1-10, 2016.

[5] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2594-2608, 2016.

[6] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," Journal of Electrical and Computer Engineering, vol. 2012, p. 7, 2012.

[7] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Optics & Laser Technology, vol. 57, pp. 327-342, 2014.

[8] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "2D Sine Logistic modulation map for image encryption," Information Sciences, vol. 297, pp. 80-94, 2015.

[9] S. Sowmya and S. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF (p)," in Contemporary Computing and Informatics (IC3I), 2014 International Conference on, 2014, pp. 1345-1350.

[10] W. Liu, Z. Xie, Z. Liu, Y. Zhang, and S. Liu, "Multiple-image encryption based on optical asymmetric key cryptosystem," Optics Communications, vol. 335, pp. 205-211, 2015.

[11] J. J. Amador and R. W. Green, "Symmetric-key block cipher for image and text cryptography," International Journal of Imaging Systems and Technology, vol. 15, pp. 178-188, 2005.

[12] H. Rifa-Pous and J. Herrera-Joancomartí, "Computational and energy costs of cryptographic algorithms on handheld devices," Future internet, vol. 3, pp. 31-48, 2011.

[13] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm", Applied soft computing, vol. 11, pp. 514-522, 2011.

[14] M. Saikia and B. Baruah, "Chaotic Map Based Image Encryption in Spatial Domain: A Brief Survey," in Proceedings of the First International Conference on Intelligent Computing and Communication, 2017, pp. 569-579.

[15] Z. Yun-Peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Wei-di, "Digital image encryption algorithm based on chaos and improved DES," in Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, 2009, pp. 474-479.

[16] A. Pahlavan Tafti and S. Janosepah, "Digital images encryption in frequency domain based on DCT and one dimensional cellular automata," Informatics Engineering and Information Science, pp. 421-427, 2011.

[17] C. Guo, S. Liu, and J. T. Sheridan, "Optical double image encryption employing a pseudo image technique in the Fourier domain," Optics Communications, vol. 321, pp. 61-72, 2014.

[18] J. B. Lima and L. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," Signal Processing, vol. 94, pp. 521-530, 2014.

[19] Y.-G. Yang, X. Jia, S.-J. Sun, and Q.-X. Pan, "Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding," Information Sciences, vol. 277, pp. 445-457, 2014.

[20] H. Singh, A. Yadav, S. Vashisth, and K. Singh, "Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain," International Journal of Optics, vol. 2015, 2015.

[21] K. T. Lin, "Image Encryption Using Arnold Transform Technique and Hartley Transform Domain," in Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on, 2013, pp. 84-87.

[22] Z. Liu, L. Xu, C. Lin, J. Dai, and S. Liu, "Image encryption scheme by using iterative random phase encoding in gyrator transform domains," Optics and Lasers in Engineering, vol. 49, pp. 542-546, 2011.

[23] S. H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," in Electronics and Information Engineering (ICEIE), 2010 International Conference On, 2010, pp. V1-141-V1-145.

[24] G. Zhao, X. Yang, B. Zhou, and W. Wei, "RSA-based digital image encryption algorithm in wireless sensor networks," in Signal Processing

Systems (ICSPS), 2010 2nd International Conference on, 2010, pp. V2-640-V2-643.

[25] Y. Zhou, K. Panetta, S. Agaian, and C. P. Chen, "Image encryption using P-Fibonacci transform and decomposition", Optics Communications, vol. 285, pp. 594-608, 2012.

[26] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," Nonlinear Dynamics, vol. 78, pp. 995-1015, 2014.

[27] L. Li, A. A. A. El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," Signal Processing, vol. 92, pp. 1069-1078, 2012.

[28] J.-x. Chen, Z.-l. Zhu, C. Fu, H. Yu, and L.-b. Zhang, "An efficient image encryption scheme using gray code based permutation approach," Optics and Lasers in Engineering, vol. 67, pp. 191-204, 2015.

[29] S. J. Shyu, "Image encryption by random grids," Pattern Recognition, vol. 40, pp. 1014-1031, 2007.

[30] Y. Wu, Y. Zhou, J. P. Noonan, and S. Agaian, "Design of image cipher using latin squares," Information Sciences, vol. 264, pp. 317-339, 2014.

[31] C.-K. Chen, C.-L. Lin, C.-T. Chiang, and S.-L. Lin, "Personalized information encryption using ECG signals with chaotic functions," Information Sciences, vol. 193, pp. 125-140, 2012.

[32] H. Zhang, J. E. Fritts, and S. A. Goldman, "An entropy-based objective evaluation method for image segmentation," Storage and Retrieval Methods and Applications for Multimedia, vol. 5307, pp. 38-49, 2004.

[33] M. A. F. Al-Husainy, "A novel image encryption algorithm based on the extracted map of overlapping paths from the secret key," RAIRO-Theoretical Informatics and Applications, vol. 50, pp. 241-249, 2016.

[34] M. A. F. Al-Husainy, "Message segmentation to enhance the security of LSB image steganography," International Journal of Advanced Computer Science and Applications, vol. 3, pp. 57-62, 2012.