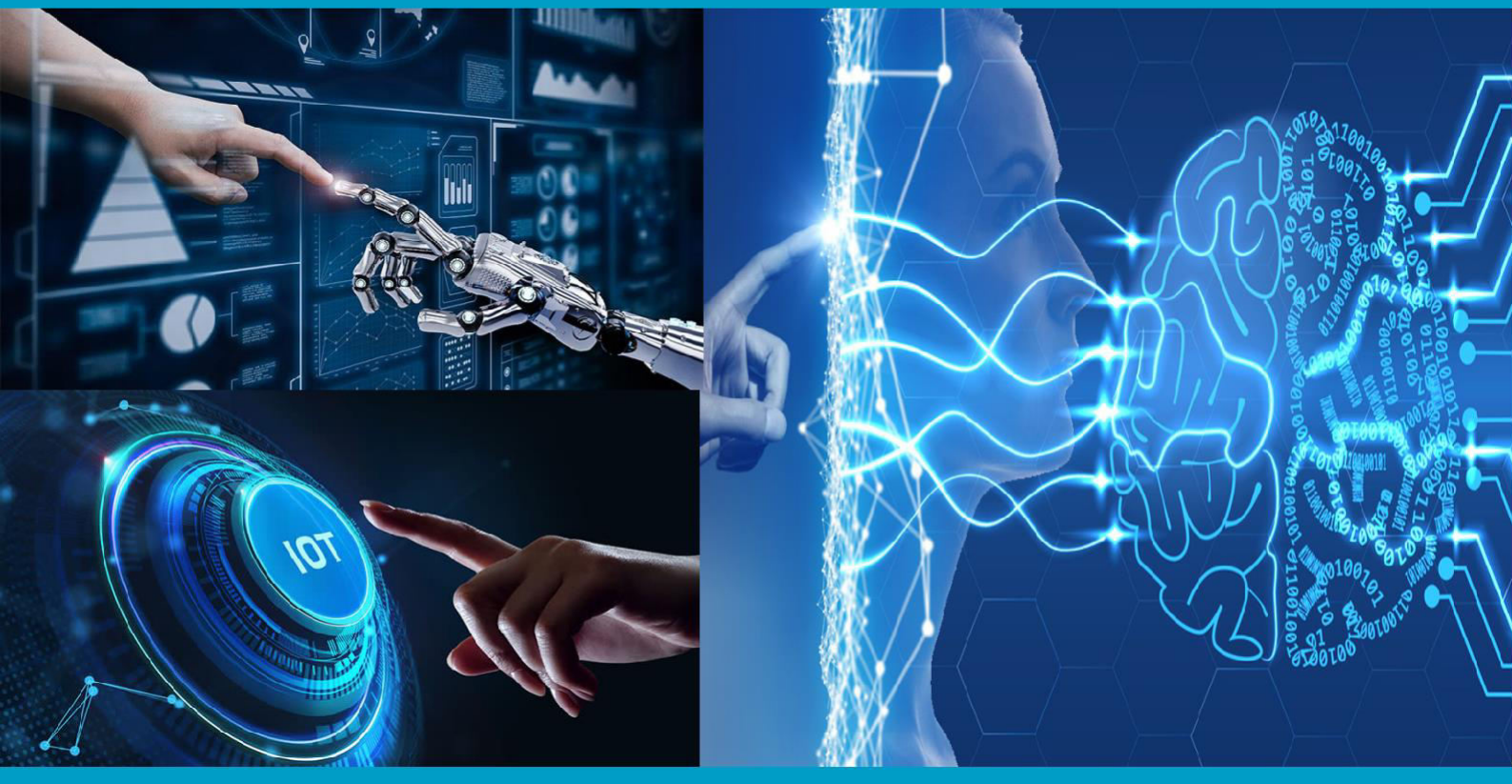
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 10, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

Information Security Using Image Encryption Methods: Recent Trends and Challenges

[1]Shakuntala Bindiya and [2]Vivek Kumar Sinha

[1]M. Tech Student, Dept. of CSE, Raipur Institute of Technology, Raipur, Chhattisgarh, India

[2]Assistant Professor, Dept. of CSE, Raipur Institute of Technology, Raipur, Chhattisgarh, India

ABSTRACT: Cryptographic algorithms are used for image encryption and decryption in the field of image security. Security has gained a lot of importance as information technology is widely used. Since the digital image has become an important medium of communication, researchers have come up with different techniques from time to time to ensure the security of the images. Cryptography refers to the mathematical methods study as well as associated aspects of data secrecy such as data confidentiality, along with high data Integrity as well as data authentication. In this article, the author's recent trends and challenges in information security using image encryption methods. Encryption is an approach of hiding distinct important information therefore on prevents unauthorized access and guaranteeingthe confidentiality of information. Such privacy requirements may be greatly assisted by cryptography including steganography, which also adds a level of verification. The study of steganography entails conveying sensitive information in a suitable multimedia provider, such as pictures, audio, as well as video clips. The image processing is hiding the information in images.

KEYWORDS: AES, DES, Image Processing, Information Security, Image Encryption, LSB, Visual Cryptography.

I.INTRODUCTION

Image processing is a technique to perform an algorithmic strategy to signal an image in a multidimensional systematic way. Cryptography is the technology to encrypt or decrypt any kind of digital signal or data for ensuring a more secure way to transmit or receive data over any security-based applications. Steganography is the more conservative technology to hide any secret information within an image. The given data is embedded into an image to hide its data. Visual Cryptography is the art of work made from a formal cryptography scheme by dividing any text-based information into N subsequent image frames [1], [2]. Well-known as well as frequently employed methods for manipulating data (messages) to cipher or conceal their presence include cryptography as well as steganography. Such approaches are employed to safeguard electronic-mail communications, credit card data, as well as other things in computer science along with various relevant subjects[3].

Electronic pictures have been employed in several applications, including healthcare scans, and surveillance, including secret meetings, as a result of technological improvements. Such pictures can include private as well as delicate data in them. Such photos are vulnerable to risks like alteration as well as unauthorized accessibility when sent over publicly accessible networks. Problems with freedom of action, and national safety, especially the armed forces might come up as a result of the disclosure of highly classified data. Additionally, people's security must be ensured whenever they are interested in sharing photographs across an open network. Pictures must thus be protected across a variety of safety threats [4].Figure 1 illustrates the image encryption methods classifications.This had been discovered through scientific research that picture methods of encryption are capable of being used to secure such photos. Through the use of a hidden key, picture encrypting transforms a plain picture into a password-protected one. Through the use of the encryption key, this decryption procedure converts the cipher picture back to the real picture.Figure 2 illustrates the common terms used in image encryption [5].

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

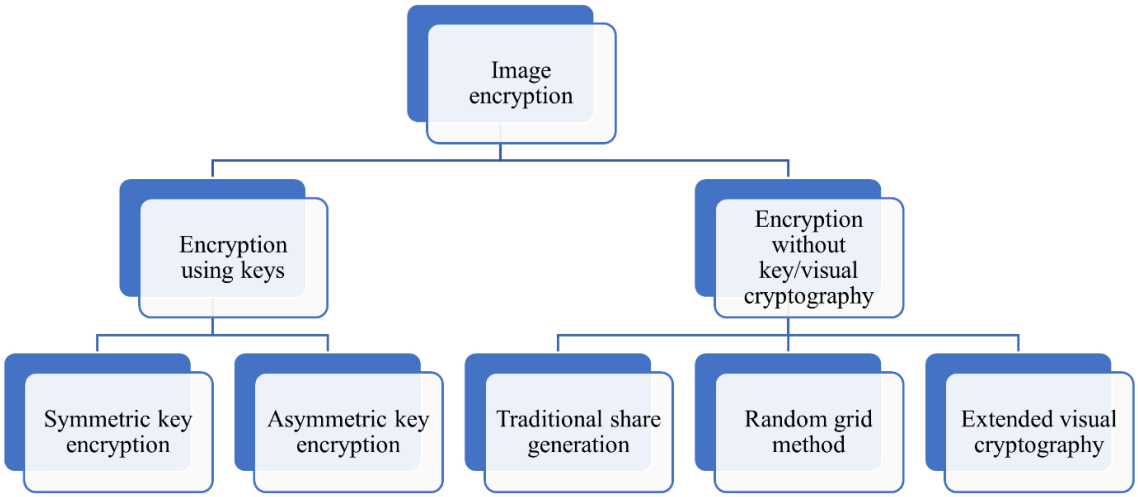


Figure 1: Illustrates the image encryption methods classifications.

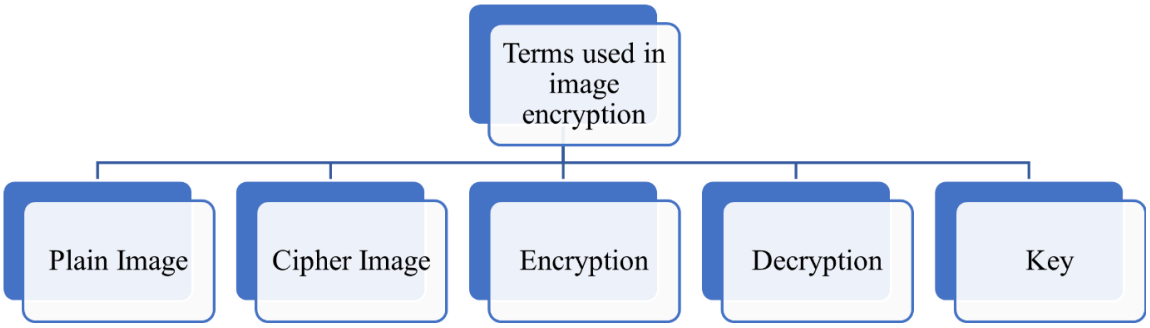


Figure 2: Illustrates the common terms used in image encryption.

The sole method to ensure privacy will be to keep attackers from learning that sensitive data is present during the entire transaction. Several methods have been investigated to do so like digital watermarking, and visual cryptography was used before image steganography [6].

There are various methods for data hiding like the spatial domain, frequency domain, and compressed data domain.

In spatial domain: in this, the picture pixels within the spatial domain are arranged to incorporate the data to be embedded. This method is very simple to implement in realtime. It offers a higher-level hiding capability. The image quality in which the data embedding is done may be effectively managed.

Frequency domain data hiding: Within this method all the pictures are initially converted in the frequency domain, as well as further information is incorporated by altering the converted coefficients of the frequency domain.

Encrypting Phases: AES algorithm is used to encrypt the message. The AES has three fixed 128-bits block ciphers along with cryptographic code dimensions of 128-bits, 192-bits as well as 256-bits size. The employed keylength is adopted limitless, wherein the block length maximal opted 256-bits. Advance Encryption Standard is a symmetric cipher that uses an algorithm that starts with a random number, in which both the key-length as well as data are encrypted and then scrambled through four rounds of mathematical processes and the key-length that is used to encrypt the message must also be used to decrypt [7]. Figure 3 illustrates the existing approach to image encryption and decryption.Figure 4 illustrates the conventional encryption method of an image using the AES algorithm.

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

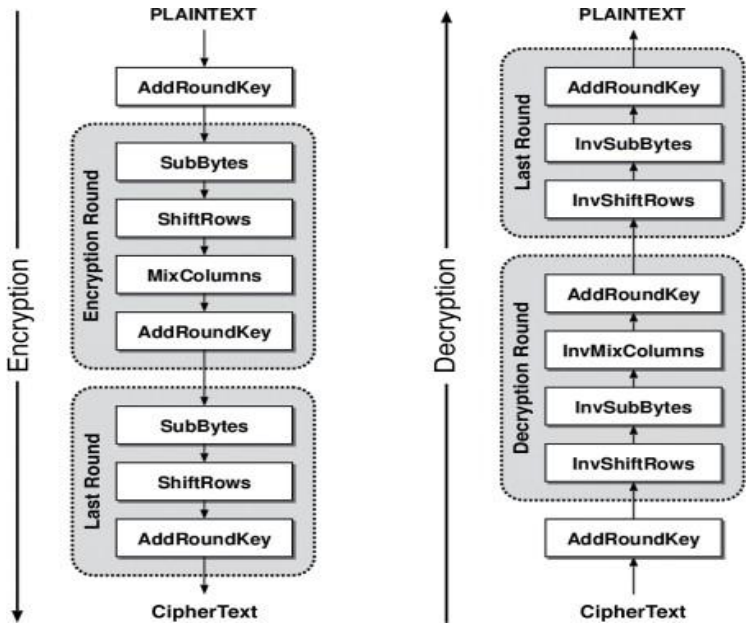


Figure 3: Illustrates the existing approach of image encryption and decryption.

Figure 4: Illustrates the conventional encryption method of an image using the AES algorithm.

The four rounds are called:

1.Sub Bytes: In this method a nonlinear substitution phase wherein, every byte is to be altered along with another following the lookup table.

2.Shift Rows: In this method, a transposition phase is to be performed wherein every row of state has been altered in a cycle at multiple times.

3.Mix column: a mixing operation that operates on the columns of the state, combining the four bytes in each column.

4.Add Round key: In this method, every byte of state has been merged along with the round-keys; every round-key is derived through the unique cipher-keys utilizing a specific key schedule.

Embedding Phase: In the Embedding phase the encrypted message is embedded into a part of the secret image therefore cipher text that is given as input in the text editor is hidden in the cipher. Hiding cipher text inside the image is done using the LSB Steganographic algorithm. In this, each bit of the cipher text is exchanged with the last bit of each pixel Value. For each Pixel the last bit is replaced with the consecutive bits of the cipher text [8].

Hiding Phase: Image steganography is performed in this phase. Kekre's Median Codebook Generation Algorithm (KNCG) is used for image steganography. KNCG technique is very faster in comparison to several codebook generation protocols.

LSB:

The greatest common as well as a straightforward method for dealing along-with pictures, it substitutes the wrap object's LSB alongside hidden texts, resulting in higher incorporating capacity as well as minimal computational hardship. Because

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

this LSB modulation has a small impact on human perception, the resulting stego-picture would appear to the vision to be identical to the wrapped picture, allowing for higher level perceptual accountability of LSB [9].

Furthermore considering the picture four distinct pixels with respective binary formats as follows:

123 = 01111011

100 = 01100100

120 = 01111000

99 = 01011010

Whenever, a secured picture (14 number), in which binary depiction is considered 1110, is to be incorporated in LSB of this part of the image, then a significant stego object is described as follows:

01111011 =123

01100101 =101

01111001 =121

01011010 =99

These LSB bits which have been altered and later incorporated have been emphasized

II.LITERATURE REVIEW

There are several picture encryption techniques currently being developed. Scholars have employed a variety of principles throughout history to improve the integrity of photographs. Considering the instance of photos, conventional methods like DES (Data Encryption Standard), as well as AES (Advanced Encryption Standard), along with IDEA are no longer applicable [10]. Plenty of picture encryption techniques have come into existence in recent years because photographs possess distinctive characteristics from written content [10]. However, for such investigation, we concentrated solely on techniques used within the previous ten years (2012–2022), since we have discovered the utilization of a variety of notions within the field of information safety [11].

Several picture encryption techniques have been developed at this point. Following an examination of the literary works, we categorizethem according to various categories, including methods for picture encryption that utilizes spatial, transform, as well as optical, along with compressive sensing [12]. The confidential information is scrambled as well as transformed into an unintelligible format using encryption. Both conventional methods of encryption, as well as Chaos-rooted methods, may be used for security. several format encryption methods (SET), which include the Rivest Shamir Adleman algorithms (RSA) [13], AES [14], as well as DES [15]. The aforementioned techniques secure the essential information before inserting it using a private password. The biggest drawback of existing methods, which renders them insecure as well as less dependable for encrypting information, is the volume of information with key sizes [16]. Traditional chaos-rooted encryption techniques have solved the SETs' limitations. The previously chaos-rooted encryption method employs initial passwords for cryptography which are responsive to modifications. Therefore, the chaos-rooted methods of encrypting utilize greater safeguard cryptographic techniques to guarantee information protection [17].

Chaos has become a type of complicated stochastic phenomenon that is created through predictable nonlinear systems. Numerous aspects of both the human community, as well as natural processes, are chaotic. Because of the identification of chaostheory within nonlinear systems, this investigation of chaos received significant consideration from academics across a wide range of disciplines as well as has established itself as a single fundamental area of nonlinear empirical evidence [18]. The attributes necessary through encryption, including the quasi-randomness of chaos-signals, extreme reactivity to initial circumstances as well as variables settings, system, as well as extremely complicated nonlinear behavior, are very identical to features associated with chaotic-signals [19]. Because of this, chaotic solutions are now frequently employed to create cryptography systems. Chaos-based cryptography provides clear benefits for picture encryption, as well as this is now the principal use for chaos-based methods [20].

Furthermore, certain research [21], [22] supported the idea that discrete systems tend to be greater complicated than ongoing ones. As a result, numerous scholars have gotten interested in creating an effective 1-dimensional discrete chaos-based system framework, while various picture encryption techniques centered around such a framework were presented. In

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

reference [23], P. Rashmi et al. put out a logistic map-based streaming-encryption technique for mobile body-based networking.

Another sensitive dynamical reciprocal encryption of images technique was presented by M. Maazouz et al. [24] employing a unique 1-dimensional chaos-based system rooted in the ratio of cosine-function over sine-function. A picture security method employing a novel hybrid electronic chaotic structure was presented by Tao Li et al. [25]. An innovative picture method for encryption was presented by H. G. Mohamed et al. [26] utilizing a one-dimensional sinusoidal-polynomial compound chaos system. Another unique picture method of encryption that utilizes a group of one-dimensional cubic maps of chaos was suggested by H. Y. Liu et al. [27].

III.DISCUSSION

To familiarise readers with the different encryption methods utilized in encoding picture that was originally carried over the internet, several significant encryption approaches are laid out as well as analyzed in this study. The findings demonstrate that each method offers benefits as well as drawbacks depending on how its approaches are put into practice to photos. We conclude that all methods of picture encrypting are effective as well as provide safety to ensure nobody can view a picture that exists on a public network.Figure 5 illustrates the information security methods classification.

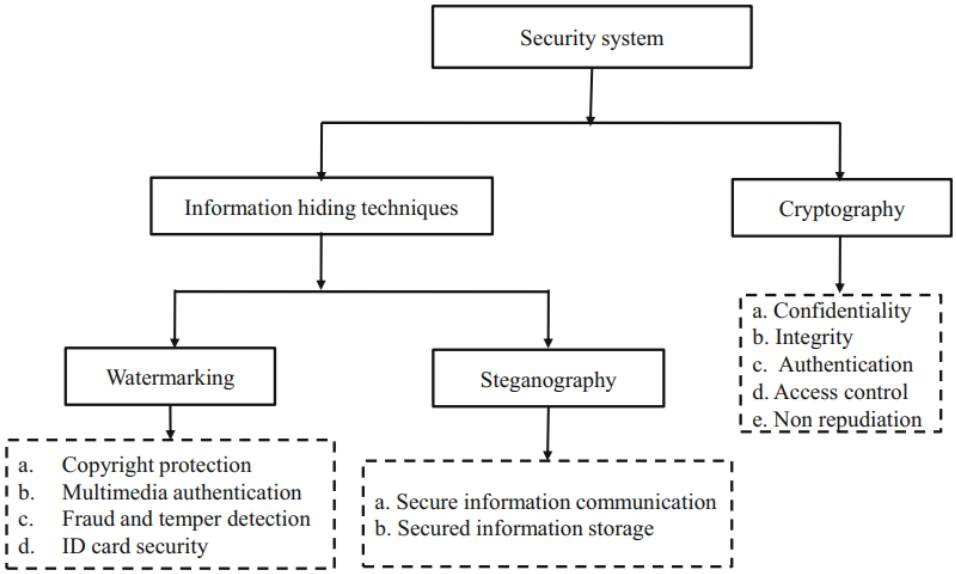


Figure 5: Illustrates information security methods classification [28].

The World Wide Web as well as electronic technological advancements over the past decade have made it easier to use audiovisual items to facilitate information exchange. Nevertheless, several privacy concerns with sharing data over the World Wide Web must be resolved [29]–[31]. Scientists are paying a lot of focus to photographic steganography for safeguarding information. This information is protected using picture steganography, which embeds information bits covertly into a picture's pixels having a low discovery likelihood. Furthermore, encrypting information before incorporating offers two levels of safeguarding from unauthorized access [32], [33]. To date, several steganography along with cryptographic techniques are being created to guarantee the security of information while it is being transmitted across an internet connection. The objective of the aforementioned study is to briefly examine current developments in safeguarding data using image encryption techniques to provide multiple layers of protection for secret exchanges [34], [35]. This research discusses the benefits including drawbacks of the crypto-steganography technologies including picture steganography technologies currently in use. The article also provides a thorough explanation of certain frequently used assessment factors for both steganography as well as cryptography techniques [36]–[38]. In general, the goal of this research is to gain a proper knowledge of photographic steganography as well as how it may be combined with image encryption techniques to produce cutting-edge double-layered protection crypto-stego solutions [39], [40].Figure 6 illustrates an existing Steganography method along with Cryptography.

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

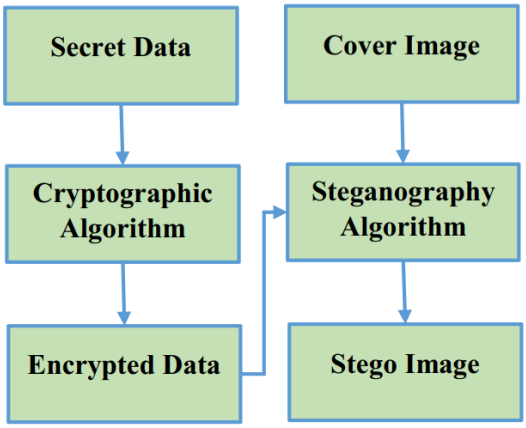


Figure 6: Illustrates an existing Steganography method along with Cryptography [1].

IV.CONCLUSION

It is possible to draw the conclusion that whenever typical picture security methods including steganography as well as enhancing processes are used, it makes it impossible for investigators to decipher the digitally encoded hidden information. Without knowing the correct code, this is challenging to interpret the crucial information as well as decode the ciphered message. This review article presents a comprehensive review of information security using image encryption methods.This provides effectiveness for confidential messages, as well as the key's use renders system operation simple and secure. We may further develop this study by employing 3D pictures in this fashion to create allocations that include a portion of a secret as well as expose that secrecy to everyone by stacking. It may be worked along with diverse Doc files as well as text-content files and protect such informational items using picture steganography technology.

REFERENCES

[1] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," *Health and Technology*. 2022. doi: 10.1007/s12553-021-00602-1.

[2] M. A. Al-Fayoumi, A. Odeh, I. Keshta, and A. Ahmad, "Techniques of medical image encryption taxonomy," *Bull. Electr. Eng. Informatics*, 2022, doi: 10.11591/eei.v11i4.3850.

[3] S. A. S. Almola, N. H. Qasim, and H. Ali Abed Alasadi, "Robust Method for Embedding an Image Inside Cover Image Based on Least Significant Bit Steganography," *Inform.*, 2022, doi: 10.31449/inf.v46i9.4362.

[4] S. F. Alqazzaz, G. A. Elsharawy, and H. F. Eid, "Robust 4-D Hyperchaotic DNA Framework for Medical Image Encryption," *Int. J. Comput. Netw. Inf. Secur.*, 2022, doi: 10.5815/ijcnis.2022.02.06.

[5] A. A. Abdallah and A. K. Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi J. Sci.*, 2022, doi: 10.24996/ijs.2022.63.1.31.

[6] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3012912.

[7] L. Anusree and M. A. Rahiman, "A New Highly Secure Optical Image Security Technique Using Gyrator Transform for Image Security-Related Applications," *Int. J. Opt.*, 2022, doi: 10.1155/2022/6165901.

[8] A. A. Neamah, "An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix," *J. King Saud Univ. - Comput. Inf. Sci.*, 2023, doi: 10.1016/j.jksuci.2023.02.014.

[9] K. N. Singh and A. K. Singh, "An Improved Encryption–Compression-based Algorithm for Securing Digital Images," *J. Data Inf. Qual.*, 2022, doi: 10.1145/3532783.

[10] H. Pan, Y. Lei, and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map," *Eurasip J. Image Video Process.*, 2018, doi: 10.1186/s13640-018-0386-3.

[11] W. Jang and S. Y. Lee, "Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment," *Int. J. Distrib. Sens. Networks*, 2020, doi: 10.1177/1550147720914779.

[12] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

level security for internet of things," *Multimed. Tools Appl.*, 2023, doi: 10.1007/s11042-022-12169-8.

[13] S. Gandhi and R. Gor, "DIGITAL IMAGE ENCRYPTION USING RSA AND LFSR," *Int. J. Eng. Sci. Technol.*, 2022, doi: 10.29121/ijoest.v6.i4.2022.351.

[14] P. Shete and S. Kohle, "Image Encryption using AES Algorithm: Study and Evaluation," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2022, doi: 10.22214/ijraset.2022.46619.

[15] S. Kumar and S. Srivastava, "Image Encryption using Simplified Data Encryption Standard (S-DES)," *Int. J. Comput. Appl.*, 2014, doi: 10.5120/18178-9070.

[16] S. Fadhel Hamood, M. S. Mohd Rahim, and O. Farook Mohammado, "Chaos image encryption methods: A survey study," *Bull. Electr. Eng. Informatics*, 2017, doi: 10.11591/eei.v6i1.599.

[17] N. Gupta, R. Vijay, and H. K. Gupta, "Performance analysis of dct based lossy compression method with symmetrical encryption algorithms," *EAI Endorsed Trans. Energy Web*, 2020, doi: 10.4108/EAI.13-7-2018.163976.

[18] A. Siswanto, N. Katuk, and K. R. Ku-Mahamud, "Chaotic-based encryption algorithm using henon and logistic maps for fingerprint template protection," *Int. J. Commun. Networks Inf. Secur.*, 2020, doi: 10.17762/ijcnis.v12i1.4395.

[19] G. Gaur and R. S. Meena, "Secure Transmission of Biometric Scan Images Using Data Encryption Standards(DES) Algorithm," *Comput. Sci. Eng.*, 2012, doi: 10.5923/j.computer.20120205.04.

[20] E. A. Jameel and S. A. Fadhel, "Digital Image Encryption Techniques: Article Review," *Tech. Rom. J. Appl. Sci. Technol.*, 2022, doi: 10.47577/technium.v4i2.6026.

[21] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, 2021, doi: 10.3390/e23030341.

[22] Y. Zhang, "The fast image encryption algorithm based on lifting scheme and chaos," *Inf. Sci. (Ny).*, 2020, doi: 10.1016/j.ins.2020.02.012.

[23] P. Rashmi, M. C. Supriya, and Q. Hua, "Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare," *Secur. Commun. Networks*, 2022, doi: 10.1155/2022/9363377.

[24] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, "FPGA implementation of a chaos-based image encryption algorithm," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022, doi: 10.1016/j.jksuci.2021.12.022.

[25] T. Li, B. Du, and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2966264.

[26] H. G. Mohamed, F. Alrowais, and D. H. Elkamchouchi, "Correcting errors in color image encryption algorithm based on fault tolerance technique," *Electron.*, 2021, doi: 10.3390/electronics10232890.

[27] H. Y. Liu, N. Hua, Y. N. Wang, J. Q. Liang, and H. Y. Ma, "Three dimensional image encryption algorithm based on quantum random walk and multidimensional chaos," *Wuli Xuebao/Acta Phys. Sin.*, 2022, doi: 10.7498/aps.71.20220466.

[28] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Arch. Comput. Methods Eng.*, 2020, doi: 10.1007/s11831-018-9298-8.

[29] M. Hanif, N. Iqbal, F. Ur Rahman, M. A. Khan, T. M. Ghazal, S. Abbas, M. Ahmad, H. Al Hamadi, and C. Y. Yeun, "A Novel Grayscale Image Encryption Scheme Based on the Block-Level Swapping of Pixels and the Chaotic System," *Sensors*, 2022, doi: 10.3390/s22166243.

[30] R. S. Salman, A. K. Farhan, and A. Shakir, "Creation of S-Box based One-Dimensional Chaotic Logistic Map: Colour Image Encryption Approach," *Int. J. Intell. Eng. Syst.*, 2022, doi: 10.22266/ijies2022.1031.33.

[31] Z. Jiang and X. Liu, "Image Encryption Algorithm Based on Discrete Quantum Baker Map and Chen Hyperchaotic System," *Int. J. Theor. Phys.*, 2023, doi: 10.1007/s10773-023-05277-0.

[32] Y. Xian, X. Wang, X. Wang, Q. Li, and X. Yan, "Spiral-Transform-Based Fractal Sorting Matrix for Chaotic Image Encryption," *IEEE Trans. Circuits Syst. I Regul. Pap.*, 2022, doi: 10.1109/TCSI.2022.3172116.

[33] G. Qu, W. Yang, Q. Song, Y. Liu, C. W. Qiu, J. Han, D. P. Tsai, and S. Xiao, "Reprogrammable meta-hologram for optical encryption," *Nat. Commun.*, 2020, doi: 10.1038/s41467-020-19312-9.

[34] Y. Zhang, A. Chen, and W. Chen, "The unified image cryptography algorithm based on finite group," *Expert Syst. Appl.*, 2023, doi: 10.1016/j.eswa.2022.118655.

[35] J. Wu, J. Shi, and T. Li, "A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion," *Entropy*, 2020, doi: 10.3390/e22010005.

[36] M. Alsafyani, F. Alhomayani, H. Alsuwat, and E. Alsuwat, "Face Image Encryption Based on Feature with

| ISSN: 2395-7639|www.ijmrset.com| Impact Factor: 7.580|A Monthly Double-Blind Peer Reviewed Journal|

|| Volume 10, Issue 4, April 2023||

| DOI:10.15680/IJMRSETM.2023.1004039 |

Optimization Using Secure Crypto General Adversarial Neural Network and Optical Chaotic Map," *Sensors*, 2023, doi: 10.3390/s23031415.

[37] Z. Tang, Z. Yin, R. Wang, X. Wang, J. Yang, and J. Cui, "A Double-Layer Image Encryption Scheme Based on Chaotic Maps and DNA Strand Displacement," *J. Chem.*, 2022, doi: 10.1155/2022/3906392.

[38] I. Kim, J. Jang, G. Kim, J. Lee, T. Badloe, J. Mun, and J. Rho, "Pixelated bifunctional metasurface-driven dynamic vectorial holographic color prints for photonic security platform," *Nat. Commun.*, 2021, doi: 10.1038/s41467-021-23814-5.

[39] M. Samiullah, W. Aslam, M. A. Khan, H. M. Alshahrani, H. Mahgoub, A. M. Abdullah, M. I. Ullah, and C. M. Chen, "Rating of Modern Color Image Cryptography: A Next-Generation Computing Perspective," *Wireless Communications and Mobile Computing*. 2022. doi: 10.1155/2022/7277992.

[40] Y. Xian, X. Wang, and L. Teng, "Double Parameters Fractal Sorting Matrix and Its Application in Image Encryption," *IEEE Trans. Circuits Syst. Video Technol.*, 2022, doi: 10.1109/TCSVT.2021.3108767.

BIOGRAPHY

Shakuntala Bindiyais currently pursuing her M.Tech degree in Computer Science and Engineering from Raipur Institute Of Technology affiliated to Chhattisgarh Swami Vivekanand Technical University, Bhilai, Chhattisgarh, India. She has completed Diploma in Computer Science and Engineering from Government girls polytechnic, Bilaspur in 2012. She completed Bachelor of Engineering (B.E.) in Computer Science and Engineering fromGovernment Engineering College Bilaspur in 2015. Her research interest fields are Data Security, Image Processing, and Artificial Intelligence.

Vivek Kumar Sinhais currently working as an Assistant Professor in the Computer Science and Engineering Department at Raipur Institute of Technology, affiliated to Chhattisgarh Swami Vivekanand Technical University, Bhilai, Chhattisgarh, India. He is having 14 years of experience in teaching. He is currently Research Scholar at Lovely Professional University Phagwara, Jalandhar, Punjab, India. He has published 21 research papers in SCI, Scopus and other reputed journals and conferences.

Impact Factor: 7.580

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com