IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 1, Ser. I (Jan - Feb 2020), PP 31-37
www.iosrjournals.org

Review of Image Encryption Techniques

Manish Kumar[1], Rachid Ait Maalem Lahcen[3], R. N. Mohapatra[3], Chandan Alwala[2], and Surya Vamsi Krishna Kurella[2]

[1]*Department of Mathematics, Birla Institute of Technology and Science, Pilani, Hyderabad Campus, Jawahar Nagar, Shameerpet, Hyderabad, 500078, Telangana, India*
[2]*Department of Electronics and Communication Engineering, Birla Institute of Technology and Science, Pilani, Hyderabad Campus, Jawahar Nagar, Shameerpet, Hyderabad, 500078, Telangana, India*
[3]*Department of Mathematics, University of Central Florida, Orlando, FL 32816, USA*

Abstract: *Security is one of the core areas of study in recent days. Encryption of the image is widely known as an effective method for its secure transmission. The objective of any image encryption method is to obtain a top quality hidden image in order to keep information secret. In this paper, the procedures and schemes of different image encryption techniques that provide privacy and security are reviewed.*

Keywords: *Chaos, Neural Networks, DNA method, Arnold Transform, Rubik Cube Method, Fractional Fourier Transform, Wavelet Transform, AES.*

Date of Submission: 26-12-2019 Date of Acceptance: 11-01-2020

I. Introduction

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. The process of encoding an image with the help of some encryption algorithm is image encryption.

Images are an integral part of our life. It has become customary to record occasions through images. We use CT scans and MRI images for diagnosis of abnormal symptoms. Often, patients seek second opinion and face with the problem of maintaining privacy as well as secure transmission of their CT or MRI images. However, transmitting and receiving images has become easier with the invention of technology and development of image encryption algorithms. But an open platform like the internet may not be safe for transmission at all times. Military and medical images can be confidential and must be kept out of the reach of unauthorized users. Therefore, there is a need for a secure image sharing method that ensures safe image transmission.

Cryptography plays a major role in achieving this goal. Due to the increasing popularity and necessity for image encryption, many methods for the same have been devised. Some of these include Chaos system [1-5] by Sudan Jha; Jui-Cheng Yen, Jiun-In Guo; Boyu Zhu, Aiping Jiang, Xue Bai, Dongdong Bai; Junxin Chen, Yu Zhang, Lin Qi, Chong Fu, Lisheng Xu, Arnold transform[6-10] by Y. L. Yang, N. Cai; B. Li and J. W. Xu; M. R. Abuturab; R. N. Bracewell, H. Bartelt, A. W. Lohmann, N. Streibl; T. K. Shih, L. C. Lu, R. C. Chang, DNA method [11-15] by Wang, Zhang, Bao; Babaei Majid; M. Khan; A. Kulsoom, D. Xiao, A. Rehman, S. A. Abbas; L. Zeng, R. Liu, Rubik Cube Transform [16-20] by K. Loukhaoukha, J.Y. Chouinard, A. Berdai; A. Westfeld, A. Pfitzmann; M. Juneja, P.S. Sandhu; M. Matsumoto, T. Nishimura; Borko Furht, Darko Kirovski, Fractional Fourier Transform [21-25] by V. Namias; C. O. Torres; C. Candan, M. A. Kutay, H. M. Ozaktas; K. N. Naveen, J. Joby, S. Kehar; A. W. Lohmann, Elliptic Curve AES method [26-30] by R. Pakshwar, V.K. Trivedi, V. Richhariya; A. Belazi, M. Khan, A.A.A. El-Latif, S. Belghith; H. Liu, Y. Liu; N. Koblitz; S. Sathyanarayana , M.A. Kumar , K.H. Bhat, Wavelet Transform [30-35] by Sweldens W; Luo Y, Du M, Liu J; Daubechies I; Loukhaoukha K, Chouinard J Y, Taieb; Singh N, Sinha A.

Our objective in this short review is to provide a brief summary of the contents of the above mentioned papers in an easy manner for readers to understand and choose the technique that best meets individual requirements. We mention each method briefly.

II. Chaos-Based Encryption

2.1 Using true Random Numbers [36]

The abstract by Hongjun Liu, Kadir, Xiabo Sun focusses mainly on true random numbers generation. A sequence/pattern is said to be truly random if it passes all the statistical tests for randomness, which we could ever find. The encrypted image should be unpredictable and reproducible by an unauthorized individual. The novelty here is the generation of one-time keys by the hash value of the truly random environmental noise (using a digitalized voice recorder). A system of equations i.e. Liu system is used to enhance the chaotic state al-

ready achieved. As the input required varies each time, this method is very resistant to external attacks. Even though the calculations required to create a chaotic state are complex, the operators used here are very easy for implementation.

2.2 Using Chen Chaotic System [37]

This method believes that encrypting the higher four bit-planes of an image selectively can result in a good level of security. Scrambling and diffusion of pixels in the image are done. The method proposed by Zhou-Feng Chen, Wei Zhao, Jiang, Chong Fu is secure against Brute force attack and is key sensitive and is effective even in terms of speed. The success of this method may be limited because of the common operations it uses. This makes the external attacks vulnerable despite having less execution time.

2.3 Using Cyclic Shift [38]

In this method, rows and columns are scrambled in a random fashion using a 1D logistic map. Diffusion of pixels can be done any number of times. Each of the scrambled processes (such as a row scrambling) is taken as a separate image and finally, all the images thus produced are XOR-ed to get the encrypted image. The method proposed by professors of Sastra University aims at improving the shortcomings of the cyclic sequence generation by Wang. However, the randomness of the row or column, as to how they can be selected may create confusion as no algorithm for such selection has been proposed.

2.4 Double Chaotic Logistic Map [39]

This method uses the key to enhance security. Two keys say a and b are generated using a logistic map. Then XOR operation is applied to each other and the result is then XOR-ed again with the original image. This method proposed by Haifaa W Safi and Ashraf Y Maghari works better than that proposed by Liu and Miao (which uses logistic map sequence as a key).

2.5 Hyper Chaos [40]

In this method, the frequency domain of the image is divided into magnitude and phase components using Fractional Fourier Transform (FFT). The method proposed by Wenting Yuan, Xueiln Yang, Wei Guo, and Weisheng Hu then the method undergoes a series of operations including the Runge-Kutta method. Magnitude and phase obtained by FFT are considered as matrices. The uncorrelated chaotic sequences are generated through the hyperchaos equations and these sequences are used to encrypt the magnitude and phase of the matrix. The combination of frequency and spatial domain significantly enhances the security level of the image.

2.6 Fuzzy Cellular Neural Networks [41]

Neural networks possess attractive properties such as high non-linearity, parameter sensitivity and ability to learn on their own. So, information can be encrypted using neural networks. Similar to neural networks, cellular neural networks (CNN) are parallel computing paradigm in which only the neighboring elements communicate with each other. Uncertainties popping out from CNN can be caught with the help of mathematical tools provided by Fuzzy theory. This article by K Ratnavelu, M Kalpana, P Bala Subramaniam, K Wang, P Raveendran uses the idea of integrating fuzzy theory into CNN paradigm to give a new image encrypting model FCNN. The idea here is to use each generated FCNN chaotic signal with each pixel of the original image to generate the output encrypted pixel. The chaotic signal can begin at any point in the originally created chaotic sequence generated by FCNN which further increases the security of this algorithm. However, if any one of the parameters generating the chaotic signal changes, it affects the channel where its parameter is changed. To avoid this, they introduced the key that depends on all the three-color channels. This method is resistant to brute force, chosen plain text attacks.

2.7 Fusion compression and encryption [42]

This article by Maher Jridi, Ayman Alfalou, Abdallah, Brosseau enhances the security of previously used methods in terms of resistance against various attacks and at the same time, aims to accelerate the key generation process. To obtain a real-time chaos-based secure simultaneous compression, fusion and encryption (SFCE) of multiple images, this method is used. Henon map is used for row and column permutations where the initial conditions are related to the original image. Then skew tent map is employed to generate another random matrix where pixel scrambling is carried out. Henon map, which is a well-known discrete-time dynamic system exhibits chaotic nature. 1-D asymmetric tent map (Skew tent map) is used in many cryptographic applications due to its simplicity, high keyspace, and high key sensitivity. In this method, the existing SFCE scheme has improved in terms of bandwidth limitation, fast approach, and resistance to attacks.

2.8 2-D logistic adjusted sine map [43]

The discrete time analog of the logistic equation is referred to as the logistic map. Sine map is retrieved using the classical sine function by transforming its inputs into the range [0, 1]. This article by Zhongyun Hua, Yicong Zhou gives the mathematical definition of the 2-D logistic adjusted sine map (lasm). The logistic equation is scaled by a factor of mhu and fed into the input of the sine map. The output points of 2-D lasm distribute in the whole data range of 2-D phase plane. Therefore, 2 D lasm outputs are more random and benefits from a better ergodicity. Some random values are generated and added to the surroundings of the plane image. These values can influence all the pixels after the confusion and diffusion operations. As these values are randomly generated, and different in each encryption cycle, to encrypt a plane image several times, the generated cipher images are different from each other. Now, bit manipulation confusion and diffusion are performed on the resulting pixels. However, the mathematical operations used are a bit complex.

III. Arnold Transform [44]

In this method, the receiver needs to select and send a reference image in addition to the original image which needs to be secure. The final encrypted image will look similar to the reference image. This reference image is double the size of the image needed to be encrypted. Discrete wavelet transform can also be used to encrypt the image. The scheme proposed by V M Manikandan and V Masilamani is used in such a way that the pixel values of the image before encryption are in the range of (0-255). Arnold transform has a special periodic property which ensures that after j (j < maximum of length, breadth of the image) iterations, the scrambled matrix will be transformed into the original one. The usefulness of this method is that the encrypted image will look like a natural image without producing the conventional noise-like image. And the receiver gets his/her image from the actual looking image.

3.1 Arnold and Logistic [45]

The method by Jinshan Wang, Xiaodong Wang, Changjiang Zhang believes that in order to obtain the robust watermark, the watermark should be embedded in the low-frequency components of the image. First, the given image is scrambled using Arnold transform. Then logistic maps are used for scrambling. The original image is decomposed by a discrete wavelet transform. The watermarked image is mixed by Arnold transform. This watermarked image is embedded into the low-frequency coefficients of the discrete stationary wavelet domain and the final watermarked image is obtained. The final reconstructed image has good visual quality; thus, this method has good invisibility and good robustness to noise, rotation, and compression.

3.2 Bit Level Arnold [46]

In this method by Zhengchao Ni, Xuejing Kang, Liwang, the decimal pixel values are transformed into eight-bit binary pixel values. It also uses Lorenz and Rossler systems to generate pseudo-random sequences, say s1 and s2. Then convert these numbers in the range of [1, n] (for columns) or [1, 8N] (for rows). Scrambling of columns and rows are done and Arnold transform is applied. This method is resistant to brute force attack. The correlation between both images is low. Since they use the hyper-chaotic system here, one can achieve more dynamical behavior. However, even though the attackers may not recover original image, but they might get some information of the scrambled image.

IV. DNA Sequence Operation [47]

This method is proposed by Xiuli Chai, Yran Chen, Lucie Vroyde. A DNA sequence consists of four nucleic acid bases, i.e. A (Adenine), C (Cytosine), G (Guanine) and T (Thymine). A, T and G, C are complementary. As zero and one are complementary in a binary system, 00 and 11, 10 and 01 are complementary. Eight of the 24 type encoding rules satisfy Watson and Crick complementary rule. This method deals with DNA encoding to encode the image. SHA-256 hash of the plane image is used to generate the external secret key. Permutation of pixels is executed followed by DNA level diffusion. This method is resistant to all kinds of brute force attacks, entropy, and differential attacks.

4.1 DNA and Chaotic Systems [48]

DNA computing method supports high parallelism and uses the concept of information density. Permutation scrambles position of an image, while diffusion gives information about the redundancy of the image. This article by Radhika K and M K Nalini combines DNA sequences and chaotic systems. In this method, the image is divided into blocks. They are then converted into binary matrices and DNA encoding is applied to them. Then scrambling of the blocks is done and the blocks are divided into equally sized sub-blocks. These blocks are then added by DNA addition and then recombined. This method leads to a hyper-chaotic system which is resistant to differential attacks and entropy.

4.2 DNA and Hyper-Chaotic Operation [49]

There are predefined formulae for the use of hyperchaos. This method by Wembo Zheng, Fei-Yue Wang, and Kunfeng Wang uses Chen's hyperchaotic system equations. Also, there are a particular set of established rules for DNA encoding of a color image. This method uses the available rules for addition, subtraction, and XOR-ing. The Hyper-chaotic system is used for secret key generation. The encrypted image is further replaced by an artificially generated random image which aids in increasing the security of the desired image. One interesting feature of this method is that the encryption is done in a parallel manner for both, the image to be encrypted as well as for the random artificial image to be generated. This method is resistant to differential attack, brute force attack.

4.3 Improved DNA [50]

In this method, they have used 0,1,2, and 3 to express C (Cytosine), A (Adenine), T (Thymine), and G (Guanine). Firstly, they scramble the position of image pixels and the wavelet chaotic make the XOR operations with image pixel values then DNA encoding is done. Then by using cubic chaos generated by a chaotic sequence, they perform XOR operations. The key space is large enough to resist attack, however, this method proposed by Qiang Zhang, Lili Liu, Xiaopeng Wei can be attacked by the phase reconstruction method.

V. Rubik Cube Transform [51]

This method proposed by Raniprima, Hidayat, Nur Andini data hiding is done by encryption with Rubic Cube Transform followed by Stenography. Two keys are randomly generated. Rows and columns of the image are circularly shifted based on the keys generated. The encrypted image is then embedded into a cover image. This method is resistant to brute-force attack and the histograms of the original and encrypted images bear no resemblance.

5.1 Rubik Cube Method with Game of Life [52]

The method proposed by K Govinda, S Prasanna is image encryption by Rubik Cube Transform and Conway's Game of life methods. Diffusion of pixels is done with the help of a random number which is generated with the help of Conway's Game of Life method. There is an initial pattern and finally, they obtain random pattern on following a pre-defined set of rules. The arrangement of the pixels obtained is compared with the turns by Rubik cube. Initial pattern is decided and it is completely random which is known to the sender. With the help of this, the scrambling of pixels is done column-wise. The sender takes a random image and sends it to the receiver. The size of this new image is supposed to be that of the original image. The chosen image is subjected to rotation column wise according to the random number. XOR operation is applied for both values and a completely random image is obtained. the decryption process is the reverse of the encryption process. This method is secure and resistance to a brute-force attack.

VI. Fractional Fourier Transform [53, 54]

Certain Formulae are devised for the calculation of the Fourier transform of functions. A Fourier transform maps a function, let's say f(x) to another function F(x). Fourier transforms as well as Fractional Fourier transform find an application in many areas. This method proposed by Juan Vilardy, Jorge Calderon, Lorenzo Mattos, Cesar Torres aims at using Fractional Fourier transform for image encryption. In this method, masks are used along with Fractional Fourier transform for efficient phase encryption of the image. The masks that are required are produced in a random manner and encryption is done on analog image rather than the digital ones. The decryption process is an inverse of the encryption process. This process is computationally fast.

VII. Elliptic Curve and Advanced Encryption System [55]

The method proposed by Shahryar Toughi, Mohammad H Fathi, Yoones A Sekhavat uses Elliptic Curve and AES encryption. AES encryption is performed in multiple rounds. Each round has four main steps that include byte substitution, row shifting, column mixing and the addition of round key. In the round key step, the output matrix of mix column is XOR-ed with round key. The security of elliptic key cryptography is promised by a discrete logarithmic problem. In the beginning, the sender and receiver compromise on a standard (Elliptic Curve Cryptography) ECC. Once random numbers are generated using the elliptic curve, they are used for creating a group of masked matrices for encryption. Each bit of the current image is XOR-ed with each bit of the masker. This method is resistant to statistical and differential attack.

VIII. Wavelet Transform

8.1 Wavelet and Chaos

This method basis is the fact that one can compress the high-frequency part of an image retaining the low-frequency part. Chaotic encryption is done for low-frequency wavelet coefficients. XOR operation is applied so that information in high-frequency wavelet coefficients is hidden. The current wavelet analysis uses Mallet algo-

rithm wherein the low-frequency component is decomposed continuously. They also use Logistic chaotic map for encryption. This method is robust for noise attack.

8.2 Wavelet transform and XOR operation [56]

Ghost imaging proposed by Kloshko is imaging through total light intensity behind the object plane and light intensity distribution before the object plane. In compressive sensing theory, an image which is sparse or can be sparse in some transfer domain such as discrete cosign transform or discrete wavelet transform can be compressed by a measurement matrix, which is selected randomly. This article by Xianye Li, Xiangfeng Meng, Xiulun Yang, Yurirong, Yongkai, Xiang, Wegui, Guoyan, Hongyi uses a sparsity adaptive matching pursuit algorithm (SAMP) modified from orthogonal matching pursuit algorithm to increase results' accuracy. Multiple plain text images of size n*n are sparse towards the lifting wavelet transformation, which transform the images into the wavelet domain. Then sparse images are scrambled to fixed positions. Then XOR operation is applied to the scrambled image. The XOR-ed image is encoded with the row scanning compressive ghost imaging scheme. Then the ciphered image is detected by BD arrays. This method performs the transform integer to integer, which results in much lower data loss and applied image encoding and decoding.

IX. S-Box and AES

AES stands for Advanced Encryption Standard. It belongs to the Rijndael family of ciphers. AES implements a symmetric key algorithm. S-Box acts a lookup table for substitution. This article by Reza, Mohsen, Seyed Hossein, Maysam implements an algorithm which tends to transform the rows cyclically based on the first-pixel value. This is opposed to the conventional way for encryption using AES. The Histograms of the original image and the encrypted image are found to have hardly any resemble. Further, the correlation coefficients for adjoint pixels are far apart from each other. This method is also easy to implement.

X. A Trio Approach [58]

This method by Sundararaman, Sivaraman, Siva Janakiraman, Har Narayan Upadhyay, Rengarajan proposes a trio method which uses cellular automata, Linear feedback shift register and synthetic image. Permutation and Diffusion are both provided by Cellular automata. The work of a pseudo-random generator is provided by the linear feedback shift register. An important thing about linear feedback shift register is that its output depends on its past state. Cellular automation is very easy to construct because of which it finds an application in many real systems. Synthetic image accounts as a collector of keys. Every next stage of the linear feedback shift register is XORed with the current stage at the rising clock edge to obtain the encrypted image. The encrypted image has high entropy and the correlation coefficients of the adjacent pixels are far apart. This method thus proves to be an efficient method for image encryption.

XI. Using Neural Networks [57]

Neural networks are now being used in almost every field. This can be attributed to its learning nature and accuracy. This method proposed by Yousef, Karim, Nooshin aims at taking advantage of chaotic systems and neural networks by combining them into a single platform for image encryption. The input image is fed into a chaotic neural layer in which methods like Chua and Liu systems are employed to bring the chaotic behavior. The output is then fed into a permutation neural network where a nonlinear mapping is performed to obtain the final encrypted output. The decryption phase is the inverse of the encryption phase. The entropy of the resulting image is high, and the histograms of the original and encrypted image bear no resemblance. The only limitation of this method is that it is difficult to implement.

XII. Using Henon Map [60]

In the method proposed by Ping Ping, Feng Xu, Yingchi Mao, Zhijian Wang, a new strategy to process two pixels simultaneously is proposed along with modifying the pixel value and the pixel position. The parameters of the Henon Map are chosen such that the Henon Map exhibits the chaotic behavior. The map is then discretized. Some of the parameters are kept as secret keys. The discrete Henon Map is used for permutation and diffusion, whereas the classical Henon Map is used for keystream generation. This method requires to pad the image into a square image. Usually, if the secret key is composed of image features, then the receiver needs to receive the secret key each time the different image is encrypted. However, in this method, the image features are inserted into the cipher image. Thus the secret key needs to be sent only once when different images are encrypted. This method decreases the correlation between two pixels adjacent to each other and is capable of transforming the given image into a random cipher image. This method is comparatively faster as it tries to manipulate two pixels simultaneously.

XIII. Using generalized Vigenére-type table in Virtual Planet Domain [62]

In this method proposed algorithm is based on a new technique using a generalized Vigenére-type table over a symmetric group of order n in the Virtual Planet Domain (VPD). The main objective of this work is to overcome on limitations of DNA based coding algorithms, those are mentioned in this research article. The designed VPD has been tested by using NIST Statistical test suits for its randomness and found to be random. A new formula for the keyspace has been designed. Any color image which is to be encrypted is first converted into the VPD domain. This step provides a fine interlacing among pixels and then a generalized Vigenére-type table is used for encryption. The encrypted image is robust against all kinds of well-known attacks.

XIV. Conclusion:

In this paper, we have mentioned several contemporary methods of image encryption which complied with the security standards required by the industry. An interested reader can read the papers in the references relevant to their own research goals. For the sake of brevity and dissemination of appropriate information, we have not elaborated the details pertaining to each of the methods. Though many methods for image encryption have emerged, there is still a lot of scope for many new methods to discover so that hackers can't hack the images for inappropriate use. However, proposing a fully secure method is not feasible due to a growing number of unauthorized image deciphering techniques, and the presence of ambitious unauthorized hackers. In view of this image encryption is a dynamic procedure where periodic change in transmission technique is essential.

Acknowledgment:

The first author is thankful to the Science & Engineering Research Board, Government of India, for providing financial support through project file no. YSS/2015/000930, and the third author is grateful to the Mohapatra Family Foundation, New Jersey, for its support to conduct this review.

References:

[1]. Sudan Jha, "Chaotic Image Encryption Techniques", International Journal of New Innovations in Engineering and Technology, Volume 6, Issue 1, Pages 12–25, October 2016.
[2]. Jui-Cheng Yen, Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", Volume: 4, Pages: 49–52 vol.4, Year: 2000.
[3]. Boyu Zhu, Aiping Jiang, Xue Bai, Dongdong Bai. "A method research of image encryption based on chaotic and secret sharing", IEEE Cyber Conference, Pages: 1823–1828, Year: 2015.
[4]. Yannick Abanda, Alain Tiedeu, "Image encryption by chaos mixing", volume 10, issue 10, p. 742 – 750, October 2016.
[5]. Junxin Chen, Yu Zhang, Lin Qi, Chong Fu, Lisheng Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression", Volume 99, Pages 238–248, February 2018.
[6]. Y. L. Yang, N. Cai, and G. Q. Ni, "Digital image scrambling technology based on the symmetry of Arnold transform," Journal of Beijing Institute of Technology, Pages 216–220, 2006.
[7]. Bing Li, Jia Wei Xu, "Period of Arnold transformation and its application in image scrambling," Journal of Central South University of Technology, Volume 12, Issue 1, Pages 278–282, 2005.
[8]. M. R. Abuturab, "Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain," Optics & Laser Technology, Volume 45, Pages 525–532, February 2013.
[9]. R. N. Bracewell, H. Bartelt, A. W. Lohmann, and N. Streibl, "Optical synthesis of the Hartley transform," Applied Optics, Volume 24, Issue 10, Pages 1401–1402, 1985.
[10]. T. K. Shih, L. C. Lu, and R. C. Chang, "An automatic image inpainting tool," Proceedings of the Eleventh ACM International Conference on Multimedia Pages 102–103, 2003.
[11]. Xing-Yuan Wang, Ying-Qian Zhang, Xue-Mei Bao, "A novel chaotic image encryption scheme using DNA sequence operations", Optical Lasers Engineering, Volume 73, Pages 53–61, 2015.
[12]. Babaei Majid. "A novel text and image encryption method based on chaos theory and DNA Computing", Volume 12, Issue 1, Pages 101–107, 2013.
[13]. Majid Khan, "A novel image encryption scheme based on multiple chaotic S-boxes", Nonlinear Dynamics, Volume 82, Issue 1-2, Pages 527–533, October 2015.
[14]. A. Kulsoom, D. Xiao, Aqel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and dna complementary rules", Multimedia Tools and Applications, Volume 75, Issue 1, Pages 1–23, January 2016.
[15]. Li Zeng and R. Liu, "Cryptanalyzing a novel couple images encryption algorithm based on DNA subsequence operation and chaotic system", Volume 126, Issue 24, Pages 5022 – 5025, December 2015.
[16]. K. Loukhaoukha, J.Y. Chouinard, A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," Journal of Electrical and Computer Engineering, Volume 2012, Article 7, 2012.
[17]. A. Westfeld, A.Pfitzmann, "Attacks on steganographic systems", International Workshop on Information Hiding, Volume 1768, Pages 61–76, 1999.
[18]. M. Juneja, P.S. Sandhu, "Designing of robust image steganography technique based on LSB insertion and encryption", International Conference on Advances in Recent Technologies in Communication and Computing, Pages 302–305, October 2009.
[19]. M. Matsumoto, T. Nishimura, "Marsenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator", ACM Transactions on Modeling and Computer Simulation, Volume 8, Issue 1, Pages 3–30, January 1998.
[20]. Borko Furht and Darko Kirovski," Multimedia Security Handbook", CRC Press, Pages 95–133, December 2004.
[21]. V. Namias, "The fractional Order Fourier transform and its application in Quantum Mechanics", Journal of Applied Mathematics, Pages 241–265, Volume 25, Issue 3, 1980.
[22]. Abhishek Singh, P.K.Banerji, "Fractional Integrals of Fractional Fourier Transform for Integrable Boehmians", Proceedings of National Academy of Sciences, Volume 88, Issue 1, Pages 49–53, March 2018.

[23]. C. Candan, M. A. Kutay, H. M. Ozaktas, "The Discrete Fractional Fourier Transform", IEEE Transactions on signal processing, Volume 48, Issue 5, 2000.
[24]. K. N. Naveen, J. Joby, S. Kehar, "Fully phase-encrypted memory using cascade extended fractional Fourier transform", Optics and Lasers in Engineering, Volume 42, Issue 2, Pages 141–151, 2004.
[25]. Adolf W. Lohmann, "Image rotation, Wigner rotation, and the fractional Fourier transform," Journal of the Optical Society of America, Volume 10, Issue 10, Pages 2181–2186, 1993.
[26]. R. Pakshwar, V.K. Trivedi, V. Richhariya, "A survey on different image encryption and decryption techniques", Int. Journal of Computer Science, Information Technologies. Volume 4, Issue 1, 2013 Pages 113–116, 2013.
[27]. A. Belazi, M. Khan, A.A.A. El-Latif, S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution based encryption", Nonlinear Dynamics. Volume 87, Issue 1, Pages 337–361, 2017.
[28]. H. Liu, Y. Liu, "Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve", Optics and Laser Technology, Volume 56, Pages 15–19, 2014.
[29]. N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, Volume 48 (177), Pages 203–209, 1987.
[30]. S. Sathyanarayana, M.A. Kumar, K.H. Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points", Network Security, Volume 12 (3), (2011) 137–150.
[31]. Sweldens W, "The lifting scheme: a custom design construction of biorthogonal wavelets", applied and computational harmonic analysis,3(2):186–200, Article 15, 1996.
[32]. Luo Y, Du M, Liu J. "A symmetrical image encryption scheme in wavelet and time domain", Communications in Non-Linear Science and Numerical Simulation, Volume 20(2):447–60, 2015.
[33]. Daubechies I, Sweldens W, "Factoring wavelet transform into lifting steps", Journal of Fourier Analysis and Application, 4(3):247–69, 1998.
[34]. Loukhaoukha K, Chouinard J Y, Taieb "Multi-objective genetic algorithm optimization for image watermarking based on singular value decomposition Lifting Wavelet Transform", 6143:394–403, 2010.
[35]. Singh N, Sinha A, "Optical image encryption using Hartley transform and logistic map", 282(6):1104–1109, March 2009.
[36]. Hongjun Liu, Abdurahman Kadir, Xiaobo Sun. "Chaos-based colour image encryption scheme with two random number keys from environmental noise", Volume 11, Issue 5, p. 324 – 332, April 2017.
[37]. Chong Fu, Zhou-Feng Chen, Wei Zhao, Hui-yan Jiang, "A New Fast Color Image Encryption Scheme Using Chen Chaotic System", 18th IEEE conference, Pages: 121–126, 2017.
[38]. Xing-Yuan, Sheng-Xian, Ying-Qian, "Novel image encryption algorithm based on cycle shift and chaotic system", Optics and Lasers in Engineering Volume 68, Pages 126–134, 2015.
[39]. Haifaa W Safi, Ashraf Y Maghari, "Image Encryption using Double Chaotic Logistic Map", ICPET conference, Pages: 66–70, 2017.
[40]. Wenting Yuan, Xueiln Yang, Wei Guo, Weisheng Hu, "A double domain image encryption using hyperchaos", 19th ICTON conference, Pages: 1–4, 2017.
[41]. K Ratnavelu, M Kalpana, P Bala Subramaniam, K Wong, P Raveendran, "Image encryption method based on chaotic fuzzy cellular neural Networks", Volume 140, Pages 87–96, 2017.
[42]. A. Alfalou, C. Brosseau, N. Abdallah, Jridi, "Simultaneous fusion, compression, and encryption of multiple images", Volume 19, Issue-24, 2011.
[43]. Zhongyun Hua, Yicong Zhou, "Image Encryption using 2-D Logistic Adjusted Sine Map", Volume 339, Pages: 237–253, 2016.
[44]. V.M. Manikandan, V. Masilamani. "An Efficient Visually Meaningful Image Encryption Using Arnold Transform", TechSym Conference Pages: 266 – 271, IEEE, 2016.
[45]. Jinshan Wang, Xiaodong Wang, Changjiang Zhang, "Digital Image Water Marking Algorithm with Double Encryption by Arnold Transform and Logistic", International Conference on Networked Computing and Advanced Information Management, Volume: 1, Pages: 329–334, 2008.
[46]. Zhengchao Ni, Xuejing Kang, Lei Wang, "A Novel Image Encryption Algorithm Based on Bit-level Improved Arnold Transform and Hyper Chaotic Map", ICSIP conference, Pages: 156–160, 2016.
[47]. Xiuli Chai, Yiran Chen, Lucie Broyde. "A novel chaos-based image encryption algorithm using DNA sequence operations", Pages 197–213, Volume 88, January 2017.
[48]. K.R.Radhika, M.K.Nalini, " Biometric Image Encryption using DNA sequences and Chaotic Systems", ICRAECT conference, Pages: 164–168, 2017.
[49]. Wenbo Zheng, Fei-Yue Wang, Kunfeng Wang, "An ACP-based Approach to Color Image Encryption Using DNA Sequence Operation and Hyper-Chaotic System", IEEE SMC Conference, Pages: 461–466, 2017.
[50]. Qiang Zhang, Lili Liu, Xiaopeng Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps", AEU, Volume 68, Issue 3, Pages: 186–192, 2014.
[51]. S Raniprima, B Hidayat, N Andini, "Digital Image Steganography with Encryption Based on Rubik's Cube Principle", ICCEREC conference, Pages: 198–201, 2016.
[52]. Govinda.K, Prasanna.S, "A Generic Image Cryptography Based on Rubik's Cube", ICSNS conference, Pages: 1–4, 2015.
[53]. Juan M. Vilardy, Jorge E. Calderon, Cesar O. Torres, Lorenzo. Mattos, "Digital Images Phase Encryption using Fractional Fourier Transform", CERMA conference, Pages: 15–18, 2006.
[54]. H Yoshimura, R Iwai," New encryption method of 2D image by use of the fractional Fourier transform", IEEE Conference on Signal Processing, Pages: 2182 – 2184, 2008.
[55]. Shahryar Toughi, Mohammad H. Fathi, Yoones A. Sekhavat, " An image encryption scheme based on elliptic curve pseudo-random and Advanced Encryption System", Volume 141, December 2017, Pages 217–227.
[56]. Xianye, Xiangfeng, Xiulun, Yurong, Yongkai Yin, Xiang Peng, Wenqi, Guoyan, Hongyi, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme", Volume 102, Pages 106–111, March 2018.
[57]. S H Kamali, R Shakerian, M Hedayati, M Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", ICEIE Conference, Year: 2010, Volume:1 Pages: 141–145.
[58]. S Rajagopalan, S Rethinam, S Janakiraman, Har Narayan Upadhyay, R Amirtharajan, "Cellular Automata + LFSR + Synthetic image: A trio approach to image encryption", ICCI conference, Year: 2017 Pages: 1 – 6.
[59]. Sudipta Singha Roy, Shaikh Akib Shahriyar, Md. Asaf-Uddowla, Kazi Md. Rokibul Alam, Yasuhiko Morimoto, "A Novel Encryption Model for Text Messages using Delayed Chaotic Neural Network and DNA Cryptography" ICCIT conference, Year: 2017 Pages: 1 – 6.
[60]. Ping Ping, Feng Xu, Yingchi Mao, Zhijian Wang, "Designing permutation substitution image encryption networks with Henon map", Neurocomputing, Volume 283, March 2018, Pages 53–63.
[61]. Majid Khan, Tariq Shah, "A Literature Review on Image Encryption Techniques", Heidelberg 2014.

[62]. Manish Kumar, R.N. Mohapatra, Sajal Agarwal, G. Satish, S.N. Raw, "A New RGB Image Encryption using generalized Vigneretype table over symmetric group associated with virtual planet domain", Multimedia Tools and Applications, Volume 78, Pages: 10227 – 10263, 2019 (Springer).
[63]. Zhongyun Hua, Binghang Zhou, Yicong Zhou, "Sine-Transform-Based Chaotic System with FPGA Implementation", IEEE Transactions on Industrial Electronics, Volume: 65, Issue: 3, March 2018.
[64]. Zhongyun Hua, Shuang Yi, Yicong Zhou, Chengqing Li, Yue Wu, "Designing Hyperchaotic Cat Maps with Any Desired Number of Positive Lyapunov Exponents", IEEE Transactions on Cybernetics, Volume: 48, Issue: 2, February 2018.
[65]. Wang J, Long F, Ou W, "CNN-based color image encryption algorithm using DNA sequence operations", International Conference on Security, Pattern Analysis, and Cybernetics, 730–736, 2017.