DOI: http://dx.doi.org/10.26483/ijarcs.v10i1.6350

Volume 10, No. 1, January-February 2019

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY OF THE MOST CURRENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES

Mohammad Ali Bani Younes
Dep. of Computer Science
Ajloun National University
Jordan

Abstract: Nowadays, the internet plays a key role in almost every aspect of life. This article presents a new set of data storage and protection challenges. It shows a general introduction to cryptography and discusses most of the available articles of image encryption techniques that increase the levels of data security. However, different encryption techniques can be used to protect the digital data confidentiality from unauthorized access. Furthermore, the cryptographic techniques discussed in this article can be used to support researchers to develop new techniques to provide high levels of security and thus reduce the risk of security. With the advancement of science and knowledge, the protection techniques lead to increase versatility and security of data transfer in the future.

Keywords: Asymmetric; Cryptanalysis; Cryptography; Image encryption

I. INTRODUCTION

Security is a basic requirement for all applications to protect data while stored and transmitted over open networks. Thus, this requirement is necessary to increase users' confidence in communication networks to complete their transactions securely. Digital images occupy a large part of our daily communications [20]. The enormous changes in technologies have resulted in an abundance of Portable Electronic Devices (PED) and advanced personal computers to be a tool of interpersonal.

Digital cameras, phones, and computers have made the process of capturing, processing and sharing images between interpersonal via instant and unrestricted communication extremely sensitive. The storage and the use of the images are stored and then used throughout various applications such as Twitter, Facebook, and WhatsApp. The fact that many areas such as the medical field and the military field carry sensitive digital images must be secured and protect against attacks in effective ways. Encryption of sensitive data is necessary, encryption algorithms designed to protect data and ensure confidentiality and the only authorized recipient can access the decryption data [10].

Encryption is a process to convert data in an unreadable format by unauthorized users using cryptographic algorithms to preserve data. It is used to keep sensitive data so that it can be difficult for unauthorized users to see it. The encryption process is used to save the sender messages via the vacuum or air. The good algorithms must have been tested to meet the requirements of the security which protect the encryption components [19].

II. CRYPTOGRAPHIC SYSTEMS

Encryption is used to convert data to secret codes while being transmitted over the public network. It allows the users to encrypt sensitive information to be stored safely or transmitted over the secure networks so that it cannot be read by anyone other than the intended recipient and encryption of the sensitive data is needed. So encryption is used to make information incomprehensible if unauthorized individuals intercept the transmission. The obvious form of information is called the original data, but the incomprehensible version is called a ciphertext [24, 25].

The process of converting the original text into a coded form is called encryption, while the process of returning the encrypted text is called the decryption.

In general, most cryptographic algorithms use a secret key. Encrypted data security depends completely on two things: the strength of the cipher algorithm and the secret key. The key is used in encryption and decryption and must be kept secret, requiring the sender and receiver to match on the same key before any data is sent. The key is independent of the plain text. Therefore, the same encrypted text encodes to different ciphertext with different keys, so both processes are impossible without using the correct key [8].

There is strong encryption and weak encryption. The strength of the encryption depends on the time and the tools that required returning the plain text. Strong encryption makes the ciphertext difficult to understand without a special tool to decrypt it. The sender and the recipient must maintain the confidentiality key between the two parties so that no one can decrypt the text without knowing the secret key [13].

While cryptography is the art of writing or solving codes, cryptanalysis is the science of analyzing and breaking protected communication, and therefore it is the process of recuperating the plaintext or key by using the ciphertext and information of the algorithm. Generally, there are two types of algorithms: symmetric that uses a single key for both encryption and decryption, and asymmetric that uses one key for encryption and another for decryption [1]. Thus, the strength of the algorithm used for encryption is very essential. Because the unauthorized entity can take the encrypted text and try to break the encryption by trying to select the secret key based on the encrypted text.

Encryption is used to ensure the path of communication through a) data integrity and non-modification during transmission; b) non-denial is achieved through digital signatures; c) authentication through authentication d) privacy

is the process of ensuring delivery of the intended object. In this section, two related categories of encryption schemes will be discussed: public key encryption and symmetric key encryption [15].

Asymmetric encryption is the public key used for encryption and decryption. The public key is known and distributed to all parties. The private key is difficult to understand to anyone except for the recipient. It is a pair of keys, one for encryption and another for decryption. This ensures the privacy of the message during transmission. There are two types of algorithms: Asymmetric that uses one encryption and decryption key, and the other is asymmetric that uses the cryptographic key for decryption [25].

A. Symmetric Key or Secret Key

In the secret key, the sender and the recipient of the message use the same key in the encryption process [15, 24]. The key remains secret between them to be used to decrypt the message. This encryption consists of five steps as shown in Figure 1 (Stallings, 2005).

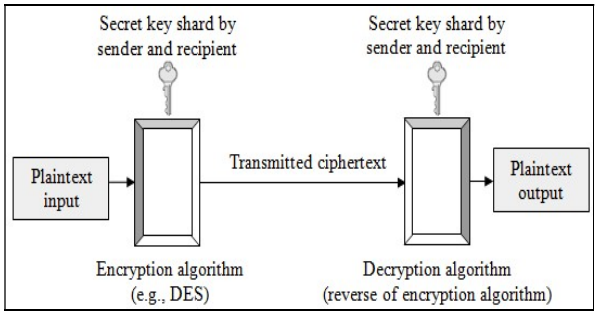

Figure1. A Simple Model of Symmetric Key Encryption (Stallings, 2005).

B. Asymmetric Key or Public Key

Asymmetric Key is called the public key that depends on the use of pairs of keys. The two keys are connected through a calculation using one-way functions to encode information. The public key is used for encryption and the other is the secret key used for decryption. The sender must distribute the public key broadly so that anyone can send messages. On the other hand, the key used for decryption must be confidential. Generally, users of this type of encryption publish their public keys on websites, blogs, and e-mail signatures [15, 24].

Figure 2. Shows the main components of a public key of the cryptography system.

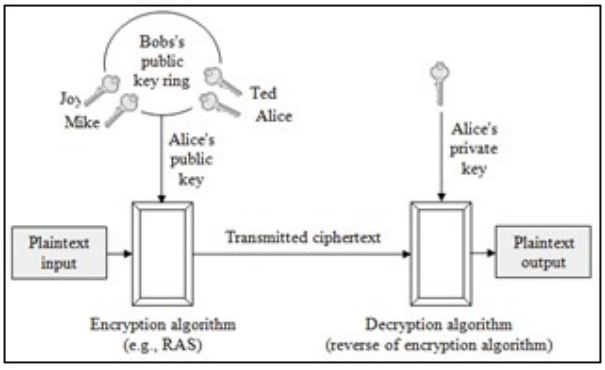

Figure 2. Public Key Encryption and Decryption Model (Stallings, 2005).

III. STEGANOGRAPHY TECHNIQUE FOR DIGITAL IMAGES

Steganography is the conceal of information inside other information so the encryption and steganography are complementary to the other. The goal of encryption is to protect the message from illegal access while hiding information inside other information is a technique to mask the message in a way that prevents anyone from detecting it. Therefore, masking technology allows the user to hide large amounts of information in an image [12; 14, 26].

The encryption problem is that the encrypted message is obvious. This makes it possible to deduce information from other parties. Thus, if the receptive information is transferred over an insecure channel such as the Internet, information hiding knowledge can be used to provide additional protection [15]. In addition, to improve the security of the encrypted image, the method of hiding information can also be used to exchange confidential information between the sender and the recipient. This method successfully masks the data in the encrypted image without affecting image quality and reduces the chance of revealing the encrypted image [12, 14, 26].

IV. ENCRYPT IMAGES

Digital images consist of pixels that have a value since the pixel set is a bitmap (BMP). Digital images contain sensitive information from individuals, government sectors, and businesses as they are sent across the web or networks. They must be stored and protected during transport using secure algorithms [15]. The traditional ways to protect digital images from illegal eavesdropping is to encrypt and hide information and watermark. These methods provide high levels of security, however, each type of data has its own advantages, so different techniques must be used to protect confidential image data from unauthorized access. Most cryptographic algorithms use text and may not be suitable for multimedia such as images [6]. Encryption algorithms for image encryption can be derived from two things: First, the ratio, the size of the image and the text size, image data. Second, is the image that contains some natural properties that are not contained in the text data holding the same encryption procedure.

Digital images demonstrate characteristics such as high repetition and the high correlation between pixels and they are huge in size. On the other hand, an image with a great deal of contrast from one pixel to the next has high entropy. Image encryption deals with a set of technologies that transform images into incomprehensible and unreadable formats so that only the licensed recipient can reconstruct the image and obtain the information. The following objectives are required to ensure the security and integrity of information: confidentiality, integrity, availability, and non-repudiation [10].

V. BLOCK AND STREAM CIPHERS

Block and stream ciphers are two groups of symmetric ciphers that used in cryptography. A block cipher is a manner of symmetric key cipher algorithm. It splits the plaintext into blocks, normally of fixed size, and the symmetric key algorithm operates on each block separately. This means that it is a method of encrypting one block of data simultaneously using the same key on each block.

A block of plaintext will always encrypt to the same block of ciphertext if the same algorithm and key are used. A block cipher consists of two algorithms, one for encryption and another for decryption. When encrypting, a block cipher takes

a 64-bit block of plaintext as input and the outputs is a corresponding 64-bit block of ciphertext. This process is achieved by using the secret key. The block cipher algorithms can operate in many forms. The commonly used modes are the Electronic Code Book Cipher (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB). ECB cipher encrypts each block independently [8].

VI. ESSENTIAL ENCRYPTION TERMS

Plaintext: It is the message that anyone can read.
Encryption: It is the message that is converted from a text that is read to encrypted text.
Decryption: It is the message that is decrypted and converted to the original text.
Encryption Algorithms: The encryption and decryption rules that are used to encrypt the plaintext and decrypt the ciphertext such as Triple DES, RC6, MARS, and RSA encryption [15, 24].
Digital Signature: It is to prove who writes the document and ensures that the information in this document is not subject to any changes.
Hash: Hashing is an encryption method that transforms any form of data into a unique string of text. Any part of the data can be hashed, regardless of size or type. In traditional hashing, regardless of size, type, or length of data, the hashing produced by any data is always the same length. A hash is designed to act as a one-way function - you can place data in the hash algorithm to get a unique string, but if you have a new hash, you cannot decrypt the entered data that you represent. Unique data always produces the same hash.
Image Correlation: It is a statistical measure of security that expresses a degree of relationship between two variables is a correlation among image elements.
Image Similarity: Estimating the degree of similarity between images based on specific measurements.
Image Entropy: The information in the image is determined by measuring the entropy of the image
Image Histogram: It is the way that the image is analyzed and extracted its information.
Communication channel: It means the use to share information.
Sender: The person who sends the information.
Receiver: The person who receives the information.
Key: The key is a changeable value used with the algorithm to produce encrypted text, or to decrypt encrypted text. It has a length that limits the difficulty of decoding the text in a particular message [6].

VII. A SURVEY ON THE CURRENT RESEARCH IN IMAGE ENCRYPTION

In general, digital image encryption is still an open area for research and a very important area of information security. Digital image encryption has become the most effective way in communication systems. It puts the higher requirements to the technology of encryption and decryption of information in the modern networks in order to ensure security and high efficiency. At the same time, internet multimedia applications have become very popular, thus, multimedia data such as digital images are vulnerable to unauthorized access either in storage or during transmission over a network. Furthermore, streaming digital images requires high network bandwidth for transmission.

The following subsections highlight the current major research in digital image encryption.

A. Use of Symmetric Algorithm for Image Encryption

Brindha, et al. (2014) have indicated the use of a symmetric algorithm to encrypt images. They presented image encryption using a symmetric algorithm (SA). The decryption keys were used to obtain the original digital data again from the encrypted data model sent. They have encrypted images using the DES algorithm, which provides more security during transmission. They used three main steps: First, converting an image into a byte array and a byte array into a string, and the string passed for encryption in DES. In addition, this article presented an analysis of the DES algorithm for image encoding. The proposed idea reproduced the original image without loss of information. A comparative study of the DES algorithm was executed with the current image encoding algorithms in this paper.

B. An Ethical Approach of Block-Based Image Encryption Using Chaotic Map

Gupta et al. (2015) have introduced an image encryption algorithm using chaos mapping. This work showed that the algorithm can hide the original image through simple permutation of the location of the pixels as well as the conversion of the gray scale value through Boolean XOR operation. To make the cipher more strongly against any attack, the secret key is exchanged after encrypting a block of the image. They have carried out statistical analysis, key sensitivity analysis, key space analysis, and entropy test analysis to demonstrate the security of the new image encryption procedure. Finally, this work expected to be useful for real-time image encryption and transmission applications.

C. Image Encryption Algorithm Based on Chaotic Economic Model

Askar et al. (2015) introduced a new algorithm to encrypt and decrypt images based on a chaotic map. This work was the first attempt to implement a chaotic economic map in the construction of chaotic encryption. All the simulation and experimental results showed that the proposed image encryption and decryption algorithm has a very large keyspace, a high sensitivity of the all secret keys, information entropy close to the ideal value 8, and low correlation coefficients close to 0. Thus, these results led to the effectiveness of the proposed image algorithm. In addition, the results suggested the application of the other known chaotic economic systems such as duopoly and tripoly economic systems.

D. A Fast Encryption Algorithm of Color Image Based on Four-Dimensional Chaotic System

Tong et al. (2015) have proposed a fast encryption algorithm of the color image based on a four-dimensional chaotic system. Firstly, they proposed a new method of designing a four-dimensional chaotic system based on the classical equations of a three-dimensional chaotic system, to increase the complexity and key space of the encryption algorithm. Secondly, according to the nature of color images' pixels channel, they design a new pseudo-random sequence generator and reuse the random sequence, to improve the speed of image encryption. Finally, the methods of row-major and column-major were used to diffuse the original image and the cat map with parameter was used to scramble the image pixels, respectively, to achieve the effect of encryption.

E. *A Fast Image Encryption Algorithm Based on Convolution Operation*

Zhang (2017) presented a new image encryption algorithm based on convolution operation. By using an external key of length 300 bits, several pseudo-random sequences were generated by Chen's chaotic system and general convolution operation, and then the statistical properties were verified. The proposed image encryption scheme includes one module of covering operation, two modules of diffusion operations, and one module of confusion operation. The covering module employs the pseudo-random sequence to cover the original plain image with a binary XOR operation.The propagation units are based on the multiplication of the finite field GF 28 and the window coils with a combination of 256, and to spreading information from any pixel in the original image to all pixels in the spread image. The unit of confusion uses each value of a pseudo-random sequence as the displacement offset to replace the pixel to neutralize the diffuse image. The simulation and comparative analysis experience show that the proposed image encryption system has the advantages of fast processing speed, strong sensitivity and high encryption density, can be used as a candidate for the practical image encryption system.

F. *A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation and Bit-Level Permutation*

Li et al. (2017) proposed a number of chaotic images-coding algorithms that use the anarchist map of lower dimensions and the structure of diffusion propagation. However, the low-dimensional anarchist map is less secure than the high-dimensional chaos system. In addition, the flipping process is independent of the plaintext and diffusion process. Therefore, they cannot effectively resist the chosen attack of plain text and the chosen attack of encrypted text. In this work, they proposed a cryptographic algorithm based on chaos. The algorithm adopts a 5-D messy system, and the key flow of the chaotic system is associated with the original image. Then, pixel-level flipping and bit-level flipping were used to enhance the security of the encryption system. Finally, a post was used to change the pixels. Theoretical analysis and numerical simulation show that the proposed algorithm is safe and reliable for image encryption.

G. *An Image Encryption Scheme Based on Chaotic Tent Map*

Li et al. (2017) have proposed an image encryption system based on the anarchist paranormal map. This paper proposes a new image encryption system, based on the chaotic map of tents. Image encryption systems based on this map show some better offers. First, the chaotic map of Khawarish has been modified to produce a more chaotic and appropriate picture-encoded image. Second, the chaos-based keystream is generated by a 1-D map, which has a better performance in terms of randomization characteristics and safety. The performance and security analysis of the image encryption scheme was performed using known methods. The results of the safe analysis of the failure are inspirational, and it can be concluded that the proposed scheme is effective and safe.

H. *A Comprehensive Study of Image Steganography Techniques*

Ali and Jawad (2017) have presented a comprehensive study of Image Steganography Techniques. Therefore, several methods are developed to protect important information for safe and secure communication. There are three main technologies used for securing digital data: watermarking, steganography and cryptography. Steganography and watermarking could be considered within the same field (information hiding). This paper presented a comprehensive study of various methodologies in the field of image steganography. Each methodology has its bad and good points, therefore, a part of advantages and drawbacks are discussed as a comparative study to help future researchers by providing a review of the existing techniques.

I. *Steganography Using AES and LSB Techniques*

Pandey and Chopra (2017) have proposed a novel method hide secret information in a combination of AES and LSB technique. The image quality is selected by the users and based on that the length of the secret message is decided. Hence user has full right to select any size of the output based on requirements. The framework provides an effective way to select output image toad to accommodate the secret information. The receiver needs to have a secret key which will be used to decode the secret message.

J. *Image Encryption Techniques Using Fractal Function: A Review*

Agarwal (2017) proposed an image encryption algorithm based on chaotic maps. Properties of Arnold's cat map were employed for creating a relationship between used key and plaintext in form of image pixel amplitudes. This correspondence seems crucial for establishing a certain level of robustness against a class of chosen-plaintext attacks which could create a list of dependencies between encrypted and plaintext image. Effects of presented algorithms were verified by a series of experiments. Their numeric results were compared with values yielded by approaches which used the same plaintext image. Processing speeds were calculated for algorithms which provided sufficient information about used images. The main advantage of the proposal is its simplicity which enables fast processing speed. Also, the correlation coefficients of adjacent encrypted pixels are in case of the presented image better than those achieved by other algorithms. However, these solutions provided higher values of NPCR. Future work can be done on the key diffusion algorithm, which currently restrains the length of entered diffusion key to 8 bytes.

K. *A New Hyperchaotic Map and Its Application for Image Encryption*

Natiq et al. (2018) have proposed a new 2D chaotic model, 2D-SHAM, derived from the H´enon and Sine maps. Basic dynamic properties, including equilibria, Jacobin eigenvalues, trajectory, bifurcation diagram, LE and sensitivity dependence test were studied to show that 2D-SHAM is overall hyperchaotic and high sensitivity to its initial values and control parameters. Furthermore, the Sample Entropy algorithm was used to investigate its complexity. Using 2D-SHAM, a new image encryption algorithm has been proposed. This algorithm achieved the essential requirements of confusion and diffusion. Moreover, the stochastic 2D-SHAM was used to enhance the security of the encrypted image. Experimental results indicate that SHAM-IEA can encrypt digital images with high complexity performance, low implementation cost, and with strong capability to withstand different attacks.

L. *Comprehensive Survey on Image Steganography Using LSB With AES*

Agrahari et al. (2018) have suggested a way to conceal unknown data in a mix of AES and LSB system. The picture quality is chosen by the clients and in light of that, the mystery

messages length are chosen. Consequently, the client has full appropriate to choose any size yield in light of necessities. The study has been done to identify with cryptography and steganography that guarantees security; however, it needs some alternative methods to proves security standards. It also shows various strategy employed for the least significant bit depending upon the efficiency as well as encryption standards used.

M. Asymmetric Image Encryption Approach with Plaintext-Related Diffusion

Oravec et al. (2018) have introduced an Asymmetric Image Encryption Approach with Plaintext-Related Diffusion. This paper proposed an image encryption algorithm based on chaotic maps. Properties of Arnold's cat map were employed for creating a relationship between used key and plaintext in form of image pixel amplitudes. This correspondence seems crucial for establishing a certain level of robustness against a class of chosen-plaintext attacks which could create a list of dependencies between encrypted and plaintext image. Effects of presented algorithms were verified by a series of experiments. Their numeric results were compared with values yielded by approaches which used the same plaintext image. Processing speeds were calculated for algorithms which provided sufficient information about used images. The main advantage of our proposal is its simplicity which enables fast processing speed. Also, the correlation coefficients of adjacent encrypted pixels are in case of the presented image better than those achieved by other algorithms. However, these solutions provided higher values of NPCR. Future work can be done on the key diffusion algorithm, which currently restrains the length of entered diffusion key to 8 bytes.

N. Color and Gray Images Encryption Algorithm Using Chaotic Systems of Different Dimensions

Lagmiri et al. (2018) have recommended an algorithm for color image and gray image encryption was designed utilizing the proposed chaotic and hyperchaotic systems. This work deals with the encryption of color and gray images using chaotic systems of different dimensions. The proposed chaotic systems show excellent chaotic behaviors. To demonstrate its application in image processing, the two systems were applied with an algorithm based on key generation based on initial conditions for encryption and decryption. The simulations results and security analysis demonstrate that the proposed systems have excellent encryption performance, high sensitivity to the security keys.

VIII. CONCLUSION

Information security is a shared responsibility that is signification to ensure the authenticity of information shared across the web from unauthorized access. In this article, different types of encryption were presented and several techniques were reviewed. These techniques encourage researchers to develop new cryptography techniques in order to provide high levels of data security and protection.

IX. ACKNOWLEDGMENT

I would like to thank all the staff of the International Journal of Advanced Research in Computer Science, and I thank Ajloun National University for encouraging research in all fields, leading to building a knowledge society, promoting scientific research.

X. REFERENCES

[1] M. AbuTaha, M. Farajallah, R. Tahboub,and M. Odeh, "Survey Paper: Cryptography Is The Science Of Information Security," International Journal of Computer Science and Security (IJCSS), vol. 5(3), 2011, pp.298-309.

[2] S. Agarwal, "Image Encryption Techniques Using Fractal Function: A Review," International Journal of Computer Science & Information Technology (IJCSIT), vol. 9(2), April. 2017, pp.53-68.

[3] A. K. Agrahari, M. Sheth, and N. Praveen, "Comprehensive Survey on Image Steganography Using LSB With AES," International Journal of Applied Engineering Research, vol. 139(8), 2018, pp. 5841-5844.

[4] T. A. Israa and J. Shaymaa, "A Comprehensive Study of Image Steganography Techniques," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Web Site: www.ijettcs.org, September-October. 2017, vol. 6(5), pp. 101-104.

[5] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image Encryption Algorithm Based on Chaotic Economic Model," Mathematical Problems in Engineering, Volume 2015, Article ID 341729, pp. 1-10.

[6] M. A. Bani Younes, and A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm: Image Encryption and Decryption Process Using Block-Based Transformation Algorithm," New York: LAP Lambert Academic Publishing, Germany, 2011.

[7] M. A. Bani Younes, and A. Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption," IJCSNS International Journal of Computer Science and Network Security, vol. 8(4), 2008, pp.191-197.

[8] M. Barakat, C. Eder, and T. Hanke, "An Introduction to Cryptography," Timo Hanke at RWTH Aachen University, 2018, pp. 1-145.

[9] K. Brindha, R. Sharma, and S. Saini, "Use of Symmetric Algorithm for Image Encryption," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2(5), May 2014, pp. 4401- 4407.

[10] S. Geetha, P. Punithavathi, A.M. Infanteena, and S.S.S. Sindhu, "A Literature Review on Image Encryption Techniques ," International Journal of Information Security and Privacy (IJISP), 12(3), 2018, pp.42-83.

[11] K Gupta, R. Gupta,, R., and S Khan, "An Ethical Approach of Block-Based Image Encryption Using Chaotic Map," International Journal of Security and Its Applications, vol. 9(9), 2015, PP.105-122.

[12] M. Jain, and S. K. Lenka, "A review of digital image steganography using LSB and LSB array," International Journal of Applied Engineering Research, vol. 11(3), 2016, pp. 1820–1824.

[13] MR. Joshi, and RA. Karkade. "Network Security with Cryptography," International Journal of Computer Science and Mobile Computing, vol. 4(1), Jan. 2015, PP. 201-204.

[14] M. Cem kasapbas and W. Elmasry, "New LSB-based color image steganography method to enhance the efficiency in payload capacity, security and integrity check," Sadhana, Indian Academy of Sciences, April 2018, 43: 68, pp.1-14.

[15] S. Kumari, "A research Paper on Cryptography Encryption and Compression Techniques," International Journal Of Engineering And Computer Science, 2017, vol. 6(4), pp. 20915-20919.

[16] S. N. Lagmiri, N. Elalami, and J. Elalami, " Color and gray images encryption algorithm using chaotic systems of different dimensions," IJCSNS International Journal of Computer Science and Network Security, 2018, 18(1), pp. 79-86.

[17] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dynamics, 87(1), 2017, PP. 127-133.

[18] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Optics and Lasers in Engineering, vol. 90, 2017, PP. 238-246.

[19] A. Mitra, Y. V. Subba Rao, and S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques," International Journal of Electrical and Computer Engineering, vol. 1(2), May.2006, pp. 127-131.

[20] M. F. Mushtaq, S. Jamel, A. H. Disina, Z.A. Pindar, N.S.A. Shakir, and M.M. Deris, "A Survey on the Cryptographic Encryption Algorithms," (IJACSA) International Journal of Advanced Computer Science and Applications, 2017, 8(11), pp. 333-344.

[21] H., Natiq, N. M. G Al-Saidi, M. R. M. Said and A. Kilicman, "A new hyperchaotic map and its application for image encryption," The European Physical Journal Plus, 133(1), Jan. 2018, pp. 6-20.

[22] J. Oravec, J. Turan, L. Ovsenik, T. Ivaniga, D. Solus, and M. Marton, "Asymmetric Image Encryption Approach with Plaintext-Related Diffusion," RADIOENGINEERING, 2018, vol. 27(1), pp. 281-288.

[23] A. Pandey and J. Chopra, "Steganography Using AES and LSB Techniques," International Journal of Scientific Research Engineering & Technology (IJSRET), June. 2017, vol. 6(6), PP. 620-623.

[24] K. Sarita, "A research Paper on Cryptography Encryption and Compression Techniques," International Journal Of Engineering And Computer Science, vol. 6(4), 2017, pp. 20915-20919.

[25] R. Tripathi and S. Agrawal, "Comparative study of symmetric and asymmetric cryptography techniques," International Journal of Advance Foundation and Research in Computer (IJAFRC). Jun. 2014, vol. 1(6), pp. 68-76.

[26] S. Singh & A. Singh, "A Review on the Various Recent Steganography Techniques," IJCSN International Journal of Computer Science and Network, vol. 2(6), 2013, pp. 2277-5420.

[27] W .Stallings, "Cryptography and network security, Principles and practices," Fourth Edition. Pearson Prentice Hall, 2006, USA.

[28] X.J. Tong, M. Zhang, Z. Wang, Y. Liu, H Xu, and J. Ma, " A fast encryption algorithm of color image based on a four-dimensional chaotic system," Journal of Visual Communication and Image Representation, Nov. 2015, vol. 33, pp.219–234.

[29] Y. Zhang, "A Fast Image Encryption Algorithm Based on Convolution Operation," IETE Journal of Research, Dec. 2017, DOI:10.1080/03772063.2017.1400406.

