A Brief Review on Modern Image Encryption Techniques

Sanjeet Kumar[1], Dakshita Joshi[2]
Computer science and Engineering Department,
Bansal Institute of Engineering and Technology, Lucknow
Sanjeet.desire@gmail.com

Abstract: Recently, the use of chaos in cryptography has attracted the attention of numerous researchers. Numerous studies have specifically centred on chaotic image encryption. In the field of chaotic image encryption, a thorough survey can shed light on under-researched subjects and identify current trends. In addition to such a review, this study investigates the key difficulties in this area, creates a chaotic image encryption environment, and creates a roadmap for future research in this topic.

Keywords: image encryption, chaos, chaotic encryption, chaotic image encryption, trend analysis.

1. Introduction:

Encryption is the method involved with utilizing a calculation to change data to make it incomprehensible for unapproved clients. The most common way of encoding a picture with the assistance of some encryption calculation is picture encryption. Pictures are a necessary piece of our life. It has become standard to record events through pictures. We use CT outputs and MRI pictures for conclusion of strange side effects. Frequently, patients look for second assessment and face with the issue of keeping up with protection as well as secure transmission of their CT or MRI pictures. In any case, sending and getting pictures has become more straightforward with the creation of innovation and improvement of picture encryption calculations. However, an open stage like the web may not be ok for transmission consistently. Military and clinical pictures can be classified and should be kept out of the range of unapproved clients. Subsequently, there is a requirement for a solid picture sharing technique that guarantees safe picture transmission. Cryptography assumes a significant part in accomplishing this objective. Because of the rising prevalence and need for picture encryption, numerous techniques for the equivalent have been concocted. A portion of these incorporate.

Throughout the last ten years, the utilization of cell phones, the Internet and mixed media innovation has exhibited broad interest. The requirement for clients isn't simply confined to message, yet additionally to share information about the expansive organization, i.e., Music, video and video are in many cases utilized on the telephone. In this way, using pictures and video [10], the requirement for a protected organization has turned into a need. Photos are really being sent and treated electronically with the end goal that the data in the picture are dependent upon change or adjustment by unapproved access [9]. Expanded pictures security is expected to integrate and advance organization foundation. Computerized imaging encryption was one of the solid assurances for picture security and was the subject of exploration. The Image Encryption strategies are characterization in displayed in Fig: 1.

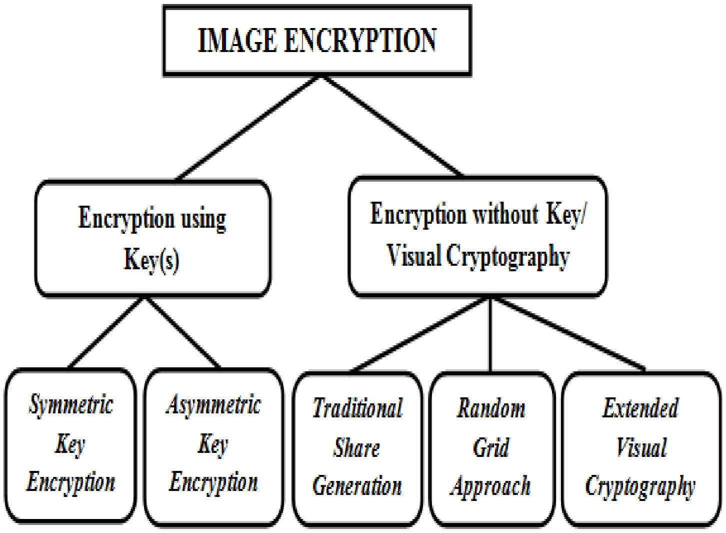
IMAGE ENCRYPTION
Encryption using Key(s)
Encryption without Key/ Visual Cryptography
Symmetric Key Encryption
Asymmetric Key Encryption
Traditional Share Generation
Random Grid Approach
Extended Visual Cryptography

Fig: 1 Image Encryption techniques

Lately, the prerequisite for the sharing or transmission of picture information on the web has added to a lot of interest in picture encryption. Various scientists have additionally presented strategies for picture encryption [6]. Modem cryptography is one strategy that ensures protection, uprightness and validness. Cryptography gives some programming confounded calculations like DES, Concept and RCS, yet they are called complex. be that as it may, they are called complex. Notwithstanding, calculations of chaotic encryption likewise have machine methods thought about solid and most well known over these years, rather than carrying out stream or block cryptosystems [9].

Wherever the presence of turmoil is found, the possibility of the unique design is viewed as the most muddled. Dynamic framework research targets ascertaining the genuine or gradual appearance of the iterative activity. Mayhem is an irregular game which intends that there is no mediation in linearity, which makes arbitrary peculiarity in a specific nonlinearity climate without other arbitrary factors. The muddled framework's creation is profoundly delicate to its underlying circumstances; the future activity of the untidy framework is thusly difficult to anticipate [6].

For multi-recurrence channels, Wavelet change is a disintegration interaction [10]. It indicates the experimental type of time recurrence and multi-goal and is utilized to arrange incomplete time and recurrence area attributes. The feature of the change in the Wavelet is decaying the painting into a sub-picture which offers data of the recurrence and afterward processes the element. Cryptography hash capabilities are a famous device. The hash values made by the message address longer messages themselves. The Fingerprint highlights are utilized as elite execution Hash works that are a passage to getting to the subtleties showing the changelessness and uniqueness of those that supply patient data with mystery and unwavering quality [l] and assume a significant part in checking the legitimacy of the message and its computerized marks [8].

Our goal in this short survey is to give a concise rundown of the items in the previously mentioned papers in a simple way for perusers to comprehend and pick the strategy that best meets individual necessities. We notice every technique momentarily.

2. Related Work:

Another clinical imaging wellbeing and security strategy was presented for Viswanathan P, Venkata Krishna.p [l]. The creator utilized the conventional FED watermarking framework for security purposes. The Fingerprint, Coding and Dual Watermarking System strategy is utilized for getting Teleradiology. The unique finger impression calculation you propose would be utilized to recover the finger impression picture alongside the watermarking of the picture encryption. The fingerprinting calculation offers another strategy for testing and checking the personality of the patient.

In [2] have a cutting edge approach to imparting and sending a picture across the organization. The proposed approach likewise executed a system. A protected organization sharing unique finger impression picture. The reversible secret change is applied to the finger impression picture, alongside halfway straight tumultuous guide. The protected picture is appropriated on the compromised network. The first finger impression picture is reproduced by the converse cycle on the beneficiary hand.

In [3] acquainted a cutting edge arrangement with a tumultuous guide with moving boundaries. The recommended approach has two fundamental highlights: synchronous encoding and message expansion. The technique utilizes a tumultuous deviated tent guide and piece-savvy direct guide to change over broadened messages blocks iteratively into an ASCII code in which boundaries are powerfully altered with the place of the particular message block list and the decimal part is then created which is then flowed to the whole number. The hypothetical assessment and reproduction of the framework's machine uncover a somewhat compelling cycle.

Turbulent casings and wavelet change are important for the proposed stage. The recommended arrangement makes inconsistent groupings by presenting the strategic guide. This alludes to the plaintext being given. The circulated plaintext is then trailed by the change of the wavelet and the problematic issue. The Inverse Wavelet Transform IS was then used to remake the scrambled picture. The calculation testing is completed based on the key review, which guarantees that a little modification of the key might profit from significant changes, a dim level histogram, hostile to commotion test and hostile to cutting tests. The examination showed that pre-encryption dissemination diminished the strength of the vagueness encryption assault. Because of hazardous cryptography, the aftereffect of dispersion is confidential and the impractical highlights of the document might be unraveled. Another computerized watermarking innovation was created by Lina [5]. The writer utilized in the article to lay out intuitive watermarks the idea of particular wavelet change and turmoil. First the discrete wavelet change is applied to the picture, then the low-recurrence part is taken out, and the wreck succession is applied to scramble the little recurrence component. The principal picture is utilized for extraction, and this is a strategy for non-blind acknowledgment. The NC coefficient and high commotion to flag proportion test the gadget (PNSR). The outcomes proposed that the combination of a consolidated specialized visual culture, a clamor assault, a filtration, and so on. The impact of the watermark picture has been very high [6]. For the information encryption strategy, the creator utilized the calculated arrangement of turmoil. The investigation of the calculation happens on the accompanying standards, like arbitrariness, similarity and intricacy. The turmoil grouping reproduction has shown that it fulfills the standards of the encryption calculation.

In [7] presented a technique for the encryption of pictures. The strategy proposed utilizes circumspect tumultuous graphs, which join change and substitute methods. A standard Lena picture confirmed the calculation that showed that the first picture was changed by turbulent series into irregular picture. The activity was successful and sensibly sound.

In [8] has given an imaginative methodology for uniform hash capability translating into propositional rationale recipes. The strategy is applied to the C jargon. The essayists have fabricated a cutting edge way to deal with convey harsh and fulfilling propositional equations and troublesome and fragmented propositional recipes. By utilizing these equations, the difference of various capabilities should be possible and inconveniences can be distinguished.

The encryption of pictures connected to the Baker outline has been improved by [9]. Tragically, techniques for the encryption of photographs have been made and tried to propose that specific keys have produced unfortunate encryption. The calculation has in this way been improved by adding new highlights, for example, changing the importance of grayscale pixels, rendering the pixels by moving and restricting a secret key to the picture to boost the encryption power. The strategy is followed by drawing the pixels and results grayscale meaning.

Picture records are progressively dispersed across the Internet. This conveyance requires security procedures that are not the same as conventional practices to oversee secrecy. The explanation is that pictures can be powerless against a few assaults, especially assuming these records are sent through uncertain channels. Clinical pictures, for instance, contain profoundly delicate information, and in this manner, sending these pictures over the organization requires major areas of strength for a calculation that safeguards against these assaults [16].

As of late, exploring the writing of picture encryption has been important to scientists [17,18]. Additionally, unique related points have been looked into. For instance, a few scientists have directed studies on the methods for scrambling plaintext into pictures through a calculation that works out the RGB esteem [19]. Besides, a few related methods, for example, picture steganography have been concentrated alongside picture encryption [16]. As one more subject of interest, some reviews have zeroed in on the uses of picture encryption in unambiguous regions [20].

Deepa and Sivamangai [22] contended that a malignantly changed clinical picture makes it more hard to analyze a real illness. This raises a basic requirement for the privacy of clinical pictures. Then again, the encryption time can represent a weighty above on the clinical correspondence and handling frameworks. They guaranteed that this tradeoff is best settled by DNA cryptography and tumultuous cryptography. In their audit, they announced a few subjective and quantitative estimations separated from existing important exploration attempts to show how the tradeoff is settled by the referenced advancements. Besides, they laid out certain rules for additional exploration around here.

Yadav and Chaware [23] accept that in spite of existing encryption and data concealing strategies, data can be taken and copyrights can be encroached on account of weaknesses in accessible techniques. They initially introduced a survey of best in class picture encryption techniques. They particularly centered around joint encoding (blunder remedy) encryption techniques. Then, at that point, they proposed an original technique in view of Low-Density Parity-Check (LDPC) code and tumultuous guides fully backed by the Advanced Encryption Standard (AES) and Substitution boxes (S-boxes).

A few existing surveys adopt a near strategy. For instance, the benefits and detriments of existing turbulent picture encryption techniques were thought about in [24]. One more important overview was accounted for in [25], where the creators explored and contrasted somebody layered turbulent guides and a hyper-layered ones concerning their applications in picture encryption. As another model, the creators of [26] featured turbulent encryption as a promising answer for scrambling pictures and recordings, wherein adjoining pixels are exceptionally related. They introduced a survey on existing turbulent strategies for picture encryption determined to recognize the most legitimate tumultuous guide.

They concentrated on tent guide, calculated map, sine map, and so on, and recommended Arnold's feline guide as the most encouraging tumultuous guide for this reason. Also, in [27], the creators explored and looked at picture encryption strategies in view of five customary calculations, in particular Blowfish, RSA, El-Gamal, AES, and DES with some confusion based techniques regarding execution.

Checking on existing AI-helped picture handling strategies has been important to numerous scientists. For instance, a study revealed in [28] zeroed in on the collaborations between AI and binocular sound system for profundity assessment from pictures. Profundity assessment has numerous commonsense purposes in fields like 3D picture recreation and independent driving. Remembered for the numerous procedures for assessing profundity, sound system matching looks at two pictures for pixel difference and uses triangulation to decide the profundity of the pixel. Information driven and learning-based procedures have been applied to sound system matchingwith exceptional achievement, yet the opposite has likewise yielded promising advances in utilizing sound system matchingto foster new strategies in light of profound organizations.

Another pertinent audit concentrated on profound learning-based Multi-Focus Image Fusion (MFIF) techniques [29]. MFIF is a picture handling method for melding different pictures with contrasting profundities of fields to make a solitary in-center picture. Recommendations for taking care of the MFIF issue utilizing profound learning strategies have been developing at a quick rate beginning around 2017, albeit none yet enjoy shown any benefits or execution upgrades over customary techniques. The utilizations of profound learning in picture division were concentrated on in another study [30]. Picture division, the most common way of parceling a picture into at least two sections, has an extensive variety of purpose cases in fields like video reconnaissance, picture pressure, expanded reality, and scene translation. Calculations in light of profound learning models have exhibited extremely great outcomes, frequently beating customary division calculations on numerous well known benchmarks.

Table 1: Summary of literature Survey in Tabular Form.

Year	Ecosystem	Chaotic	Reference
2021	No	No	[17]
2020	No	No	[18]
2020	No	No	[19]
2020	No	No	[32]
2022	No	Yes	[22]
2021	No	Yes	[23]
2021	No	Yes	[25]
2021	No	Yes	[26]
2021	No	No	[28]
2021	No	No	[29]
2021	No	No	[30]

4. Conclusion:

This publication built an ecosystem and provided a thorough overview of the prior research on chaotic picture encryption.

We recognised the difficulties associated with this research area's chaotic, image, and encryption aspects. Some of these problems include choosing between various chaos domains, sources, and dimensions, as well as between block and stream cyphers or symmetric and asymmetric encryption. The results of this survey will aid in laying a solid foundation for future study. While expected trends incline toward quantum and bio-inspired AI, present research trends imply an emphasis on AI and neural networks.

References:

[1] P. Viswanathan, Member, P. Venkata Krishna, "A Joint FED Watermarking System using Spatial Fusion for Verifying the Security issues of Teleradiology", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, pp. 1-12,2013.

[2] Gaurav Bhatnagar and Q. M. Jonathan Wu, "Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission", IEEE TRANSACTIONS ON INSTRUMENT A TION AND MEASUREMENT, VOL. 61, NO.4, pp. 876-887 APRIL 2012.

[3] Yantao Li, Di Xiao, Shaojiang Deng, Qi Han and Gang Zhou, "Parallel Hash function construction based on chaotic maps with changeable parameters", SPRINGER, Neural Computing and Applications, pp. 1305-1312, 17 February 2011.

[4] Runhe Qiu, Y uzhe Fu, Y un Cao, "Image Encryption Research based on chaotic sequences and wavelet stransform", IEEE, pp.1511-1516, 2010.

[5] Qiang Wang, Qun Ding, Zhong Zhang, Lina Ding, "Digital Image Encryption Research Based on DWT and Chaos", IEEE Computer Society Fourth International Conference on Natural Computation, pp. 494-498, 2008.

[6] Gannan Yuan, Research on Data Encryption Technology Based on Chaos Theory", IEEE Computer Society Eighth ACIS International Conference on Sofuvare Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 93-98, 2007.

[7] Guosheng Gu and Guoqiang Han, An Enhanced Chaos Based Image Encryption Algorithm", IEEE Computer Society First International Conference on Innovative Computing, Information and Control, 2006.

[8] Gopal Ghosh et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 993 012062.

[9] Mazleena Salleh Suhariah Ihrahim Ismail Fauzi lsnin, Enhanced Chaotic Image Encryption Algorithm Based on Baker's Map", IEEE, pp. 508-511, 2003.

[10] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[11] T. S. Ali and R. Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map," in IEEE Access, vol. 8, pp. 71974-71992, 2020.

[12] P. Li and K. -T. Lo, "Survey on JPEG compatible joint image compression and encryption algorithms," in IET Signal Processing, vol. 14, no. 8, pp. 475-488, 10 2020.

[13] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," in IEEE Access, vol. 6, pp. 19876-19897, 2018.

[14] A. Umoh, O. N. Iloanusi and U. A. Nnolim, "Image multi-encryption architecture based on hybrid keystream sequence interspersed with Haar discrete wavelet transform," in IET Image Processing, vol. 14, no. 10, pp. 2081-2091, 21 8 2020.

[15] H. Diab, "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations," in IEEE Access, vol. 6, pp. 42227-42244, 2018.

[16]. Dahiya, M.; Kumar, R. “A literature survey on various image encryption & steganography techniques”. In Proceedings of the First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018.

[17]. Makki, Q.H.; Abdalla, A.M.; Tamimi, A.A. A survey of image encryption algorithms. In Proceedings of the International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021.

[18]. Jasra, B.; Moon, A.H. Image encryption techniques: A review. In Proceedings of the 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 29–31 January 2020.

[19]. Abusukhon, A.; AlZu’bi, S. New direction of cryptography: A review on text-to-image encryption algorithms based on rgb color value. In Proceedings of the Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020.

[20]. Pavithra, V.; Jeyamala, C. A survey on the techniques of medical image encryption. In Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 13–15 December 2018.

[21]. Sankpal, P.R.; Vijaya, P.A. Image encryption using chaotic maps: A survey. In Proceedings of the Fifth International Conference on Signal and Image Processing, Bangalore, India, 8–10 January 2014.

[22]. Deepa, N.R.; Sivamangai, N.M. A state-of-art model of encrypting medical image using dna cryptography and hybrid chaos map—2d zaslavaski map: Review. In Proceedings of the 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 21–22 April 2022.

[23]. Yadav, K.; Chaware, T. Review of joint encoding and encryption for image transmission using chaotic map, ldpc and aes encryption. In Proceedings of the 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 7–9 October 2021.

[24]. Suneja, K.; Dua, S.; Dua, M. A review of chaos based image encryption. In Proceedings of the 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019.

[25]. Bu, Y. Overview of image encryption based on chaotic system. In Proceedings of the 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 28–29 January 2021.

[26]. Ayad, J.; Hasan, F.S.; Ali, A.H.; Hussein, Z.K.; Abdulkareem, H.J.; Jalil, M.A.; Ahmed, G.; Sadiq, A. Image encryption using chaotic techniques: A survey study. In Proceedings of the International Conference in Advances in Power, Signal, and Information Technology (APSIT), Bhubaneswar, India, 8–10 October 2021.

[27]. Thein, N.; Nugroho, H.A.; Adji, T.B.; Mustika, I.W. Comparative performance study on ordinary and chaos image encryption schemes. In Proceedings of the International Conference on Advanced Computing and Applications (ACOMP), Ho Chi Minh, Vietnam, 29 November–1 December 2017.

[28]. Poggi, M.; Tosi, F.; Batsos, K.; Mordohai, P.; Mattoccia, S. On the synergies between machine learning and binocular stereo for depth estimation from images: A survey. IEEE Trans. Pattern Anal. Mach. Intell. 2021.

[29]. Zhang, X. Deep learning-based multi-focus image fusion: A survey and a comparative study. IEEE Trans. Pattern Anal. Mach. Intell. 2021. [CrossRef]

[30]. Minaee, S.; Boykov, Y.Y.; Porikli, F.; Plaza, A.J.; Kehtarnavaz, N.; Terzopoulos, D. Image segmentation using deep learning: A survey. IEEE Trans. Pattern Anal. Mach. Intell. 2022, 44, 3523–3542. [CrossRef]

[31]. Su, J.; Kankani, A.; Zajko, G.; Elchouemi, A.; Kurniawan, H. Review of image encryption techniques using neural network for optical security in the healthcare sector-pno system. In Proceedings of the 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, Australia, 25–27 November 2020.

[32]. Kumar, S.; Singh, B.K.; Akshita; Pundir, S.; Batra, S.; Joshi, R. A survey on symmetric and asymmetric key based image encryption. In Proceedings of the International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 28–29 February 2020.