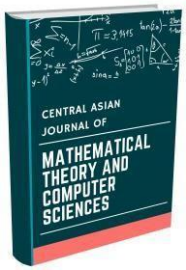

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 05 Issue: 03 | July 2024 ISSN: 2660-5309

Article

Robust Image Watermarking for Tamper Detection and Self-Recovery Using SVD and RSA Methods

Taha Y. Abdulqader[1], Neam Salim Mohammed[2],Lujain Younis Abdulkadir[3]

1. Department of Electronic Technologies, Mosul Technical Institute, Northern Technical University, Mosul, Iraq
2. Department of Electronic Technologies, Mosul Technical Institute, Northern Technical University, Mosul, Iraq
3. Department of Electronic Technologies, Mosul Technical Institute, Northern Technical University, Mosul, Iraq

* Correspondence: mti.lec27.taha@ntu.edu.iq

Abstract: To The paper proposes an Image watermarking technique for identifying and self-recovering tampered images. The system identifies tampered images by comparing the SVD values of 4X4 blocks and average pixel intensities of 2×2 blocks. In the process of SVD computation, the RGB channel images are divided into 4X4 blocks, after which a further 2X2 blocks division is executed for determination of average pixel intensity. Within the same block, tamper-detection data is entered, whereas the self-recovery data is scattered all over the image utilising inverse and RSA techniques for neighborhood block-based recovery. This method assures easy long-term self-healing. The outputs produced from testing with 15 multiple host images in varied attacks were constantly performing better with a PSNR ratio upto an average of 45 dB.

Keywords: Peak Signal-To-Noise Ratio, Rivest-Shamir-Adleman, Singular Value Decomposition, Tampered Images

1. Introduction

In the modern world, people rely on computer communication in their everyday lives which enables them to send pictures, texts and videos within seconds (Alharbi & Kashyap, 2024; Kanojia et al., 2023; Kashyap et al., 2021; Kashyap, Wazir, et al., 2024; Kaur et al., 2024; Wazir, Kashyap, Malik, et al., 2023). Although this tool has improved our lives tremendously, it threatens personal privacy. Many software programs for changing images can steal or modify any image available publicly, leading to false accusations or scams. To prevent such misuse – secret information is hidden in the host image so that tampering can be detected, ownership verified, and self-recovery from image fabrication enabled – through a process known as image watermarking. The Least Significant Bit substitution method uses a simple watermark with a checksum inserted into the LSB to prevent any changes to the image. This method substitutes the other bits depending on whether the pixel values are even odd, so our odd and even-numbered pixels within the image. We can verify the pixel information by checking if the parity has changed. Yet, this easy technique limits detection ability as even minor modification shall not lead to decline until and unless they do so between other data showcasing every pixel.

Citation: Taha Y. Abdulqader. Robust Image Watermarking for Tamper Detection and Self-Recovery Using SVD and RSA Methods. Central Asian Journal of Mathematical Theory and Computer Sciences 2024, 5(3), 193-204.

Received: 03th Jul 2024
Revised: 11th Jul 2024
Accepted: 18th Jul 2024
Published: 25th Jul 2024

Also, Rivest-Shamir-Adleman (RSA) encryption alongside Singular Value Decomposition (SVD) resolves multiple issues linked with image watermarking. SVD builds a robust method for categorizing an image into multiple blocks and identifying the singular values of these blocks which are more likely to get change. This technique leverages detection sensitivity towards minor modification happened by tampering trials and enhances preciseness in detecting anonymous alterations. RSA encryption also ensures self-recovery data's safety is inclusive in the image making, making the image hard to decrypt. Also, the cryptographic methods were utilized by this paper for assuring retrievability recovery verification embedded data alongside maximizing the security in the watermarking procedure.

The paper proposes applicability in a multiple of situations where genuineness and image integrity are important. To preventmis details, fraud, or legal issues, industries comprising media, forensics, and digital rights management largelydependent on the capacity to authenticate images. The suggested watermarking technology has the potential to become the industry standard for digital image security due to its robustness and effectiveness in detecting tampering across a variety of host images and attack situations. Protecting the integrity of visual content with cutting-edge watermarking technology is becoming more and more important as digital communication develops and grows. This will help to maintain the credibility and dependability of digital media across a range of industries.

The study is structured as follows: background is provided in Section II, related works are presented in Section III, implementation is reviewed in Section IV, experimental analysis is carried out in Section V, and we wrap up the investigation with some conclusions and future work in Section VI.

2. Methods

The research method employed in this article focuses on the development and evaluation of robust image watermarking techniques for detection of tampering and self-recovery, using a combination of Singular Value Decomposition (SVD) and Rivest-Shamir-Adleman (RSA) encryption methods. The study begins with identifying the primary issues faced in current digital communication, specifically threats to personal privacy through image manipulation which can lead to false accusations or fraud.

3. Result and Discussion

3.1 Singular Value Decomposition

Singular value sensitivity to changes in image data — SVD is an important method for detecting tampering in image watermarking. In practical applications, an image matrix is decomposed into its constituent parts by the SVD, that is the diagonal matrix $\sum$ containing the singular values and the orthogonal matrices U and V representing the singular vectors. These numbers, arranged in descending order, reflect statistical characteristics of the image and variations in intensity level, thus serving as sensitive indicators of any modifications made to it. To makeminor changes more present and to enable the utilization of watermarks, these values may be allocation within defined boundaries. This signifies that such a techniqueis able to hide the data from the human eye, but it remainsavailable for detectionfor computes which is quite helpful in field like digital forensics, media authentication or assuring compliance with IPR when the reliability of visual contextmust be sustain at any cost. Also, SVD is adaptable so it can easily work in combination with adaptive systems that alter the embedding method based uponspecialcharacteristicspresent in the host image and multiplekinds of potential attacks which leverage the resistance from any sort of tampering attempts. However, there remains many issues with SVD-based watermarking too as this technique works better. One of the keyissues is how to assure that embedded watermarks stayeffective under varied operations for imageprocessing. Error correction codes and algorithms for concealingdata which can

remainintact even in the most usual distortions without losing its integrity – are two potentialmethods towards resolving the highlighted difficulty. Moreover, the realization of SVD on large-scale matrices representing images might lead to significant computational complexity therefore efficient methods must be employed if real-time processing across numerous platforms and applications is desired.

3.2 Rivest-Shamir-Adleman

The security of cryptographic protocols like RSA is rooted in modular arithmetic and number theory. In the beginning, two very large prime numbers are multiplied together; let these be p and q. Their product will become the public modulus n (i.e., n = p * q). All encryption and decryption operations rely on this modulus. An appropriate public exponent e must then be chosen such that 1 < e < (p-1)(q-1) and e is coprime with (p-1)(q-1), thereby ensuring a valid public key. Anyone who wants to send a message to someone else can freely use the public key (n, e) to encrypt it so that only that person can read it. However, looking for an integer d like the e * d ≡ 1 (mod (p-1)(q-1)) is crucial for determining the private key. This signifies that any kind of message encoded with the public key is decoded utilizing the private one (d, n). The text message *M* is further sub-divided into smaller blocksrepresenting letter M_i,In this, Mi signifies $0 \leq M_i < n$ to execute the encryption process. Afterwards, every block M_i is encrypted with the help of the formula $C_i \equiv M_{ie} \, (mod\, n)$ to generateciphertextC_i. With the help of this process of modular exponentiation, efficiency and security can be achieved by assuring the size of the encrypted ciphertextdoes not exceed the modulus n. In transmission, the message encrypted stays as an integer in the range from 0 to n-1. Subsequently, decryption uses private key component d to derive theciphertext C and generate original plaintext M message. The decryption function is elaborated as M ≡ C_d (mod n). Within this context, just a recipient with accurate private key is able to decrypt and recover the actual message due tothe private exponent d. Modular exponentiation assuressecure recovery of the original message while maintain the data confidentiality and integrity in the decryption process. Note that RSA encryption neither increases nor reduces original message size during encryption or decryption.According to the restrictions imposed by the modulus n, both the plaintext message and the generated ciphertext remain as integers between 0 and n-1.This feature is essential for efficient data transport and storage since it lowers computational overhead and ensures interoperability with a variety of data formats and communication protocols. The difficulty of factoring the composite modulus n into its prime constituents, p and q, determines how secure RSA encryption is in practical implementations. The larger the prime integers p and q that are initially chosen, the more difficult it is for adversaries to deduce the private key d from the public key components (n, e).

Many researchers has been published such as (Haouzia & Noumeir, 2008) in his paperproposed a method that utilize a Local Binary Patterns (LBPs) and Convolutional Neural Networks (CNNs) to put a watermark in the image's LBPs and then trace tampering by using the CNNs. A notional image authentication scheme was introduced in (Salama & King, 2005). The scheme is based on the Discrete Wavelet Transform (DWT) and secret sharing—with the watermark embedded into the DWT coefficients. In (Kapre et al., 2022)—they presented a technique which employs chaos in the Discrete Cosine Transform (DCT) domain to enhance tamper resistance while embedding a watermark into the DCT coefficients. Block-independent coding was found vulnerable to Vector Quantization (VQ) attacks by (Bhavani et al., 2023). A color image watermarking method using pair-linked maps are described in (Singh et al., 2023). On the other hand, (Garg & Jain, 2023) proposed a hybrid approach for tamper detection that uses a two-pass logistic map followed by the hamming algorithm. For

various cover images and owners, (Steinebach & Dittmann, 2003) offered a comprehensive and efficient watermarking solution. An irregular pattern in the watermark design should be used to counter VQ attacks as suggested by (Pavani & Sriramya, 2021). However, their approach has limited tamper localization due to the 8 × 8 block size. Speech recognition, image reduction and watermarking are some applications—where SVD is useful because of its simplicity. SVD has been utilized in several robust watermarking strategies. (Liu et al., 2019) proposed an image authentication scheme—which uses SVD together with logistic regression—where singular values are used for embedding a watermark into an image. (Nadeem & Javed, 2005) introduced a strong scheme based on SVD and quaternion wavelet transform which embeds the watermark into SVD coefficients and then uses this transfer to improve robustness. (Safavipour et al., 2022) proposed a semi-fragile watermarking system using SVD for tamper detection in grayscale images without self-recovery ability. VQ attacks due to lack of block independence render—(Vilić, 2017) fragile watermarking system based on DWT—vulnerable to them but excellent at detecting tamper. Hence, this study presents a fragile watermarking system based on SVD that provides self-recovery for colored images.

The study key objective is to localize the affected region. The proposed method achieves this by inserting specific information block-by-block—which changes when the original host image is altered. In Fig. 1—this process is shown block-wise The goal is to enable the damaged areas to self-recover. Each 4 × 4 block is divided into two 2 × 2 blocks, and the average pixel intensity of each 2 × 2 block is computed. These bits are referred to as self-recovery data in a host image using a certain algorithm. Fig. 2 shows how a 4 × 4 block can be divided into 2 × 2 blocks whose average pixel intensity should always be maintained for generating self-recovery data that can be used to recover tampered regions on an image.

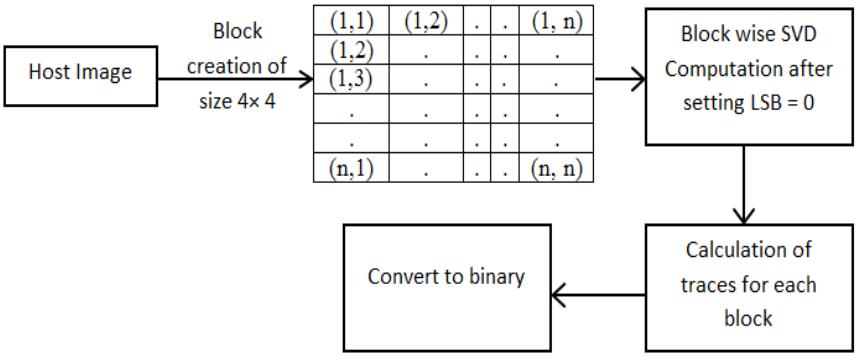

Fig. 1. Block-by-block trace computation (tamper detection data)

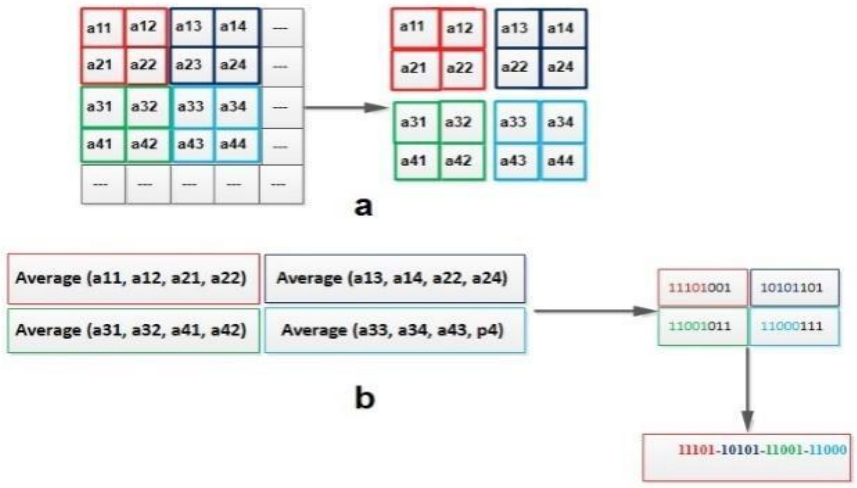

Fig. 2. The procedure for splitting a 4 x 4 block into 2 x 2 blocks and figuring out the average pixel intensity of each 2 x 2 block

3.3 **Scheme for the watermark**

The steps involved in watermark embedding are outlined in Fig. 3 and are intended to improve the security and integrity of digital images. Initially, the RGB image is broken down into its individual red, green, and blue channels. Through independent processing of each channel made possible by this breakdown, tamper detection and self-recovery methods can be applied to the image's distinct color components with efficacy. SVD is used to every channel in order to obtain important tamper detection information. SVD decomposes the channel's matrix representation into its singular vectors and values—where the singular values stand for the channel's orthogonal projections' magnitudes. These single values are affected by any channel modification—including purposeful manipulation and accidental distortion—which modifies the computed tamper detection data. The foundation for identifying unauthorized image modifications is the sensitivity to changes [19]–[24]. Techniques for fragile watermarking are used to provide extra information to each image channel. Checksums, digital signatures, and other identifiers that improve the capacity to detect tampering are frequently included in this extra data. To ensure that only authorized parties may verify and extract the watermark information without jeopardizing the secrecy of the image—RSA encryption is used to secure and protect the integrity of the embedded data. When embedding the watermark, both the computed tamper detection and self-recovery data are merged with the image. In each channel's LSBs there are hidden tamper detection data that have been put carefully, it is achieved through SVD analysis and can be improved by subtle watermarking techniques as well. With the help of this embedding—tampered sections can be learned based upon the differences among the original and observed data—whereas the detection data remain invisible to the human eye and obtained for executing the computational analysis. The altered channels are combined to produce the final watermarked image once the tamper detection and self-recovery data have been implanted into each of the individual channels. This composite image incorporates the embedded information required for further recovery and verification procedures—while maintaining the original's visual integrity.

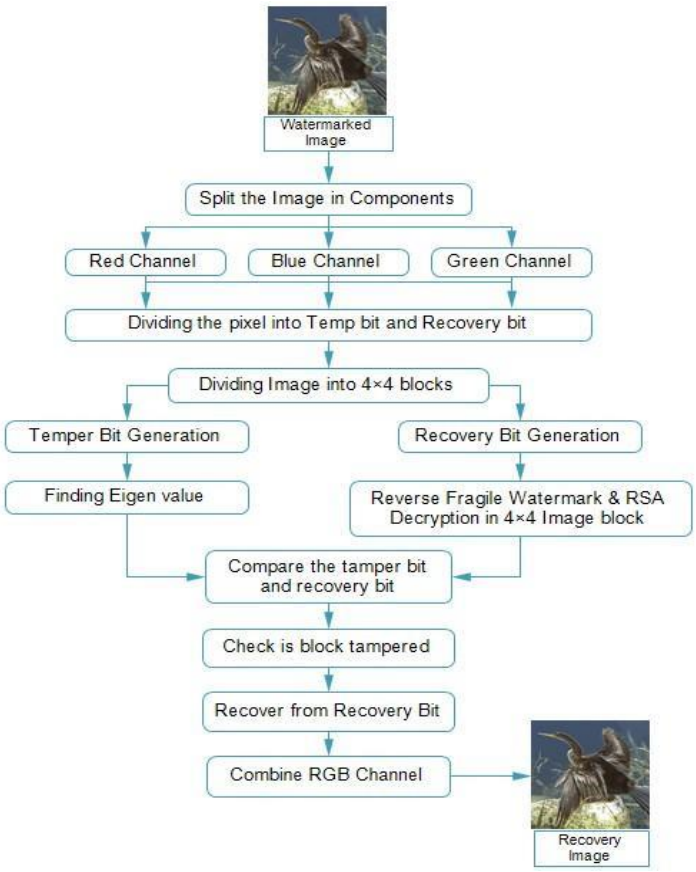

Fig. 3. Embedding watermark

3.4 Extraction of Watermarks and Self-Recovery

Several crucial processes are involved in the extraction process—which is shown in Fig. 4, with the goal of recovering manipulated portions and confirming the image's authenticity. Initially, the watermarked image is divided into its red, green, and blue parts. Every component goes through LSB extraction, and embedded tamper detection and self-recovery data are found in the LSB plane of every channel. Each channel's integrated tamper detection data is extracted from its LSB plane. This data contains information that is essential for figuring out whether or not certain blocks in the image have been altered. Discrepancies that indicate possible regions of manipulation or unauthorized adjustments can be found by comparing the returned data with the originally inserted tamper detection information. Blocks that have been tampered with within the image are identified by comparing the returned tamper detection data with the original embedded data. The term "tampered blocks" designates locations where the integrity of the image may have been jeopardized and is found in blocks where differences in tamper detection data are found. When altered blocks are found—the user key is required for additional analysis—and restoration is obtained using RSA decryption. By converting encrypted data back into its original format—the decryption process makes it possible to restore modified blocks to their original condition by using the inherent self-recovery information. Simultaneously, self-recovery information embedded in the image components' LSB planes is retrieved. The information on the watermark embedding process in this self-recovery data is vital to bringing altered blocks back to their initial pixel worth. For undetected tampering or alteration, the method of extraction helps ensure that the content of original images can be recovered by neighbourhood block-based recovery algorithms. Also, this technique further uses neighbourhood block-based recovery methods to increase the precision of recovered images from identified tampered blocks. In such algorithms, multiple pixels are forecasted and restored by identifyingsections which are around the tampered areas. Such a system relies on intrinsic tedium and spatial coherence in digital images. Even under severe data loss or serious deviation, the

restored images will emerge and be more available when integrated with RSA decryption technology. Throughout all stages after unauthorized editing or interference but before final restoration work has been done embedding data application mitigates iterative recognition for tampered block retrieval alongside restorative procedures saving faithfulness towards originality at every phase following illegal The usage of data embedding software prevents iterative detection for tampered block retrieval at every stage following unlawful alteration or interference but prior to the completion of the final restoration procedure. This happens in tandem with restorative processes, guaranteeing fidelity to the original at every stage after illicit modification or tampering

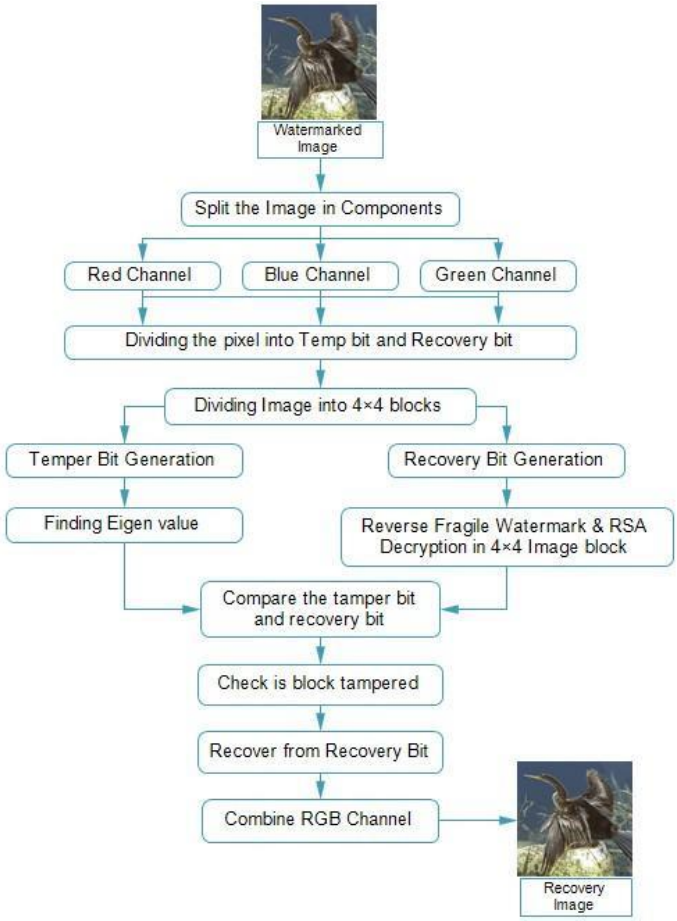

Fig. 4. The extraction of self-recovery and watermarks flowchart

Experimental Analysis

This study evaluates the effectiveness of an advanced image watermarking system using three primary host images that have been standardized to 512 × 512 pixels. Watermarks are inserted into these photos using a base approach in the least significant bits (LSBs) by using RSA encryption parameters where p=1, q=1, and s=512. The method guarantees secure information embedding while remaining imperceptible and resistant to many kinds of image alterations. Five crucial criteria were carefully calculated in order to evaluate the overall effectiveness of the scheme: False Positive Rate (FPR), False Negative Rate (FNR), Tamper Detection Rate (TDR), Normalized Cross-Correlation (NCC), and Peak Signal-to-Noise Ratio (PSNR). When all of these requirements are met, it is feasible to precisely find and identify any tampered area inside an image while preserving its integrity and veracity globally.

The first step is to extract watermarked images from the original images, making sure that the PSNR value stays high throughout, ranging from 45.06 dB to 45.88 dB. This indicates strength because there is no distortion after watermarking, and the images also need to look good for various real-world applications. In order to verify robustness, these watermarked images are put through a series of simulated attacks in the second stage. Adding text ('Swan' and 'Bird' with extra text), copying and pasting extra elements into photos ('Swan' example with extra plant leaves), or removing specific contents from specified places ('Owl bird' and 'Swan' with some elements deleted) are a few popular assaults. The technique's ability to identify tampered regions accurately can be seen in Figs .5 and Fig. 7 which shows results obtained after carrying out such attacks locally. Another problem brought about by the Visual Quality(VQ) attack is the capability to forge an image by combining parts from several watermarked images which may have differing spatial arrangements thus compromising detection accuracy.

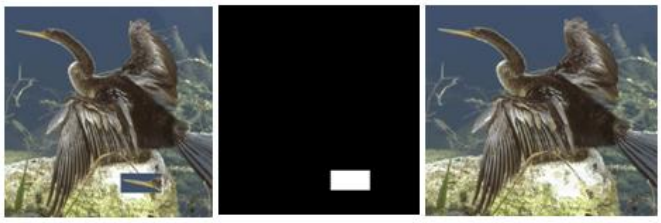

Fig. 5. The assault is shown as a copy-paste attack with the attacked watermarked images displayed on the right side and the attack localization in the center. The self-recovered host appears on the far left

Fig. 6. The attacked images (top right), the attack location (middle), and the self-recovering host (leftmost) as a result of the text insertion

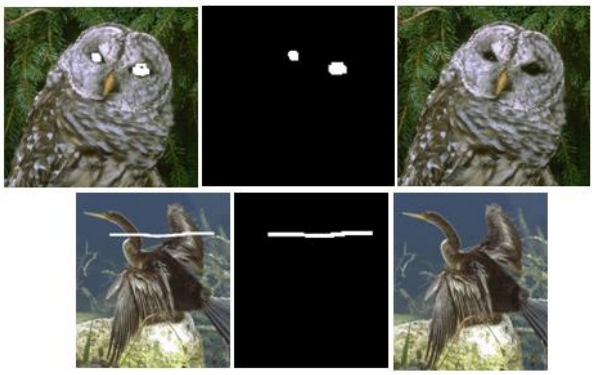

Fig. 7. The assault localization is displayed in the center, and the attacked watermarked photos are displayed on the rightmost side. The self-repaired host appears on the leftmost side

In spite of this, Fig. 8 shows that the technique achieves an impressive PSNR of roughly 48.35 dB, demonstrating its capacity to preserve image quality and precisely restore altered content. A thorough examination of the FPR, FNR, and NCC values for both

watermarked and recovered images under various attack scenarios is also shown in Table I. The scheme's efficacy in embedding watermarks without sacrificing visual quality is confirmed by the high NCC values (NCC1) for watermarked images, which show barely any discernible difference from the original hosts. The near-to-one NCC values (NCC2) of the recovered images also highlight the accurate restoration of altered material, which is essential for trustworthy data verification and forensic analysis. The suggested method clearly outperforms current watermarking systems when compared to them, as shown by Table II's extensive analysis of PSNR for self-recovered photos across a range of host images. Higher PSNR values (48.45 dB to 51.86 dB) than references (Salama & King, 2005), (Awasthi & Srivastava, 2023), (Bhavani et al., 2023), and (Garg & Jain, 2023) consistently confirm the resilience and efficacy of the system in maintaining image quality and integrity under various manipulation scenarios.

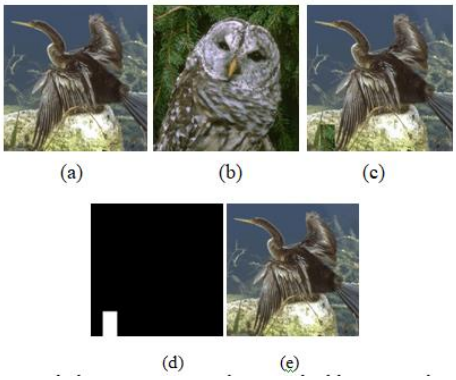

Fig. 8. Post the VQ attack, watermarked images were generated. VQ attacked Image with Swan -1 (a), Owl bird -2 (b), and Swan -3 (c)

TABLE I
FPR AND FNR VALUES CALCULATED FOR EACH ASSAULT

Type of Attacks	**Host images**	**FPR**	**FNR**	**NCC (watermarked image)**	**NCC (recovered host)**
Copy and paste	Swan	0.41	0.009	0.9997	0.9983
	Lena	0.43	0.010	0.9993	0.9987
Text addition	Swan	0.46	0.008	0.9996	0.9991
	Bird	0.49	0.009	0.9995	0.9983
Content Removal	Bird	0.43	0.01	0.9998	0.9976
	Owl bird	0.45	0.01	0.9997	0.9988
VQ	Owl bird+ Swan	0.81	0.03	0.9994	0.9964
	Lena+ Girl	0.89	0.03	0.9997	0.9961

TABLE II
COMPARES THE PSNR VALUE (DB) TO THOSE OF OTHER SYSTEMS

Host Images	(Salama & King, 2005)	(Awasthi & Srivastava, 2023)	(Bhavani et al., 2023)	(Garg & Jain, 2023)	**Proposed**
Lena	36.67	38.55	39.33	40.73	48.45
Baboon	36.69	38.57	39.36	40.71	49.48
Boat	36.72	38.59	39.35	40.58	44.81
Peppers	N/A	N/A	N/A	N/A	46.44

Plane	36.68	38.55	39.37	40.86	48.66
Swan	36.70	38.61	39.38	40.67	51.86
Bird	36.70	38.57	39.36	40.71	49.59
Owl bird	36.73	39.60	39.35	40.58	50.79

4. Conclusion

The study concludes with the presentation of a novel and secure image watermarking method that makes use of sophisticated RSA encryption. This method is backed by thorough assessments against a variety of attack vectors and comparisons with the most recent approaches. The scheme could be used to protect digital assets, improve data integrity in multimedia applications, and advance secure image transmission technologies because of its strong watermark embedding capabilities, accurate tamper detection, and high fidelity image restoration capabilities. To increase the scheme's practical usefulness in real-world security domains and digital media protection, future research approaches might concentrate on improving computational efficiency, investigating adaptive watermarking techniques, and bolstering resilience against emerging digital threats.

REFERENCES

[1] F. Alharbi and G. S. Kashyap, "Empowering Network Security through Advanced Analysis of Malware Samples: Leveraging System Metrics and Network Log Data for Informed Decision-Making," *International Journal of Networked and Distributed Computing*, pp. 1–15, 2024. doi: 10.1007/s44227-024-00032-1

[2] D. Awasthi and V. K. Srivastava, "Hessenberg Decomposition-Based Medical Image Watermarking with Its Performance Comparison by Particle Swarm and JAYA Optimization Algorithms for Different Wavelets and Its Authentication Using AES," *Circuits, Systems, and Signal Processing*, pp. 1–32, 2023. doi: 10.1007/s00034-023-02344-z

[3] Y. Bhavani, K. K. Bejjanki, and T. Nagasai Anjani kumar, "Singular Value Decomposition and Rivest–Shamir–Adleman Algorithm-Based Image Authentication Using Watermarking Technique," pp. 387–395, 2023. doi: 10.1007/978-981-19-8563-8_37

[4] P. Garg and A. Jain, "A robust technique for biometric image authentication using invisible watermarking," *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 2237–2253, 2023. doi: 10.1007/s11042-022-13314-z

[5] H. Habib, G. S. Kashyap, N. Tabassum, and T. Nafis, "Stock Price Prediction Using Artificial Intelligence Based on LSTM–Deep Learning Model," in *Artificial Intelligence & Blockchain in Cyber Physical Systems: Technologies & Applications*, CRC Press, pp. 93–99, 2023. doi: 10.1201/9781003190301-6

[6] A. Haouzia and R. Noumeir, "Methods for image authentication: A survey," *Multimedia Tools and Applications*, vol. 39, no. 1, pp. 1–46, 2008. doi: 10.1007/s11042-007-0154-3

[7] M. Kanojia, P. Kamani, G. S. Kashyap, S. Naz, S. Wazir, and A. Chauhan, "Alternative Agriculture Land-Use Transformation Pathways by Partial-Equilibrium Agricultural Sector Model: A Mathematical Approach," 2023. [Online]. Available: https://arxiv.org/abs/2308.11632v1

[8] B. S. Kapre, A. M. Rajurkar, and D. S. Guru, "Self-embedding and Variable Authentication Approach for Fragile Image Watermarking Using SVD and DCT," *Communications in Computer and Information Science*, vol. 1697, pp. 366–379, 2022. doi: 10.1007/978-3-031-22405-8_29

[9] G. S. Kashyap, K. Malik, S. Wazir, and R. Khan, "Using Machine Learning to Quantify the Multimedia Risk Due to Fuzzing," *Multimedia Tools and Applications*, vol. 81, no. 25, pp. 36685–36698, 2022. doi: 10.1007/s11042-021-

11558-9

[10] G. S. Kashyap, A. Siddiqui, R. Siddiqui, K. Malik, S. Wazir, and A. E. I. Brownlee, "Prediction of Suicidal Risk Using Machine Learning Models," 2021. [Online]. Available: https://papers.ssrn.com/abstract=4709789

[11] G. S. Kashyap et al., "Detection of a facemask in real-time using deep learning methods: Prevention of Covid 19," 2024. [Online]. Available: https://arxiv.org/abs/2401.15675v1

[12] G. S. Kashyap et al., "Revolutionizing Agriculture: A Comprehensive Review of Artificial Intelligence Techniques in Farming," 2024. doi: 10.21203/RS.3.RS-3984385/V1

[13] P. Kaur et al., "From Text to Transformation: A Comprehensive Review of Large Language Models' Versatility," 2024. [Online]. Available: https://arxiv.org/abs/2402.16142v1

[14] X. Liu et al., "DPatch: An adversarial patch attack on object detectors," *CEUR Workshop Proceedings*, vol. 2301, 2019. [Online]. Available: https://arxiv.org/abs/1806.02299v4

[15] N. Marwah, V. K. Singh, G. S. Kashyap, and S. Wazir, "An analysis of the robustness of UAV agriculture field coverage using multi-agent reinforcement learning," *International Journal of Information Technology (Singapore)*, vol. 15, no. 4, pp. 2317–2327, 2023. doi: 10.1007/s41870-023-01264-0

[16] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in *Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005*, pp. 84–89, 2005. doi: 10.1109/ICICT.2005.1598556

[17] S. Naz and G. S. Kashyap, "Enhancing the predictive capability of a mathematical model for pseudomonas aeruginosa through artificial neural networks," *International Journal of Information Technology*, pp. 1–10, 2024. doi: 10.1007/S41870-023-01721-W

[18] K. Pavani and P. Sriramya, "Enhancing public key cryptography using RSA, RSA-CRT and N-Prime RSA with multiple keys," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, pp. 661–667, 2021. doi: 10.1109/ICICV50876.2021.9388621

[19] M. H. Safavipour, M. A. Doostari, and H. Sadjedi, "A hybrid approach to multimodal biometric recognition based on feature-level fusion of face, two irises, and both thumbprints," *Journal of Medical Signals and Sensors*, vol. 12, no. 3, pp. 177–191, 2022. doi: 10.4103/jmss.jmss_103_21

[20] P. Salama and B. King, "Efficient secure image transmission: compression integrated with encryption," in *Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, p. 47, 2005. doi: 10.1117/12.587011

[21] D. Singh, S. K. Singh, and S. S. Udmale, "An efficient self-embedding fragile watermarking scheme for image authentication with two chances for recovery capability," *Multimedia Tools and Applications*, vol. 82, no. 1, pp. 1045–1066, 2023. doi: 10.1007/s11042-022-13270-8

[22] M. Steinebach and J. Dittmann, "Watermarking-Based Digital Audio Data Authentication," *Eurasip Journal on Applied Signal Processing*, vol. 2003, no. 10, pp. 1001–1015, 2003. doi: 10.1155/S1110865703304081

[23] V. M. Vilić, "Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace," *Balkan Social Science Review*, vol. 10, no. 10, pp. 7–24, 2017.

[24] S. Wazir, G. S. Kashyap, K. Malik, and A. E. I. Brownlee, "Predicting the Infection Level of COVID-19 Virus Using Normal Distribution-Based Approximation Model and PSO," in *Springer, Cham*, pp. 75–91, 2023. doi: 10.1007/978-3-031-33183-1_5

[25] S. Wazir, G. S. Kashyap, and P. Saxena, "MLOps: A Review," 2023. [Online]. Available: https://arxiv.org/abs/2308.10908v1