Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

A Survey of Chaos based Cryptography and Steganography Techniques

Kusum Lata[1], Dr Savita Rathee[2], Dr Meenakshi[3*],Vinita Yadav[4], Navita Dhaka[5]

[1,4,5] *Research Scholar, Dept of Mathematics, Maharshi Dayanand University, Rohtak-124001, Haryana, India*

[2]*Associate Professor, Dept of Mathematics, Maharshi Dayanand University, Rohtak-124001, Haryana, India*

[3]*Assistant Professor, Dept of Mathematics, Maharshi Dayanand University, Rohtak-124001, Haryana, India*

Corresponding Author (*) - meenakshi.maths@mdurohtak.ac.in

Contributing Author (1) E-mail: kusum.rs24.maths@mdurohtak.ac.in

Abstract:-In this modern era, as the data is transmitted through the use of digital media, there is a need of secure communication. Steganography is one of such practices. It is the art and science of hiding the existence of a message within the cover media like image, text, audio, video etc. Another such practice is cryptography which is the art and science to change the message into unreadable form. For high security and robustness of a steganographic method, cryptography and steganography can be combined where the secret message is encrypted firstly and then encrypted data is embedded in the cover media. Due to sensitivity of initial conditions and ergodicity of chaotic maps and fuzzy logic approaches, as a tool to make decisions about different conditions, are used in steganography. This paper presents a survey of cryptography and steganography techniques based on chaos. Fuzzy logic approaches are also used in generating parameters used to modify chaotic maps' initial keys to ensure the unpredictability of the image steganographic methods.

Keywords*: Steganography, Cryptography, Fuzzy logic, Chaotic map, Chaos, Image processing*.

1. Introduction

From the small institutions to the largest enterprises, everyone can understand the importance and sharing of data. It is difficult to prevent the misuse and theft of data for improper purposes by eavesdroppers. Data cannot be protected from eavesdroppers with just a password; special methods and specific security systems need to be used for this purpose. The security system's significance can be observed nowadays for secure communication and for maintaining confidentiality of secret data. Security system is classified as shown in the figure 1 [1].

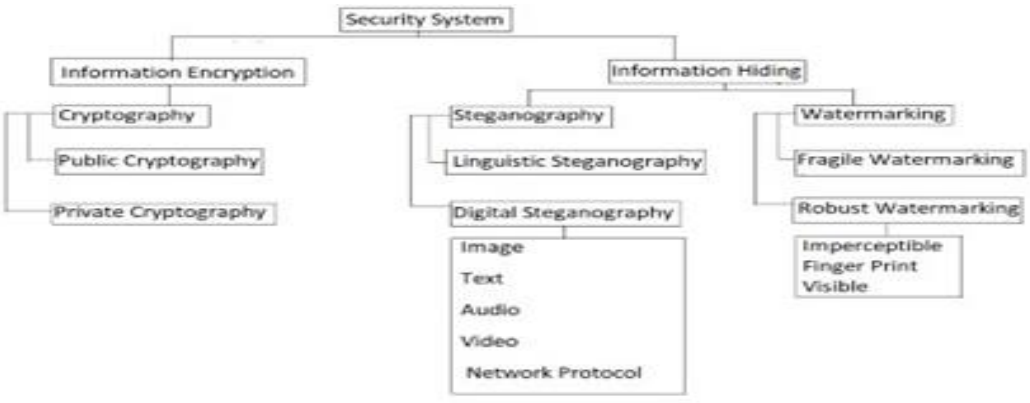

Figure1: Classification of security system

Cryptography, steganography, and watermarking are well-known techniques for protecting data from theft and unauthorized interference. According to the Merriam-Webster online dictionary, cryptography is secret writing in which a message is enciphered and deciphered using a secret code or cipher. In the digital medium, cryptography involves encoding and decoding information with the help of computers [2]. The term

steganography is derived from Greek words 'Stegano' means 'Covered/Hidden' and 'Graphia' means 'Writing'. Steganography can be defined as the art and science of hiding a secret multimedia data in another multimedia data such as image, text, audio or video. One can emphasize that steganography is just not about the art of hiding data, it is a technique that hides the transmission of secret data also. As steganography and cryptography both are used to protect data from unauthorized interference, still, there is a difference between steganography and cryptography. In steganography, the secret message is hidden in another media, such as text, video, audio, etc., so that the unauthorized party does not even know about the existence of the secret message. In contrast, in cryptography, the secret data is available to the unauthorized party in an unintelligible form. Data security cannot be ensured by using cryptography and steganography technique separately. Therefore to ensure the security of secret data, good results can be achieved by combining cryptography and steganography techniques.

1.1 Classification of steganography

Steganography is basically of two types: Natural language steganography and technical steganography [3]. Natural language steganography includes text steganography, as clear from name, in which secret text is hidden in tabs, white spaces, capital letters etc. of carrier text, while technical steganography includes image, audio, video steganography which are described as given below:

1.1.1 Image Steganography [4]: The technique of hiding secret data inside an image is called image steganography. In this technique, the secret data is embedded within the pixels or spectral components of the image depending on image domain. It hides the data in BMP, PNG, JPEG file formats.

1.1.2 Audio Steganography: The technique of hiding secret data in audio files is called audio steganography. This method hides the data in WAV, AU, MP3 file formats.

1.1.3 Network Steganography [4]: The technique of hiding secret data in the network protocols such as TCP, UDP, ICMP, IP is called network protocol steganography.

1.1.4 Video Steganography: The technique of hiding secret data in video files is known as video steganography. It hides the data in AVI, MP4, MKV, MOV, FLV file formats.

1.1.5 Text Steganography: The technique of hiding secret data in text files is called text steganography. This is the most common type of steganography in which some tabs, white spaces, capital letters are used to attain information hiding.

There are various applications of image steganography such as copyright control, covert communication, smart ID's etc. In last decade, an image is being preferred as the cover media to hide the secret data due to high payload and imperceptibility. Steganalysis [5] unlike steganography is described as a tool to analyze stego-image (image hides the secret data based on some algorithms), to detect and to extract the secret data hidden within a digital media.

1.2 Factors affecting image steganography techniques [6]

The following are the factors used to analyze the performance of a steganographic technique:

1.2.1 Robustness: It refers to the ability of steganographic techniques to resist the statistical attacks and unauthorized extraction of secret data.

1.2.2 Hiding capacity: It refers the maximum load of secret data hold by cover image, maintaining the visual quality of stego-image, it is also known as payload capacity. Sahu et al. [5] calculated it mathematically.

1.2.3 Imperceptibility: It refers to the quality of method to hide secret data in such a way so that it is unnoticeable and undetectable to human visual system.

2. Chaos Theory based Methods in Image Steganography

2.1 Chaos Theory

Due to randomness behavior of chaos system, chaos theory is well known and has applications in field of steganography where cover is any digital media. Chaos is a non-linear dynamical, deterministic system, sensitive to initial conditions and parameters (an $\epsilon > 0$ change, however small it may be, in initial condition and parameters, known as bifurcation parameters, leads a large change in output), have ergodicity property (outputs depend on

inputs directly and cover each available output), and generates random behavior in sequences which are not random but generated by a deterministic model [7][8]. The other characteristics of chaotic methods are absence of periodicity and have either oscillating or divergent behavior. Since text is not the only way to share information, images also play significant role, hence fuzzy theory, combined with maps reflecting chaotic behavior [9], is used to encrypt secret images. Some important chaotic maps used to obtain sequences (pseudo random) for secret data encryption (whether it is in image or text form) and find locations in cover image to embed secret data: Logistic [10][11], Tent [12][13], Bernoulli [7], Quadratic [14], 2D Henon map [15], 3D LCA Map [8] etc.

There are a number of steganographic techniques, consisting of combination of methods in chaos and fuzzy theory, proposed in image steganography in which suffled secret data, suffling done by chaotic maps, is hidden in cover image's pixels or spectral components depending of its domain [16]. Some well known steganographic techniques are LSB [17] [18], PVD [17], BPCS [4] in spatial domain and DCT [19] [20] [18], DWT [21] [18], DHT [21], IWT [23], DFT [24] etc. in frequemcy domain.

2.2 Chaos based encrypted text embedding in edge pixels detected by fuzzy set theory

It is a steganographic technique in which secret data, in form of text, is encrypted by using a chaotic map, named as Bernoulli map, also known as binary shift map, and embedded in edge pixels of cover image by LSB substitution [1][7][25][26]. Bernoulli map is defined as

$$\gamma_{n+1} = a(1 - \gamma_n)$$

where γ_0 is the initial condition and a is control parameter. To encrypt data, by choosing $\gamma_0 \in [0,1]$, γ_0 is taken as secret key of this cryptographic techniques, a pseudo random sequence is created by above defined map which leads a binary sequence, created by choosing a convenient threshold. By XORing this new sequence with the binary sequence of secret message, secret text is encrypted. To embed the cipher text in image, fuzzy inference system (FIS is a tool to make decisions based on fuzzy logics) is considered which follows strictly the following steps: fuzzification, rule base, inference engine, aggregation, defuzzification [7][11]. Cipher text is embedded in edge pixels (pixels with rapid change in intensity), as edges are the less sensitive areas to human visual system as compared to smooth areas. To detect edges, there are a number of methods which can be combined to propose robust techniques in steganography. Canny edge detection and fuzzy edge detection are both combined to obtain modified fuzzy edge detector [7], gives a large number of edges in which data is embedded. Other common chaotic map used for encryption is logistic map. It is a discrete time chaotic system, defined as

$$\gamma_{n+1} = a\gamma_n(1 - \gamma_n)$$

where $4 > a > 0$ is called control parameter / bifurcation parameter / biotic potential of the map. For $a \in (0,3)$, the system represents stable system, for $a \in (3,3.57)$, the system attains periodicity and for $a \in (3.57,4)$, the system exhibits chaotic behavior, however periodicity can be observed in the system. Sabery et al. [27] made use of logistic map to find addresses in cover image to hide a secret image.

2.3 Steganography technique includes chaos based pixels' address to embed secret data in color image compressed by fuzzy logics

In reference to Tayel et al. [11], one can embedded an image within an image by using chaos distribution. The secret image is compressed by using fuzzy logic compressor, then secret image bits are embedded in LS Bits of cover image in random locations determined by a 2D chaotic map. One of such 2D chaotic map is defined as

$$\begin{cases} \alpha_{n+1} = mod(1 - 2{\beta_n}^2 \times 10^5, 1) \\ \beta_{n+1} = mod(\cos(6cos^{-1}(\alpha_n) \times 10^5), 1) \end{cases}$$

where $\alpha_n, \beta_n \in [0,1]$. This map is used to find positions in a digital image to embed secret data bits.

2.4 Image steganography technique with increased sensitivity to initial conditions in 3D chaotic map to address pixels

In reference of Sharif et al. [8], by using four parameters based on MSBs, LSBs, lengths of MSBs, LSBs, obtained initial condition and generates three sequences of length more than twice of the length of secret bits, hence find required components (row, column number and color component) of cover image to embed secret bits. With strong chaotic characteristics, a LCA (3D chaotic map) is used to determine the addresses in cover image in which secret data bits are embedded by divided secret bits in 2 classes (known as MSBs and LSBs). The LCA map is defined as

$$a_{n+1} = \frac{1}{\alpha^2} tan^2\left(\beta tan^{-1}\sqrt{b_n}\right) mod\ 1$$
$$b_{n+1} = r c_n (1 - c_n)$$
$$c_{n+1} = 16{a_n}^5 - 20{a_n}^3 + 5\, a_n$$

where $\alpha \in \left[0, \frac{1}{\beta}\right]$, $r \in [3.65,4]$ and $a_n,\ b_n, c_n \in [0,1]$.

2.5 Image steganography technique based on merging two or more chaotic maps by additive and multiplicative operations to robust

One can combine the three chaotic maps (logistic, tent and quadratic) to obtain a single pseudo random sequence by using addition and multiplication operations. Two or more than two chaotic maps are combined to increase security level. If C_1, C_2, C_3 are different chaotic maps, then a new map

$$C = [kC_1 + (1-k)C_2] * C_3$$

where $k \in (0,1)$ is obtained to generate a random sequence to encrypt data. To check that the generated sequence has chaotic behavior or not, correlation of the generated sequence is compared with the correlation of Gaussian filters, that should be a delta function [12].

2.6 Steganography techniques involving combination of fuzzy, chaotic and DNA based image encryption

In this technique, chaotic map, Choquet's fuzzy integral sequence and DNA coding is used for image encryption. As we know, DNA is a polymer made up of nucleotides, which are composed of four nitrogenous bases: adenine (A), cytosine(C), guanine (G), and thymine (T). 'A & T' and 'C & G' are complements of each other. As DNA can store a vast amount of information within their structure, so DNA is used in image encryption. In this DNA based image encryption technique [28], confusion and diffusion [29] techniques are followed. To achieve high security and high sensitivity in image encryption, the fuzzy integral, differs from the classical integral, is used to integrate all fuzzy sets to the used fuzzy measure space. Therefore, requires a fuzzy measure for representing the fuzzy integral, which is obtained through fuzzy rules. Choquet's fuzzy integral is an output of these rules [30]. In this technique, the secret image is first defined as an 8-bit length binary sequence. This binary sequence is shuffled using a chaotic (logistic) map. Afterward, the shuffled image is encoded using DNA complementary rules (by replacing 01 with A, 10 with T, 00 with G, and 11 with C). From this encoded image, four images are extracted, and each image is divided into four blocks. Then each block is diffused using a random sequence generated with the help of Choquet's fuzzy integral (in which initial conditions depends on external key and secret image to enhance security level), followed by Discrete Wavelet Transformation (DWT) based fusion of each of four encrypted image for the production of final encrypted image. For robustness of steganography technique, this encrypted image can be hidden in multiple cover images. This can be done by dividing the encrypted image into a number of images, then each image is embedded in distinct cover files by using any traditional method.

Analysis of chaotic systems used for cryptography and image steganographyis shown in table 1.

Table 1. Chaos Theory in Cryptography and Steganography Analysis

Referred paper	Form of data	Is Chaos System used in encryption	Chaos system used in encryption	Is Chaos System used in embedding	Chaos system used to guide embedding positions	Are Fuzzy Logics used in proposed work	Use of Fuzzy Logics	Embedding Technique used in proposed work
Khalil et al. [31]	Image, Audio, Text	No	_	Yes	Sine-cosine chaotic map [32]	No	_	LSB

Akram et al. [33]	Image	Yes	Modified tent map	No	_	Yes	To modify chaotic map	_
Badar et al. [34]	Image	Yes	Lorenz Chaotic System	No	_	No	_	LSB
Rubaie et al. [3]	Image	Yes	1D SCS [35] 2D LSCM [36]	Yes	1D CP [37]	No	_	LSB
Abdelhakm et al. [38]	Image	Yes	Logistic Map	Yes	Piecewise logistic-sine chaotic map	No	_	LSB
Tayel et al. [11]	Image	Yes	Logistic Map	No	_	Yes	Fuzzy Logic Compressor and Fuzzy logic decompressor	LSB
Vanmathi et al. [7]	Image, Text	Yes	Bernoulli Map	No	_	Yes	To find edges to hide secret encrypted message	LSB
Sharif et al. [8]	Text	No	_	Yes	3D LCA Map	No	_	LSB
Saidi et al. [20]	Image	No	_	Yes	Piecewise linear chaotic map	No	_	DCT
Ghebleh et al. [39]	Image	No	_	Yes	3D cat map	No	_	Lifted DWT

3. Evaluation Parameters

3.1 Methods to analyze chaotic behavior of generated sequences

3.1.1 Lyapunov Exponent

A tool to measure sensitivity to initial conditions (determines how two initials diverge with time to go through available space) and chaos behavior of a dynamical system. If F describes a dynamical system, then Lyapunov exponent, say L, is given as

$$L = \lim_{m\to\infty} \frac{1}{m} \sum_{j=1}^{m} \log |F'(t_j)|$$

where t_j are the outputs (paths) generated by dynamical system and $F'(x)$is derivative of F(x). Observations based on value of L:

I. If L < 0, then system is not chaotic.

II. If L = 0, then the system is stable.

III. If L > 0, then the system reflects chaotic behavior [10].

3.1.2 Poincaré Section

A technique to identify periodic and chaotic behavior of a dynamical system by analyzing a proper subspace of available space. A dynamical system has chaotic behavior when system has a collection of dense points which are characterized by fractal structure.

3.1.3 0-1 Test

A map is chaotic if the discrete path given by generated sequence is Brownian, otherwise the system will be regular.

3.2 Methods to Analyze Performance of Encrypted Image

3.2.1 Histogram analysis

In images, histogram is a chart showing distribution of pixels [40]. Histogram of the encrypted image should have almost equally distributed pixels values [41].

3.2.2 Correlation analysis

In images, correlation is the statistical measure of association of two adjacent pixels. Correlation coefficient ρ is defined as the ratio of covariance of two variables to product of variances of the two variables, and also $-1 \leq \rho \leq 1$. If the magnitude of the correlation coefficient is near to 1, then adjacent pixels are highly correlated, and if it is near to 0, then it directs that adjacent pixels are unrelated.In image encryption , ρ should be near to 0 so that it leads difficulty to recognise pattern of original image and original image can't be recovered by unauthorised interference.

3.2.3 Information entropy

Entropy, introduced by Claude Shannon measures how uncertain or random pixels of an image are. Entropy is mathematically calculated as

$$H(K) = -\frac{\sum_{i=1}^{i=2^k} P(k_i) log P(k_i)}{log 2}$$

Where [0, k-1] is is the intensity level of the original k-bit image [40]. Low wntropy value leads pattern recogniton in encrypted image readily while high entropy value leads hign randomness present in encrypted image.

3.3 Methods to Analyze Performance of Steganographic Techniques

3.3.1 MSE

Mean Square error is a measurement, to measure the accuracy of a steganographic method and distortion in image. The mathematical equation to compute MSE [42] (quantifies the difference matrix of cover and stego image matrix) is given as

$$MSE = \frac{1}{r \times s} \sum_{\substack{i=1 \\ j=1}}^{\substack{i=r \\ j=s}} (c_{ij} - s_{ij})$$

where cover image is of size $r \times s$, c_{ij} and s_{ij} are pixels of cover and stego image respectively.

3.3.2 PSNR

Peak Signal to Noise Ratio is used to measure quality of stego mage measured in decibels, calculated as [42]

$$PSNR = \log_{10} \frac{p^2}{MSE} \times 10$$

where p is peak signal level for an image, i.e., maximum numerical pixel value. A stego image with PSNR 30 dB or more is considered of good quality. A stego image with low MSE value will have high PSNR.

3.3.3 SSIM

Structural similarity index is a tool to assess imperceptibility quality of stego image and also a mathematical equation is in literature to compute SSIM for gray scale image [43] and color image [17].

3.3.4 NAE

Normalized Absolute Error is used to measure the distortion between cover and stego images calculated as [21]

$$NAE = \frac{\sum_{\substack{i=1 \\ j=1}}^{\substack{i=r \\ j=s}} (c_{ij} - s_{ij})}{\sum_{\substack{i=1 \\ j=1}}^{\substack{i=r \\ j=s}} |c_{ij}|}$$

where cover image is of size $r \times s$, c_{ij} and s_{ij} are pixels of cover and stego image respectively. Low NAE leads a stego image with high invisibility, even NAE should be near to zero.

Histogram Ananlysis and Entropy Analysis also used to analyse quality of stego image. To have a stego image of good quality, there should not be significant difference in histograms of cover and stego image and stego image should have low entropy value to avoid randomness in stego image.

4. Conclusion

This survey paper presents chaos based cryptography and steganography techniques to increase security level. For robustness, chaos method based encryption techniques are used in image steganography and embedding is done by any of traditional methods based on spatial and transform domain. Fuzzy logic based algorithm can be used in data embedding, image compression etc. to increase hiding capacity. Multiple chaotic maps can also be combined to obtain a new map which is able to generate pseudo random sequence. Application of Chaotic theory is not only in encryption, but it is used to address pixels where secret message bits can be embedded. By using fuzzy logics and chaotic methods, high imperceptibility, high payload and high security level of steganographic techniques can be ensured.

References

[1] Hussain, M., Wahab, A.W.A., Idris, Y.I.B., Hoc, A.T.S., Jung, K.H. (2018). Image steganography in spatial domain: A survey. , Signal Processing: Image Communication, Elsevier, 65, 46-66.https://doi.org/10.1016/j.image.2018.03.012

[2] Chuck Easttom, Modern Cryptography Applied Mathematics for Encryption and Information Security, Second Edition. https://doi.org/10.1007/978-3-031-12304-7

[3] Rubaie, S.F.S.A., Azawi, M.K.M.A. (2023). High capacity double precision image steganography based on chaotic maps. Bulletin of Electrical Engineering and Informatics, 13(1), 320-331. DOI: 10.11591/eei.v13i1.6055

[4] Nagpal, K.D., Dabhade, D. S. (2015). A Survey on Image Steganography & its Techniques in Spatial & Frequency Domain. International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, 3(2), 776-779.

[5] Sahu, A. K., Sahu, M. (2020). Digital image steganography and steganalysis: a journey of the past three decades. Open Computer Science, 10(1), 296-342. DOI:10.1515/comp-2020-0136

[6] Kour, J., Verma, D. (2014). Steganography Techniques - A Review Paper. International Journal of Emerging Research in Management & Technology ISSN: 2278-9359, 3(5), 132-135.

[7] Vanmathi, C., Prabu, S. (2017). Image Steganography Using Fuzzy Logic and Chaotic for Large Payload and High Imperceptibility. International Journal of Fuzzy Systems. https://doi.org/10.1007/%40815-017-0420-0

[8] Sharif, A., Mollaeefar, M., Nazari, M. (2017). A novel method for digital image steganography based on a new three-dimensional chaotic map. Multimedia Tools and Applications, 76, 7849-7867, 7849-7867. DOI 10.1007/s11042-016-3398-y

[9] Mfungo, D.E., Fu, X., Xian Y., Wang, X. (2023). A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information.Applied Sciences, 13, 7113. https://doi.org/10.3390/app13127113

[10] Xian, Y., Ma, R., Liu, P., Zhou, L. (2023).Image Encryption Scheme Based on New 1D Chaotic System.Digital Forensics and Watermarking - 22nd International Workshop, IWDW 2023, 3-17. https://doi.org/10.1007/978-981-97-2585-41

[11] Tayel, M., Shawky, H., Hafez, A.E.D.S., (2013). A Hybrid Chaos- Fuzzy - Threshold Steganography Algorithm for Hiding Secure Data. Transactions on Advanced Communications Technology (TACT) , 2 (1), 156-161.

[12] Alwan, H.H., Hussain Z.M. (2023). A Multiplicative-Additive Chaotic-Address Steganography. Journal of Kufa for Mathematics and Computer, 7(2), 16-25. DOI:http://dx.doi.org/10.31642/JoKMC/2018/070204

[13] Kadhim, O. N., Hussain, Z. M.(2018).Information Hiding using Chaotic- Address Steganography. Journal of Computer Science, 14(9), 1247-1266, DOI: https://doi.org/10.3844/jcssp.2018.1247.1266

[14] Elkamchouchi, H., Salama, W. M., Abouelseoud, Y., (2017).Data hiding in a digital cover image using chaotic maps and LSB technique. 12th International Conference on Computer Engineering and Systems (ICCES).DOI: 10.1109/ICCES.2017.8275302

[15] Nazari, M., Ahmadi, I.D. (2019).A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity. Multimedia Tools and Applications, 79, 13693-13724. https://doi.org/10.1007/s11042-019-08415-1

[16] Yadav, P., Dutta, M., (2017). A overview of various steganographic domains and its applications. International Journal of Engineering Trends and Technology (IJETT), 52(3), 137-141. ISSN: 2231-5381

[17] Setiadi, D. R. I. M. (2020). PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimedia Tools and Applications, 80, 8423–8444. https://doi.org/10.1007/s11042-020-10035-z

[18] Goel, S., Rana, A., Kaur, M. (2013). A Review of Comparison Techniques of Image Steganography. IOSR Journal of Electrical and Electronics Engineering, 6(1), 41-48. DOI:10.9790/1676-0614148

[19] Gunjal, M., Jha, J. (2014). Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm. International Journal of Computer Trends and Technology (IJCTT), 11(4), Page144-150. ISSN: 2231-2803

[20] Saidi, M., Hermassi, H., Rhouma, R., Belghith, S. (2017). A new adaptive image steganography scheme based on DCT and chaotic map. Multimedia Tools and Applications, 76(11), 13493-13510. DOI:10.1007/s11042-016-3722-6

[21] Wang, W., Liu, X., Lu, M., Liu, J., Jiang, P. (2022). Intelligent Fuzzy Approach Based High Performance Steganography in Wavelet Domain. Automatic Control and Computer Sciences, 56, 189–197.

[22] Zhang, Y.Q., Zhong, K., Wang, X.Y. (2022). High Capacity Image Steganography based on Discrete Hadamard Transform. IEEE Access, 10, 65141-65155. DOI: 10.1109/ACCESS.2022.3181179

[23] Shafi, I., Noman, M., Gohar, M., Ahmad, A., Khan, M., Din, S., Ahmad S. H., Ahmad, J. (2017). An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment. Soft Computing, 22, 1555–1567. https://link.springer.com/article/10.1007/s00500-017-2944-5

[24] Melman, A., Evsutin, O. (2023). Comparative study of metaheuristic optimization algorithms for image steganography based on discrete fourier transform domain. Applied Soft Computing, 132, Issue C. https://doi.org/10.1016/j.asoc.2022.109847

[25] Ker, A.D.(2005). Steganalysis of LSB Matching in Grayscale Images. IEEE signal processing letters, 12(6), 441-444.DOI: 10.1109/LSP.2005.847889

[26] Hiary, H., Sabri, K.E., Mohammed M.S., AlDhamari, A. (2016). A Hybrid Steganography System based on LSB Matching and Replacement. (IJACSA) International Journal of Advanced Computer Science and Applications,7(9). DOI: 10.14569/IJACSA.2016.070951

[27] Sabery, K.M., Yaghoobi, M. (2008). A Simple and Robust Approach for Image Hiding using Chaotic Logistic Map. In Advanced Computer Theory and Engineering, 2008 ICACTE'08. International Conference on IEEE, 623–627.

[28] Gasimov, V. A., Mammadov, J. I. (2020). DNA-based image encryption algorithm. IOP Conference Series: Materials Science and Engineering. doi:10.1088/1757-899X/734/1/012162

[29] Panduranga, H.T., Kumar, S.K.N., Kiran (2014). Image Encryption based on Permutation Substitution using Chaotic Map and Latin Square Image Cipher. The European Physical Journal. DOI:10.1140/epjst/e2014-02119-9

[30] El-Khamy, S.E., Korany, N.O., Mohamed, A.G. (2020).A new Fuzzy-DNA Image Encryption and Steganography Technique. IEEE Access, 8(99).DOI: 10.1109/ACCESS.2020.3015687

[31] Khalil, N., Sarhan, A,. Alshewimy, M.A.M. (2024). A secure image steganography based on LSB technique and 2D chaotic maps. Computers and Electrical Engineering, 119, 109566. https://doi.org/10.1016/j.compeleceng.2024.109566

[32] Khalil, N., Sarhan, A,. Alshewimy, M.A.M. (2021). An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. Optics & Laser Technology, 143(3), 107326. DOI:10.1016/j.optlastec.2021.107326

[33] Akraam, M., Rashid, T., Zafar, S. (2022). An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers. Multimedia Tools and Applications, 82(6). DOI:10.1007/s11042-022-13941-6

[34] Bader, A.S., Mohammed, K. A., Jasem, F. M., Sagheer, A. M. (2024). Image Steganography Technique based on Lorenz Chaotic System and Bloom Filter. International Journal of Computing and Digital Systems, 15(1). DOI:10.12785/ijcds/160161

[35] Wang, X., Liu, P. (2020). A New Image Encryption Scheme Based on a Novel One-Dimensional Chaotic System. IEEE Access, 8, 174463-174479. DOI: 10.1109/ACCESS.2020.3024869.

[36] Huang, H. (2019). Novel Scheme for Image Encryption Combining 2D Logistic – Sine - Cosine Map and Double Random – Phase Encoding. IEEE Access, 7, 177988-177996. Doi:10.1109/ACCESS.2019.2958319.

[37] Talhaoui, M. Z., Wang, X., Midoun, M. A. (2021). A new one - dimensional cosine polynomial chaotic map and its use in image encryption. The Visual Computer, 37(3), 541 – 551. doi: 10.1007/s00371-020-01822-8.

[38] Abdelhakm, M., Salah, A., Askar, S., Abouhawwash, M., Karawia, A., A. (2024). An image steganography algorithm via a compression and chaotic maps. AIP Advances, 14, 045236. doi: 10.1063/5.0202343

[39] Ghebleh, M., Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898-1907. https://doi.org/10.1016/j.cnsns.2013.10.014

[40] Gonzalez, R.C., Woods, R.E. (2016). Digital Image Processing (3). Pearson Education India, ISBN 978-9332570320 DOI: 10.4236/ijg.2014.55050.

[41] Aparna, H., Madhumitha, J. (2023). Combined image encryption and steganography technique for enhanced security using multiple chaotic maps. Computers and Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2023.108824.

[42] Bandyopadhyay, D., Dasgupta, K., Mandal, J. K., Dutta, P. (2014). A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1). DOI : 10.5121/ijsptm.2014.3102

[43] Nagarajegowda, S., Krishnan, K. (2024). An adaptive approach for multi-media steganography using improved chaotic map and discrete cosine transform. Signal, Image and Video Processing. https://doi.org/10.1007/s11760-024-03345-4