iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.67981

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Transmission Security of Multispectral Images Using Chaotic Maps, Three Dimensional Discrete Wavelet Transform and Secure Hash Algorithm

Shubham Borhade[1], Dr. K. Rajeswari[2]
Department of ComputerEngineering, Pimpri Chinchwad College ofEngineering Pune, India

Abstract: ***A rapidly evolving technological world hasrevolutionized human lives, one such important part of this amazingworld is the internet with almost 330 million terabytes of data generated each day. Most of the images generated are multispectralimages and these images contains sensitive information which can be related to military, medical, research, agricultural etc. domains. So, when these images are transmitted over the network, there is risk of attacks such as Adversarial attacks which can compromise the accuracy of image analysis, another is spatial attacks where alteringthe spatial structure of multispectral images can disrupt the relationships between different spectral bands, leading to inaccuracies in feature extraction and analysis, Noise injection, watermarking attacks etc are some of the attacks normally encountered. Hence, to provide overall security to such multispectralimages is important. This paper proposes various security approaches which can provide confidentiality, Integrity and authenticity to the images.***

Keywords: SHA-256, 3-DWT, Chaotic maps, Watermarking, Hashing, Multispectral images.

I. INTRODUCTION

As a part of the evolving world, the Internet has connected people in more than one way. The best way to send updates regarding particular scenarios is through images, it be spatial or sensitive medical images. The information gained from images has a lot of significant meaning in them, thus loss or leak of such sensitive data can be harmful. Hence, there arises a need of ways to safeguard the images. This paper reviews a way to provide encryption and authentication to multispectral images having various electromagnetic spectrum bands, unlike a traditional colour image.

Image data consumes more storage space than text data and often has high correlation and redundancy between adjacent pixels therefore traditional encryption methods cannot satisfy the demand for image encryption. However, chaos-based systems yield different motion trajectories even if there is a small amount of change in initial conditions. The chaotic mapswith control parameters higher than 3.57 helps in encryption. Maintaining the Authenticity of the image is also crucial due toincrease in piracy attacks. Thus, this survey discusses a robust system which configures to provide encryption authentication and confidentiality to multispectral images.

II. LITERATURE SURVEY

A. *Encryption*

1) In 2020, Zhenlong Man, et al. [1] has proposed anencryption technique that combines a chaotic system with a fingerprint key. The fingerprint coordinate pairis then obtained through the interaction of the encryptor and decryptor fingerprint images. The fingerprint coordinate pair controls the image encryption process, ensuring that the fingerprint image's information is closely linked to the encryption algorithm. To increase scrambling efficiency, it uses brand-new selective scrambling method (SSM) at the same time.

2) In 2019, Essam Abdelwaness, et al. [2] has examined the possibility of using joint encryption compression to safeguard compressed images during their transmission. By spontaneously switching between two coding modes in the entropy coder stage of the CCSDS-123 compression standard, for CCSDS images, two stages are used; prediction stage and entropy coding stage by using an adaptive linear predictive model for good balance in performance andcomplexity, block adaptive encoding uses the Golomb-rice technique on a group of samples.

3) In 2022, Mark McCartney, et al. [3] has discussed typical public key cryptosystems like RSA and El- Gamal may be utilized with chaos-based cryptosystems like Chebyshev polynomials to increase security. The paper summarizes different types of cryptography and edge chaos-based has over other techniques, due to its entropy as well as computational efficiency. Four methods of image encryption spatial, compressive sensing, optical, and transform domains are covered in this work

4) In 2022, Nirmal Chaudhary, et al. [4] has examined the implementation and analysis of block cipher and chaos-based picture encryption methods. In order to assess the effectiveness of each algorithm, the chaotic and AES methods are used to encrypt images. They are then measured using various performance metrics, including peak signal to noise ratio (PSNR), number of pixels change rate (NPCR), unified average changing intensity (UACI) etc. as per the findings. The Arnold cat map outperforms other two but AES is more resistant to statistical attacks due to low PSNR value.
5) In 2020, El-Habib Bensikaddour, et al. [5] has proposed a multispectral image encryption technique based on Fridrich's approach. The acquired experimental findings demonstrate that the suggested technique may achieve a throughput of 120 Mbit/s while having good security, minimal hardware complexity and low power use. A two-dimensional chaotic map, such as the Standard or Cat map is utilized to carry out a complicated substitution between the pixel locations in order to achieve confusion. The Cat map has been chosen for on-board implementation because of its relative simplicity when compared to the other maps.
6) In 2017, Ramkrishna Das, et al. [6] has discussed the Secret Sharing technique, Character Repositioning Technique, Bit Wise Masking and Alternate Sequence(BWMAS) operation, and Image Key Encryption and Text Key Encryption. A combination of four encryption levels has been used. This encryption method encrypts the image key with a user-defined character-positioned text key before using it to encrypt the original picture. The encrypted picture is now separated into N shares, each of which is further encrypted at the encryption end using a different image key. By executing BWM&AS original picture is recovered.
7) In 2021, Chao Chen, et al. [7] has discussed Arnold Transformation using Fractional Logistic Map to encrypt the G and B primary color of matrix of the image. Encrypted R, G and B factors are combined to obtain the encrypted color digital images also the Arnold inverse transform of the provided image is used. When the original R-base image is encrypted, the number of scrambling of the Arnold transform is k, after that, the encrypted R-base color is re-transformed using the T-k Arnold transform, returning the unencrypted R-base color.
8) In 2019, Rui Zhang, et al. [8] has proposed novel permutation comprehensive strategy being used which is good against plaintext attacks to maintain privacy, it hides plain text statistics. The idea revolves around cs- based cipher production with chaotic permutation- substitution encryption as the key to the encryption process, along with a sparse signal that is compressed. The encrypted picture has well-distributed pixel values throughout the range of 0 to 255, indicating a good encryption result.
9) In 2013, Riah Ukur Ginting, et al. [9]has discussed about encryption technique based on the chaotic logistics map and the RC4 stream cipher algorithm. The Technique first converts the external key into an initial value, then it uses the initial value to create a key stream using the chaotic logistic map function. Finally, it processes a permutation, XOR-ing the outcome with a digital picture byte stream. The technique removes statistical correlation between the plain- and cipher-images. It is extremely sensitive to small changes in the key, and has no change in the contents of the image during the encryption and decryption process as the plain image's hash value (MDS) matches the hash value of the cipher image.

B. Water Making

1) In 2014, Lalit Kumar Saini, et al. [10] has discussed analysis of all watermarking techniques, with an emphasis on picture watermarking varieties and their contemporary uses. Various techniques for watermarking included in the paper are DWT, Fingerprinting, and transfer domain techniques. Research also includes properties and applications of watermarking. Threats for watermarking and the Performance evaluation of watermarking algorithms were also studied thoroughly.
2) In 2014, Hussain Nyeem, et al. [11] has discussed formal general paradigm for digital picture watermarking with the goal of facilitating the methodical development of watermarking techniques. The study also defines a range of potential assaults based on the capabilities of the opponent and illustrates several winning scenarios using the model. The research summarizes various attacks on watermarking techniques such as collusion attacks, active attacks, distortion attacks, masking attacks, etc.
3) In 2021, Lei Pei, et al. [12] has introduced the approach for watermarking digital images using singular value decomposition and scrambling. The digital watermark undergoes preprocessing through encryption and dimensionality reduction. The digital watermark picture is integrated into the digital image watermark through the utilization of the sound channel's low-frequency energy ratio technology. Distributed properties of image matrix data are explained, and the visual effect is improved based on the uniqueness of the singular value matrix.
4) In 2015, Payal Kaushal, et al. [13] has provided research on digital watermarking technique, ideas, applications, and contributions. The watermarking system is created with several key considerations, including copyright protection, capacity, security, robustness, etc. Various techniques of image watermarking such as Spatial domain and frequency domain watermarking, DWT, and DCT are studied along with some applications of watermarking in the medical field, telecast industry,

software industry, andcopyright protection, etc.

5) In 2011, Hebah H.O. Nasereddin, et al. [14] has introduced the technology of digital watermarking, a data-hiding method that incorporates a message into a multimedia piece like an image, text, or other digital item. The preservation of digital copyrights is one of the suggested techniques in many significant applications. The study also discusses 3D object watermarking, a new way to digital watermarking, refers to privacy principles of digital watermarking, and applications of watermarking. Briefly studies the attacks on digital watermarks such as State of the art watermarking attacks and estimation-based attacks.
6) In 2020, Mahbuba Begum, et al. [15] reviews current trends in digital image watermarking techniques to identify state-of-the-art methods and their limitations, provides details of standard watermarking system frameworks, and lists some standard requirements such as DWT, DCT, DFT, SVD that are used in designing watermarking techniques for several distinct applications in multiple industries and fields. Some conventional attacks on watermarks such as active, passive, removal, cryptographic, geometric, and protocol attacks are also discussed. The paper also summarizes the state-of-the-art watermarking techniques and includes some threats to watermarking.
7) In 2021, Shweta Wadhera, et al. [16] has discussed the idea of digital picture watermarking with an emphasis on the methods for embedding and extracting the watermark. Additionally, the article covered the latest applications of digital watermarking in the fields of healthcare, distant learning, electronic voting, and the armed forces. The robustness is assessed by looking at how image processing attacks affect the recoverability of the watermark and the signed content.
8) In 2021, Jaspreet Kaur, et al. [17] has provided a prescribed explanation of the fundamentals of digital watermarking, as well as a classification, review, and summary of the various techniques used in the field. The methods and features associated with each of the parameters presented in tabular form. The techniques of watermarking such as DFT, DWT, DCT are studied thoroughly. Mostly used tools Matlab, XSG and Xilinx Vivado are mentioned in this review. Batch and cloud processing in image is implemented.

C. *Hashing*

1) In 2018, Kaimeng Ding, et al. [18] has discusseda vacuum in the literature by presenting a novel perceptual hash algorithm for verifying the authenticity of multispectral remote sensing images. In order to get a hash value, the technique first preprocesses the multispectral image by band grouping and grid partitioning. Edge feature extraction and perceptual feature reduction come next. By comparing the normalized Hamming distance between the original and recomputed hash values, authentication is accomplished.
2) In 2016, Neha Kishore, et al. [19] has proposed the importance of cryptographic hashing algorithms, with a particular emphasis on Secure Hashing Algorithms (SHA). A thorough examination of performance metrics and the degree of defense against algorithmic attacks are also included in the study. Also includes a comparative analysis and documented attacks for SHA-0, SHA-1, SHA-2, and SHA-3. In order to improve information security, the study attempts to provide insights into the dynamic field of cryptographic hashing algorithms and their parallel implementations.
3) In 2020, F. Hamami, et al. [20] has introduced theapplication of facial recognition technology in a smartattendance system. Face recognition privacy concernsare acknowledged; however, the main emphasis is on how face recognition might be used to track attendance instead of more conventional techniques like fingerprinting. The solution offers a practical andeffective substitute for attendance tracking in a varietyof industries by utilizing big data technologies and deep learning algorithms for real time facial recognition with hash encryption.
4) In 2021, Weiwei Song, et al. [21] has discussed how to tackle the difficulty of managing large-scale remote sensing image retrieval (RSIR) data. It presents a new Deep Hashing Convolutional Neural Network (DHCNN) that can classify semantic labels and retrieve related images at the same time. The DHCNN incorporates a fully connected layer for semantic label classification, a hash layer for effective retrieval, and a pretrained Convolutional Neural Network (CNN) for deep feature extraction.
5) In 2016, Fatma A. Omara, et al. [22] has discussed security issues in modern IT and cloud computing domains, with a focus on cloud storage.

TABLE 1. COMPARISON TABLE

SR NO	PAPER NAME	AUTHORNAME	METHODOLOGY	ADVANTAGES	DISADVANTAGE
1	Image Encryption Algorithm Based onDual Fingerprint Control	Zhenlong Man (et al.)[1]	Fraction Chen hyper, chaossbio metric encryption SSM	High encryption efficiency resists common attacks.	Need both party biometrics complex system.
2	Secure Transmission of Space Images using Joint Encryption Compression	Essam Abdelwarness(et al.) [2]	CCSDS, sample adaptive entropy coding Hamming distance.	Good compression performance, HDto quantify avalanche attack	No PNG, while it provides compression and recessive againstplain text attack but not that strong encryption.
3	Survey on image encryption techniques using chaotic maps in spatial, transformand spatiotemporal domains	Mark McCartney (et al.) [3]	Chaotic maps Spatial domain Transform domain Spatiotemporal domain Image encryption.	the given data is transformed from spatial to frequency domain. Thus, images are encrypted by changing the positions of the coefficients of the image.	needs maturity in security issues, computational efficiency and parameter tuning.
4	Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach	Nirmal Chaudhary (et al.) [4]	Arnold cat map, logistic map, block cipher & AES	Preserves image quality, statistical and differential attack resistant and computationally efficient.	Weak keys and low randomness.
5	Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher	El-Habib Bensikaddour (et al.)[5]	Arnold's Cat map confusion is chaotic maps Fridrich's scheme EDAC	low hardware complexity and low power and can reach a throughput of 120 Mbit/s.	Require great hardware spatialradiation, which can alter the encryption process and cause errors.
6	Cumulative Image Encryption Approach based on User Defined Operation, Character Repositioning, Text Key and Image Key Encryption Technique and Secret Sharing Scheme	Ramkrishna Das (et al.) [6]	K-N Secret Sharing Scheme;Text Key Encryption Technique; BWM AS Operation; Character Repositioning	Four level of encryption techniques have been combined together Secret Sharing Scheme, Image Key and Text key Encryption using BWM and Character Repositioning Technique.	Due to use of various technique of algorithms makes encryption process long have and have high computational cost.
7	Image Encryption Based on Arnod Transform and Fractional Chaotic	Chao Chen (et al.) [7]	fractional derivative; Arnold transform; XOR involving fractional order chaotic sequence;	encryption and decryption algorithm proposed in this paper is simple and easy, which not only reduces computational complexity of encryption algorithm	Arnold transforms in one encryption go is easy to attack After finding the Arnold Transform inverse function, the key can be quickly obtained we have used dual encryption but riskstill remain of it.
8	A secure image permutation–substitution framework based on chaos and compressive sensing	Rui Zhang (et al.) [8]	Image security, compressive sensing, chaotic system, permutation, confusion	the potential of integrating sampling, compression, and encryption in the only one physical layer at a minimal cost Confusion and diffusion are key strengths in this method.	cannot provide an adequate guaranteeof confidentiality, an intrinsic weakness of CS-based cipher, an additional encryption approach based on chaos, and diffusion–confusion mechanism has been proposed
9	Digital Color Image Encryption Using Rc4 Stream Cipher and Chaotic LogisticMap	Riab Ukur Ginting (etal.) [9]	RC4 Stream Cipher; Chaotic Logistics Map; Digital Image Encryption	very sensitive to any changes in external key value, has no content size change between plain-image andcipher-image.	If a strong MAC is not used, RC4 is vulnerable to a bit-flipping attack. RC4 does not support authentication. RC4 is not feasible to be implementedon small streams of data
10	A Survey of Digital Watermarking Techniques and its Applications	Lalit Kumar Saini (etal.)[10]	DWT, DCT, DFT, SVD, LSB, Spread spectrum	Focuses on image watermarkingtypes and their applications in today's world	Semi Fragile i.e. Resist from only some type of Attacks.
11	Digital image watermarking: its formal model, fundamental properties, and possible attacks	Hussain Nyeem (et al.)[11]	Spread-spectrum, bit-carrier selector, Decoder, Encoder,	Perceptual similarity. Invertible, Robust. Allows a unified treatment of all practically meaningful variantsof digital image watermarking.	Limited consideration of inputs, outputs, and component functions and watermarking properties.
12	Research on Digital Image Watermarking Algorithm Based on Scrambling and Singular Value Decomposition	Lei Pei (et al.)[12]	sparse domain watermarking, DCT, k-singular value decomposition, DWT	Image contrast and singular value have been significantly improved. Watermark has strong robustness and can resist various attacks. Better anti-attack ability when attacked.	Poor performance for an embedded image. More techniques are not used which could have better performance.
13	A Review on Digital Image Watermarking	Payal Kaushal (et al.) [13]	FT, DWT, DCT, LSB modification	Tamper detection Impalpability Copyright protection	Security of the watermark after it is embedded in the image is not considered anywhere.
14	Digital watermarking a technology overview	Hebah H.O. Nasereddin (et al.) [14]	Information tagging, LSB modification, DCT, DWT	Study on Watermarking in 3D Objects. digital copyrightsprotection.	Prone to state-of-the-art watermarking attacks, Estimationbased attacks.
15	Digital Image Watermarking Techniques:A Review	Mahbuba Begum (et al.) [15].	LSB, DCT, DFT, DWT, SVD, LSB and ISB modification	DWT is the best technique. Good imperceptibility. Robust against Gaussian noise, salt-and-pepper noise, speckle noise, and brightness. PSNR >50 dB	Security is a big challenge. Not robust against cropping and scaling. Complex implementation

16	A Comprehensive Review on Digital Image Watermarking	Shweta Wadhera (etal.) [16]	LSB, Patchwork method, SSM Modulation, DCT, DFT, and DWT	Help the new researchers to gather knowledge. Frequency domain techniques are preferred. Imperceptible.	More research can be done to identifythe best technique. Fragile.
17	A Review Paper on Digital Watermarking Techniques	Jaspreet Kaur (et al.)[17]	RCM, DFT, DWT, DCT,	High speed, improves performanceand robustness. Increases the embedding rate and less visual distortion	High computational cost due to multiple techniques.
18	A Novel Perceptual Hash Algorithm for Multispectral Image Authentication	Kaimeng Ding (et al.)[18]	Affinity Propagation (AP) Clustering, Perceptual Hash Generation, Grid Entropy Based Adaptive Weighted Fusion Rules, PCA	Strong against modifications that preserve content, efficiently verifies that multispectral remote sensing photos' content integrity makes useof grid entropy-based adaptive weighted fusion rules, band fusion,and band clustering.	Robustness against JPEG compression is not specifically mentioned, Limited discussion onexpansion to hyperspectral remotesensing images.
19	Attacks on and Advances in Secure Hash Algorithms.	Neha Kishore (et al.)[19]	SHA family covering SHA-0, SHA-1, SHA-2, and SHA3, CHF's	summary of the various cryptographic hashing methods andhow they are used. covers implementations based on hardware as well as software	SHA algorithms are used which are traditional methods and complex to handle.
20	Implementation Face Recognition Attendance Monitoring System for Lab Surveillance with Hash Encryption	F. Hamami (et al.)[20]	Multi Cascaded Convolutional Neural Network, KNN, FaceNet model for face recognition using a compact Euclidean space	Utilization of deep learning algorithms based on ConvolutionalNeural Network (CNN). Real-timemonitoring and reporting through web and Android devices	Privacy concerns associated with face recognition technology are not enhanced. Possible issues related to data leakage if not securely encrypted.
21	Deep Hashing Learning for Visual and Semantic Retrieval of Remote Sensing Images	Weiwei Song (et al.)[21]	Deep Hashing Convolutional Neural Network (DHCNN), Euclidean Distance based Retrieval, Hashing Methods	Combines image pair similarity and semantic info. Efficient Retrieval: Hash codes enable quick retrieval via Hamming distance. End-to-End Training: Comprehensive learning of hash codes and semantics	Complex Comprehensive learning of hash codes and semantics
22	A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing FatmaA.	Fatma A. Omara (etal.) [22]	AES, RSA, Hybrid Algorithm, SHA 256	Improve the security of cloud storage by implementing a hybrid encryption algorithm along with theuse of SHA256 for hashing. Aims confidentiality, Integrity	Hybrid-SHA256 algorithm, while providing increased security, resultsin higher computational overhead compared to the hybrid algorithm. Hybrid-SHA256 algorithm consume more time than the hybrid algorithm
23	A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512	Sihan long (etal.)[23]	MD5, SHA 1, SHA 512	Hashing significantly shortens the working process, enhancing efficiency in database operations. Suitable for establishing relationships among elements due to random scattering in hash tables	MD5 is considered weak due to vulnerabilities like collision attacks, raising security concerns. Hashing is suitable for relationship-based operations but not for operations relying on other data relationships

vulnerabilities. It proposes a hybrid encryption technique that combines the SHA256 hash function with the RSA and Advanced Encryption Standard (AES) algorithms. The study is conducted on EyeOS2.5, the selected cloud platform and highlights the significance of data integrity, recommending the use of SHA256, RSA, and AES to support confidentiality, integrity, and non-repudiation.

6) In 2019, Sihan Long, et al. [23] has provided summary of watermarking as well as a classification technique. The methods associated with each of the parameters are presented in tabular form. The techniques of watermarking such as DFT, DWT and DCT are studied thoroughly. Batch and cloud processing in image is implemented and RCM is further implemented by an interpolation technique in future in order to meet the IQA parameters.

III. PROPOSED CONCEPTUAL FRAMEWORK

A multispectral image may consist of several bands for instance, the Landsat 5 satellite may produce images between 450nm and 1250 nm consisting of 7 bands, there arises a need to propose a model to Encrypt as well as Authenticate multispectral Images using watermarking technique. Figure 1, shows the model flow of the proposed system. First, take a multispectral image then 3D-DWT algorithm is used to add a watermark in the image, which will result in the embedded image, after which encryption is performed on it using logistics map technique of chaos-based encryption followed by calculation of hash value using SHA-256 algorithm for Authentication. Figure 2, shows the receiver side where operations similar to sender side are performed in reverse order.In order to enhance the security parameters and entropy value of encrypted images, a hybrid model is implemented with robust and simple mechanisms.

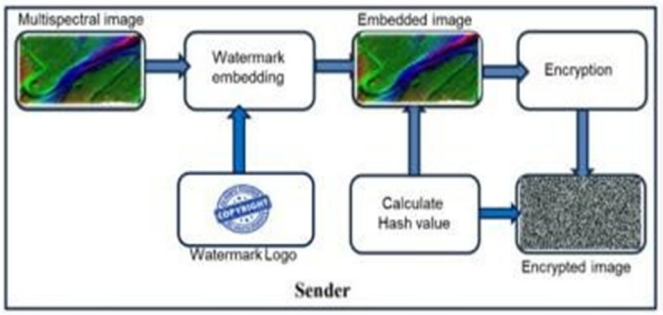


Figure 1

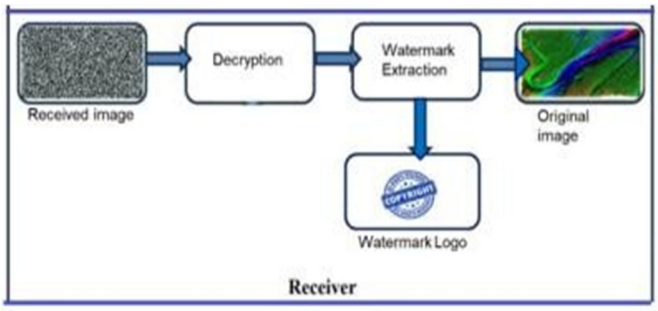


Figure 2

A. Logistic Maps

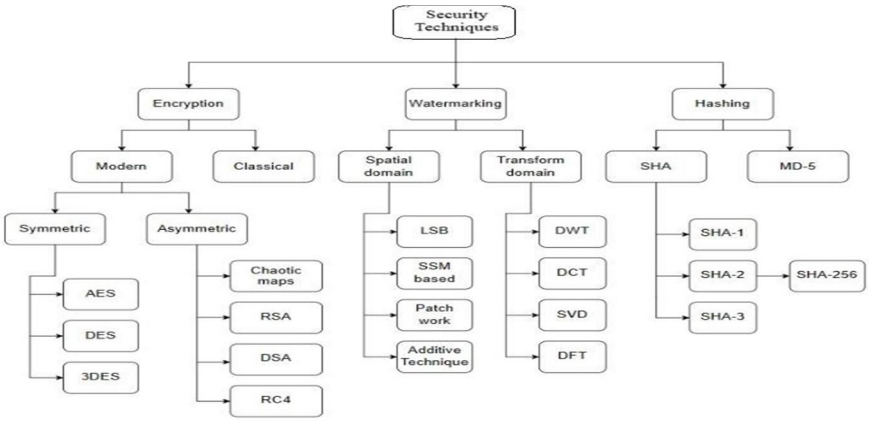
Logistic map is used to generate chaotic behavior from systems having non-linear dynamic equations The mathematical formula is **$U_{S+1}=*U_S(1U_S)$** Where **U_S** varies in [0,1], it shows s^{th} position sequence in control parameter responsible for the whole chaotic sequence which lies in the range [3.57,4]. These maps are often used in algorithms for generating pseudo- random numbers, encrypting data, and simulating complex dynamic systems. The unpredictability and complexity of chaotic maps make them valuable in applications like cryptography, where their inherent disorder enhances security.

B. 3D-DWT

3D-DWT watermarking is applied to hide information in Images and maintaining minimum distortion. It is a mathematical technique used foranalyzing and processing three-dimensional data. 3D-DWT decomposes the input data into different frequency components, allowing for efficient compression, and feature extraction in three- dimensional datasets.

C. SHA-256

SHA-256, is a widely used cryptographic hash function that belongs to the SHA-2 family. It producesa fixed-size 256-bit (32-byte) hash value, providing a high level of data integrity and security. SHA-256 is commonly employed in blockchain technology, digital signatures, and various security protocols to ensure the integrity of data and verify its authenticity.



IV. RESEARCH GAPS

Existing systems use complex Key Handling for encryption and decryption which is resolved in the proposed system. Previous systems provide encryption mostly for regular images, but this proposed system will provide encryption along with authentication for multispectral images.

Many existing spatial watermarking techniques embed watermarks by modifying pixel values directly, which weakens the robustness of the system, and the watermark information is easily destroyed by filtering, image compression, and other attacks. This issue is resolved in the proposed system using transform domain watermarking.

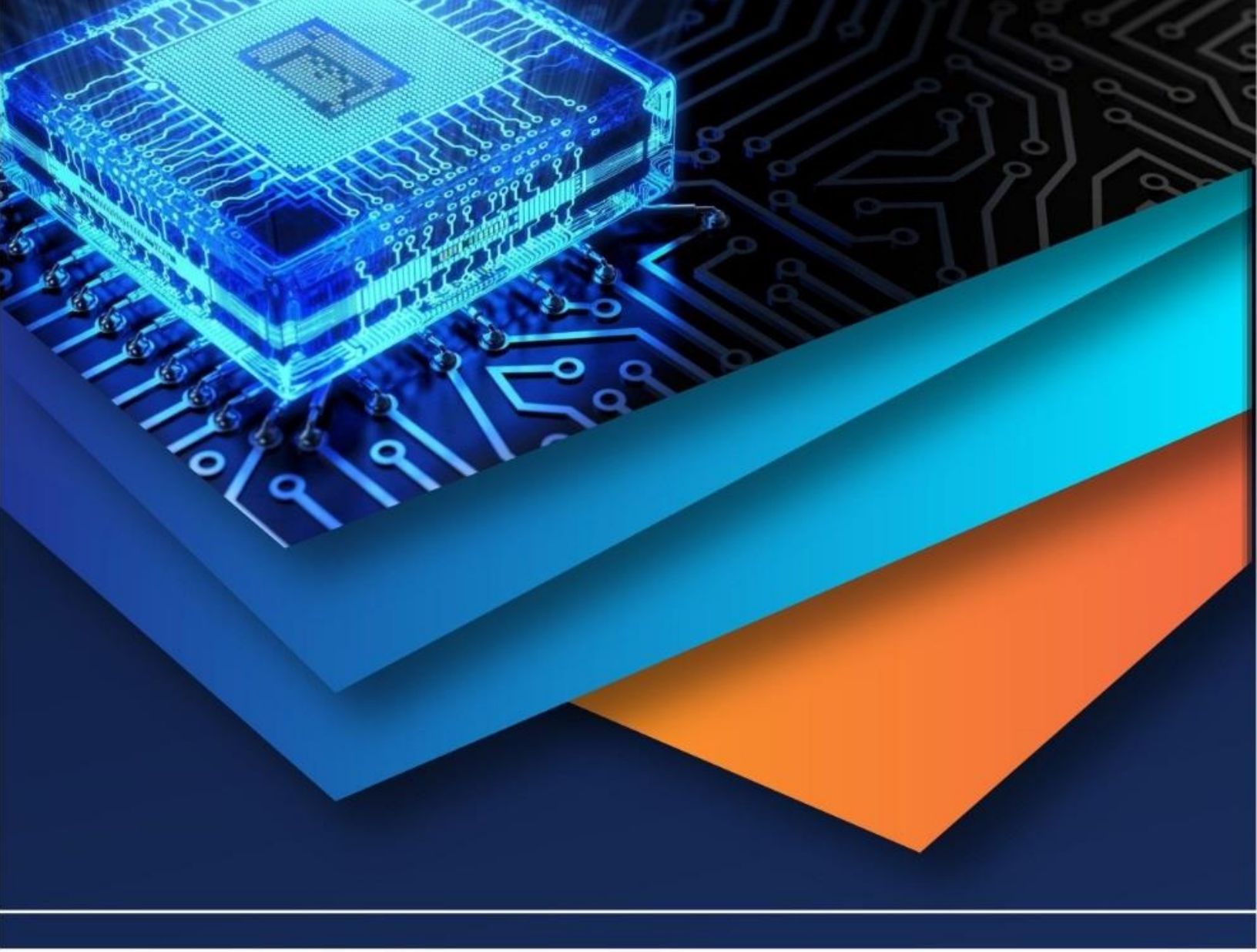
V. CONCLUSION

In summary, this survey article explores the combination of hashing, watermarking, and encryption methods for safe picture transfer. The wide range of techniques, such as neural network applications, AES vs. RSA, and chaotic cryptography, highlights the variety of ways to improve image security. Strong security procedures are important while managing image data because of the needs for confidentiality, integrity, authentication, and protection against different threats that have been identified. The classification diagram helped to select the best approaches for particular needs by providing an adequate summary of the surveyed methodologies. This survey addresses current issues with data privacy, integrity, and ownership in our digitally connected society, greatly increasing secure image transmission techniques. The combination of 3D-DWT, SHA-256, and chaotic maps appears to be a strong foundation for secure transmission of images. The proposed system provides Confidentiality using a Chaotic maps Encryption algorithm, Authentication using SHA-256 along with 3-D DWT as a watermarking technique thus enhancing security while multispectral image transmission.

REFERENCES

[1] Abdullah, Hamsa A., and Hikmat N. Abdullah," Secure image transmission based on a proposed chaotic map." Multimedia Security Using Chaotic Maps: Principles and Methodologies (2020): 81-109.
[2] Agarwal, Shafal," Secure image transmission using fractal and 2D- chaotic map." Journal of Imaging 4.1 (2018): 17.
[3] Sathishkumar, G. A., and Dr N. Sriraam," Image encryption based on diffusion and multiple chaotic maps." arXiv preprintarXiv :1103.3792 (2011).
[4] Bremnavas, I., B. Poorna, and I. Raja Mohamed," Secured medical imagetransmission using chaotic map." Elixir Comp. Sci. Eng 54 (2013): 2472- 2478.
[5] Feng, Wei, Jing Zhang, and Zhentao Qin," A secure and efficient image transmission scheme based on two chaotic maps." Complexity 2021 (2021): 1-19.
[6] Hamdi, Mohamed, and Noureddine Boudriga," Four dimensional chaotic ciphers for secure image transmission." 2008 IEEE International Conference on Multimedia and Expo. IEEE, 2008.
[7] Abdelfatah, Roayat Ismail," Secure image transmission using chaotic- enhanced elliptic curve cryptography." IEEE Access 8 (2019): 3875- 3890.
[8] Yadav, Kanchan, and Trushita Chaware," Review of joint encoding and encryption for image transmission using chaotic map, ldpc and aes encryption." 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2021.
[9] Sankpal, Priya R., and P. A. Vijaya," Image encryption using chaotic maps: a survey." 2014 fifth international conference on signal and image processing. IEEE, 2014.
[10] Fridrich, Jiri," Image encryption based on chaotic maps." 1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation. Vol. 2. IEEE, 1997.
[11] G. Goth, "Steganalysis gets past the hype," IEEE Distributed Systems Online, vol. 6, no. 4, p. 2, 2005.
[12] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography. Morgan Kaufmann, 2007.
[13] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal processing, vol. 90, no. 3, pp. 727–752, 2010.
[14] F. Yaghmaee and M. Jamzad, "Estimating watermarking capacity in grayscale images based on image complexity," EURASIP Journal on Advances in Signal Processing, vol. 2010, no. 1, p. 851920, 2010.
[15] A. A. Tamimi, A. M. Abdalla, and O. Al-Allaf, "Hiding an image inside another image using variable-rate steganography," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 4, no. 10, 2013.
[16] T. Pevny, T. Filler, and P. Bas, "Using high-dimensional image modles to perform highly undetectable steganography," in International Workshop on Information Hiding. Springer, 2010, pp. 161–177.
[17] G. C. Kessler and C. Hosmer, "An overview of steganography," Advancesin Computers, vol. 83, no. 1, pp. 51–107, 2011.
[18] V.Patidar, N.K.Parreek, G.Purohit, K.K. Sud, "Modified substitutiondiffusion image cipher using chaotic standard and logistics maps", Communication in Nonlinear Science and Numerical Simulation 20 10; 1 5(10); pp 2755-2765.
[19] Liu Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin, "Image scrambling algorithm based on chaos theory and sorting transformation",International journal of computer science and network security, Vo1.8 No. 1, January 2008.
[20] EI-Alfy E.S and Al-Utaibi K. An Encryption Schemefor Color Images Based on Chaotic Maps and Genetic Operators.,2011. URL: http://www.thinkmind.orglindex.php?view=artic1eartic1eid=icns 20 11 5 10 1 0212, Visited on August 1 8, 2012.
[21] LA. lsmail, Mohammed amin and Hossam Diab "An Efficient Image Encryption Scheme Based Chaotic Logistic Map ", International Journal of Soft Computing, 285-29 1,2007.
[22] Wang XV, Yu Q., "A block encryption algorithm based on dynamic sequences of multiple chaotic system", Communications in Nonlinear Science and Numerical Simulation 2009; 14(2):574-8 1.

[23] Yu, S. S., Zhou, N. R., Gong, L. H., Nie, Z. (2020). Optical image encryption algorithm based on phase-truncated short-time fractional
[24] Fourier transform and hyper-chaotic system. Optics and Lasers in Engineering, 124, 105816.
[25] Yang, Y. G., Guan, B. W., Li, J., Li, D., Zhou, Y. H., Shi, W. M. (2019). Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2D compressed sensing and DNA encoding. Optics Laser Technology, 119, 1.
[26] Ansari, S.; Gupta, N.; Agrawal, S. An image encryption approach using chaotic maps in frequency domain. Int. J. Emerg. Technol. Adv. Eng. 2012,2,287-29.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY