Enhancing Secure Image Communication through Fully Homomorphic Watermarking: A Robust Approach for Privacy-Preserving Data Transmission

Mohd Shajid Ansari*, Dr. Siddhartha Choubey, Dr. Abha Choubey

Mohd Shajid Ansari, Department of Computer Science and Engineering, Shri Shankaracharya Technical Campus Shri Shankaracharya Group of Institution Bhilai, Chhattisgarh, India, Shajidavis@gmail.com.
Dr. Siddharth Choubey, Department of Computer Science and Engineering, Shri Shankaracharya Technical Campus Shri Shankaracharya Group of Institution Bhilai, Chhattisgarh, India, sidd25876@gmail.com
Dr. Abha Choubey, Department of Computer Science and Engineering, Shri Shankaracharya Technical Campus Shri Shankaracharya Group of Institution Bhilai, Chhattisgarh, India, abha.is.shukla@gmail.com.

Abstract

The increasing prevalence of cyber-attacks calls for advanced solutions for secure data exchange, particularly in the area of image sharing. This paper focuses on creating a secure framework for image communication by utilizing homomorphic watermarking techniques. A comprehensive approach for securely transmitting images via cloud servers, drawing on the advantages of 2D-Discrete Wavelet Transform (2D-DWT) and homomorphic encryption is presented. In proposed method, first 2D-DWT is applied to break down the image into unique coefficients, which we then encrypt using homomorphic techniques to bolster security. To safeguard intellectual property, a watermark is also incorporated into the image. The proposed approach has been effectively deployed and assessed, demonstrating encouraging outcomes in both security and data fidelity. Performance evaluation is carried out using three primary metrics: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Squared Error (MSE). The result analysis also examined how the algorithm performs under different cryptographic key lengths and image sizes. The findings indicate high-quality image output coupled with reasonable computational demands, positioning proposed methodology as a practical choice for secure and efficient image transmission.

Keywords: Secure Communication, Image Encryption, Watermarking, Homomorphic Encryption.
DOI Number: 10.48047/nq.2021.19.3.NQ21040 **NeuroQuantology 2021; 19(3): 1217-1228**

1. Introduction

The Internet of Things (IoT) has revolutionized how images or videos are shared across applications such as smart healthcare, intelligent infrastructures, and advanced transportation systems. In our modern digital era, visual content has become a cornerstone of daily interactions, serving as an effective medium to transmit both information and feelings [1]. Yet, as the ease of image sharing has grown, so have concerns surrounding security and privacy. Threats like unauthorized access, potential data breaches, and the wrongful use of private visual content

loom large. In response, cryptographic techniques have been employed as a defense against harmful interventions. While traditional cryptographic methods like AES, IDEA, RC6, and TDES may be well-suited for text data encryption [2], their effectiveness wanes when it comes to encrypting digital images. This ineffectiveness stems from image attributes like their voluminous data, inter-pixel correlations, and repetitive data patterns. Using these methods in commercial software or devices with limited computing power proves challenging. Historically, images have been instrumental in conveying human stories and experiences [3]. In contemporary times, technological advancements have made image sharing a common practice, influencing numerous facets of our existence. Platforms on social media are inundated with pictures that forge global connections. Concurrently, businesses leverage visual strategies to craft memorable brand identities. From scientific discoveries to our cosmic understanding, images play a pivotal role [4]. Our digital age has transformed visual narrative sharing, making it an inclusive activity. Today, memes, videos, and other visual formats have emerged as potent mediums, influenced viewpoints and initiating discussions [5]. However, this visual communication proliferation has given rise to challenges related to privacy, security, and genuineness. Issues like unauthorized usage, alteration, and falsification become pressing in a world where visual content often stands as proof or valuable data. Conventional strategies such as watermarking and digital signatures, unfortunately, have their constraints [6]. Researchers are exploring innovative solutions like homomorphic encryption to enhance image communication security, enabling secure processing and sharing of visual data. This paper aims to explore the significance of image communication and investigate the use of homomorphic encryption for securing visual content. Fig. 1 presents the representation how image communation takes place.

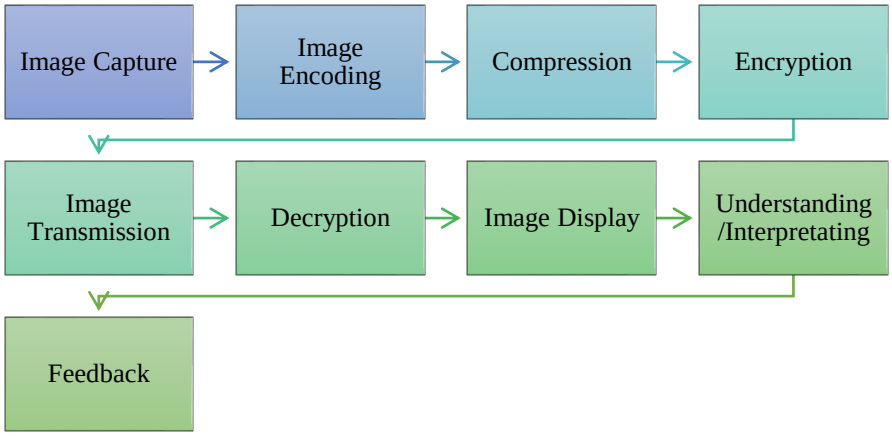

Figure 1. Schematic Representation of Image Communication

2. Related Work

Secure image communication is of utmost importance across various domains due to the sensitive and private information often contained in images [7]. Unauthorized access can lead to privacy breaches and identity theft. Data integrity is vital in professional settings to prevent manipulation of critical evidence. It also protects intellectual property rights, builds trust in media, and ensures compliance with data protection laws. In military applications, secure image communication is essential for national security interests [8][9]. As cloud storage usage grows, secure communication safeguards against unauthorized access and potential breaches. It also helps mitigate denial-of-service attacks and protects against evolving cyber threats like hacking and ransomware [10][11]. In the domain of image communication security, researchers have developed various techniques to address the issue, as presented in fig 2.

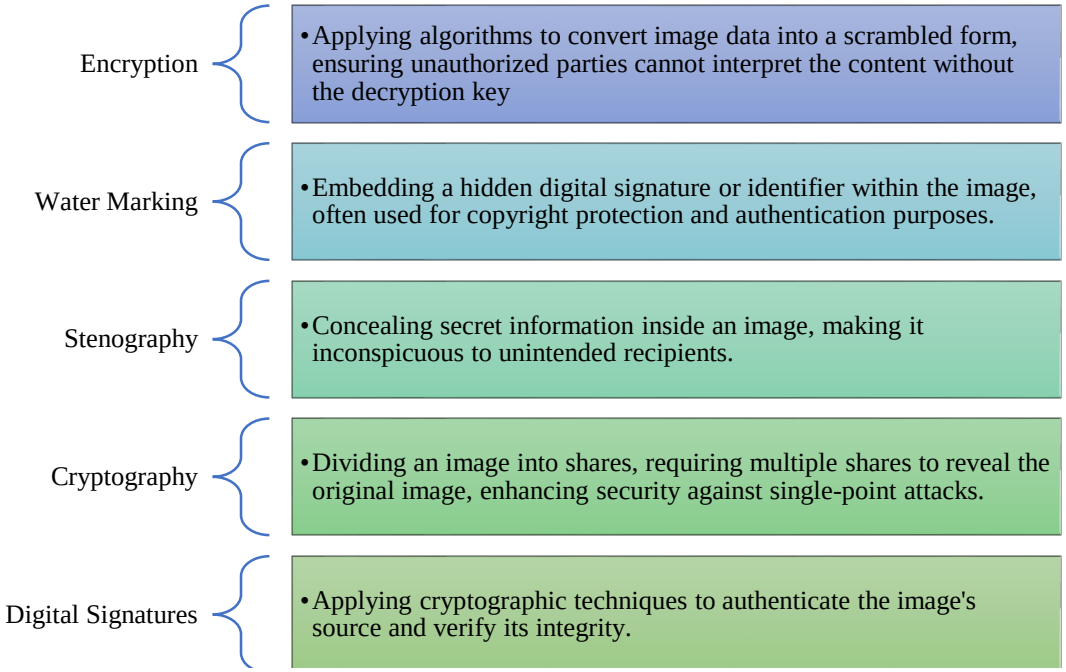

Figure 2. Techniques for Securing Image Transmission

Zhang et al. [12] explored the use of compressive sensing for secure wireless communications, enabling the recovery of sparse signals from limited data to reduce transmission. Subhedar and Mankar [13] conducted a survey on image steganography, which involves hiding information imperceptibly within images. Eichelberg et al. [14] provided a comprehensive overview of cybersecurity in Picture Archiving and Communication Systems (PACS) and medical imaging, addressing the increasing concern about securing medical data with the growing adoption of digital technologies in healthcare.Patel et al. [15] proposed several image encryption methods for secure communication. One two-phase method uses pixel scrambling, bit-level operation, and double sorting quantization with a strong HaLT map generated from a combination of CLT map and Halton sequence. Hash values from MD5 and SHA-256 algorithms add additional security, resulting in high resistance to attacks and fast performance for practical

applications. Mondal et al. [16] put forth an algorithm that was examined for its robustness, quality, and invisibility. When used on standard grayscale images, the watermarking encryption displayed high entropy (approaching values of 7.999). This indicated a minimal relationship between the original and encrypted pictures and notable changes in pixel values during the encryption process, as evidenced by the high NPCR percentages. Norouzi et al. [17] highlighted a unique image encryption technique that leveraged hyper-chaotic systems. The high NPCR and UACI values from this study suggest a robust defense against alterations to the encrypted image even if just one pixel in the source image is changed. Furthermore, the properties of chaotic attractors, such as the Chen attractor's sensitivity and diffusion characteristics, have been investigated in the context of image encryption by Arumugham et al. [18]. Li et al. [19] presented an image encryption technique using an FPGA-generated synthetic image with low resource utilization and power consumption. The system is designed for IoT monitoring applications, addressing resource constraints and data transmission security. It incorporates a new compressed sensing (CS) model and parallel reconstruction algorithm, reducing encryption/decryption time significantly. By integrating quantization and diffusion operations based on chaotic systems, transmission security is further enhanced. Simulations demonstrate the effectiveness, with a significant reduction in computation time and storage requirements for large-scale images compared to traditional CS methods. Blesswin et al. [20] proposed an enhanced semantic visual secret sharing (ESVSS) scheme, securely transmits a grayscale secret image using two color cover images. At the receiver end, the secret image is reconstructed by stacking the shares digitally. The ESVSS achieves improved image quality with a higher Peak Signal to Noise Ratio (PSNR) and reduced Mean Square Error. Additionally, the reconstructed image demonstrates high Universal Image Quality Index (UIQI) results with minimal computational complexity.Table 1 presents a detailed comparison of various techniques used for secure image communication. The table emphasizes the significance of robust security measures when dealing with sensitive and private visual information during digital data exchange. It showcases the key findings of different methods aimed at improving image quality, strengthening security measures, and reducing data transmission in image communication.The study primarily centers on the "Homomorphic Encryption" technique, which is a promising approach for secure image communication. This technique enables computations to be performed on encrypted data without decryption, ensuring enhanced security and privacy during image exchange. The upcoming sections will provide an in-depth exploration of Homomorphic Encryption, its applications in secure image communication, and its potential benefits and challenges in protecting sensitive visual data across different domains.

This section introduces the importance of secure image communication and elaborates on the existing methods, highlighting the gaps in the current techniques. Following research questions is designed for proposed methodology:

- How effective is homomorphic watermarking in securing image communication?

What is the level of imperceptibility, robustness, and security provided by homomorphic watermarking

3. Methods Used

3.1 Homomorphic Encryption

Images are communicated in diverse contexts, serving different purposes. Personal photographs capture memories, while business graphics include infographics for presentations and marketing. Medical images aid in healthcare, artwork expresses creativity, and product images are used in e-commerce. Satellite images serve mapping and environmental studies, while security and surveillance images monitor activities. Social media and internet memes entertain and communicate, scientific images support research, and news images document events

visually. Robust security measures are essential for image communication due to privacy concerns, protection from exploitation, and compliance with legal requirements. Homomorphic encryption emerges as a promising solution to ensure secure image communication. Homomorphic encryption allows you to perform calculations on encrypted data without first having to decrypt it. In this encryption scheme, if E_k is the encryption function and $D_k$is the decryption function, and the plaintext is represented by $M = m_1, m_2, \dots \dots m_n$, then the scheme is homomorphic if it allows certain operations α and β to be carried out directly on the ciphertexts in a way that is equivalent to performing these operations on the plaintexts. In other words, homomorphic encryption allows you to transform encrypted data in a meaningful way such that when it is decrypted, the result is the same as if the transformation had been applied to the original, unencrypted data.

$$\alpha(E_k(m_1), E_k(m_2), \dots \dots \dots \dots, E_k(m_n)) = \beta(E_k(\mathrm{M})) \quad (1)$$

In homomorphic encryption, you can perform operations directly on encrypted data without exposing the original values. If data $M = m_1, m_2, \dots \dots m_n$ is there then it can encrypt each piece of data to get $E_k(m_1), E_k(m_2), \dots \dots \dots \dots, E_k(m_n)$. Then, some operation α are performed on these encrypted values. When decryption is done on the given result, it will be equivalent to having performed the β operation on the original $m_1, m_2, \dots \dots m_n$, unencrypted data. This encryption scheme supports operations like addition and multiplication directly on the encrypted data.

$m_1 + m_2 + \cdots \dots m_n$=$D_k(E_k(m_1) + E_k(m_2) + \cdots \dots \dots \dots + E_k(m_n))$. (2)

$m_1 . m_1 \dots . m_n$=$D_k(E_k(m_1) . E_k(m_2) + \cdots \dots \dots \dots . E_k(m_n))$. (3)

Key Generation

1: Two large prime numbers p and q are randomly selected.
2: N is calculated as $N = p \times q$.
3: λ (lambda) is calculated as the lowest common multiple (LCM) of $(p-1) and\ (q-1)$.
4: A random g is selected from $Z^*_{N^2}$such that $gcd(L(g^{\lambda} mod N^2), N) = 1$conditions are satisfied.
5: This sets up the public and private keys for encryption and decryption. At the end of the key generation process, the public key is (N, g) and the corresponding private key is λ.

Encryption

1: A random parameter r is chosen from $Z^*_{N^2}$.
2: The plaintext m from Z_N is encrypted into ciphertext c using the formula $c = E[m, r] = (gm \cdot rN) \mathrm{mod} N^2$.
3: Different ciphertexts c can be generated for the same plaintext m by varying the parameter r, enhancing security.

Decryption

1: The original plaintext m is decrypted from the ciphertext c using the formula $m = D[c] = L(g\lambda \mathrm{mod} N^2) L(c\lambda \mathrm{mod} N^2) \mathrm{mod} N$.
2: These encryption and decryption processes ensure the cryptographic properties of the Paillier system, including its homomorphic and probabilistic features.

3.2 Proposed Methodology

To enhance the safety of image stored in cloud environments, we suggest a robust and reversible watermarking technique based on fully homomorphic encryption. The workflow of this proposed approach is illustrated in Figure 3.

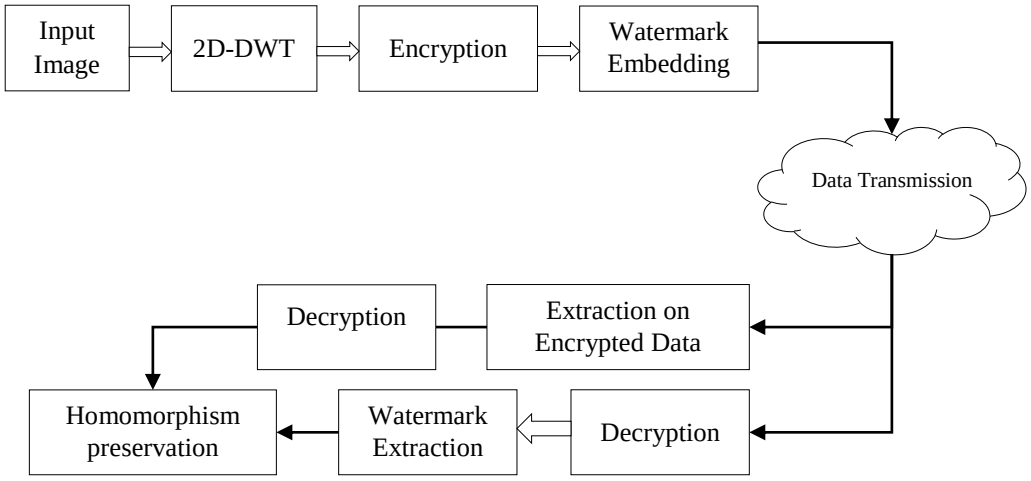

Figure 3. Proposed Methodology

The working of this method can be understood through the following steps, algorithm 1:

- Division into Blocks: The first step involves breaking down the original image into 2-Discrete Wavelet Transform (DWT) blocks. DWT is a mathematical technique that breaks down a signal into different frequency components, often used in image processing.
- Homomorphic Encryption: Each of these blocks is then encrypted using Fully Homomorphic Encryption (FHE). FHE allows computations to be performed on the encrypted data without needing to decrypt it first. This ensures that the security of each block is maintained.
- Watermark Insertion: A watermarking image, which could be a logo or some identifiable pattern, is then combined with each of the encrypted blocks. This embedding process ensures that the image is marked as proprietary or contains some form of identification metadata.
- Secure Transmission: After watermarking, the image blocks are securely transmitted over the internet to a cloud server. Since the blocks are encrypted, this transmission is secure, ensuring that unauthorized users cannot easily tamper with or interpret the content.
- Retrieval: At the receiving end, usually a cloud server, the transmitted blocks are retrieved.
- Watermark Extraction and Decryption: Finally, the watermark is separated from the encrypted image block. Since the image is encrypted using Fully Homomorphic Encryption, operations like watermark extraction can be performed without decrypting the image block. After the watermark is extracted, the image can be decrypted, resulting in an image that is virtually identical to the original pre-encrypted and pre-watermarked image.

Through this method, we can achieve dual benefits: the security of the image data through encryption and the protection of intellectual property through watermarking, all while being able to perform these operations securely over the cloud.

Algorithm: Secure Image Transmission

Input: I original_image, I_w watermark image

1: Begin

2: Generate public Pu_{key} and private keys Pr_{key}

3: $[I_{LL}, I_{LH}, I_{HL}, I_{HH}] \xleftarrow{2D-DWT} I$
4: $[EI_{LL}, EI_{LH}, EI_{HL}, EI_{HH}] \xleftarrow{FHE} [I_{LL}, I_{LH}, I_{HL}, I_{HH}]$
5: Embed watermark into Horizontal Coefficients EI_w
6: Data Transmission
7: $RI \xleftarrow{2D-IDWT} EI_w$
8: $RI_1 \xleftarrow{Decrypt} EI_w$
9: $RI_2 \xleftarrow{2D-IDWT} RI_1$
10: If $RI_2 == RI$
11: Homomorphism preserved
12: Output RI_2
13: End

4. Results and Discussions

The performance assessment of the proposed methodology is covered in this section. The experimental investigation was performed on Intel Core i5 processor with an 8 GB hard drive. Using Python platform, simulation analysis was carried out.

To evaluate the performance of the proposed work following parameters are used:

PSNR (Peak Signal-to-Noise Ratio): A measure of the quality of reconstruction in image processing. Higher values generally indicate better quality.

$$PSNR = 10.log_{10}(\frac{Max_i^2}{MSE}) \quad (4)$$

MSE (Mean Squared Error): Measures the average of the squares of the errors between the estimated and actual values. Lower MSE values generally indicate better image quality.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(O_i - P_i)^2 \quad (5)$$

Where, N is the total number of pixels, O_i is the original image and P_i is the decrypted image.

SSIM (Structural Similarity Index): Measures the structural similarity between two images. The values range from -1 to 1, with higher values indicating more similarity.

$$SSIM\ (x_1, x_2) = \frac{(2\mu_1\mu_2 + k_1)(2\sigma_{12} + k_2)}{(\mu_1^2 + \mu_2^2 + k_1)(\sigma_1^2 + \sigma_2^2 + k_2)} \quad (6)$$

Where, μ_1= mean of x, μ_2 = mean of, σ_{x1}^2 = variance of x1, σ_{x2}^2= variance of x2, σ_{x1x2}= co-variance of x_1 and x_2, k_1 and k_2 are variables to stabilize the separation with weak denominator.

Key Gen Time (in sec): The time taken to generate the cryptographic key, measured in seconds. Lower values are generally better for real-time or near-real-time applications.

Enc Time (in Sec): The time taken in seconds to encrypt the image. Lower times indicate more efficient performance.

Dec Time (in Sec): The time taken in seconds to decrypt the image. Lower times indicate more efficient performance.

The table 4.1 evaluates the performance of different images based on three metrics: PSNR (Peak Signal-to-Noise Ratio), SSIM (Structural Similarity Index), and MSE (Mean Squared Error). The PSNR values are fairly consistent across all the images, ranging from 27.04 to 27.90. The average is 27.34. The SSIM values range from 0.65 to 0.89. MSE values range from 117.10 to 128.63. Lower values are generally better. The average PSNR is 27.34, SSIM is 0.82, and MSE is 125.85. These values indicate that the images are generally of moderate quality, but there is room for improvement, especially in SSIM and MSE. The variation in PSNR is not significant, but there is a notable difference in SSIM and MSE, suggesting that structural integrity and error may be more variable across the different images. Given the lower SSIM and higher MSE in some images, future work could focus on improving the structural similarity and reducing the error in the reconstructed images.

Table 1. Performance Evaluation on Different Images

Images	PSNR	SSIM	MSE
Image 1	27.44	0.83	117.10
Image 2	27.08	0.84	127.35
Image 3	27.05	0.88	128.19
Image 4	27.04	0.67	128.63
Image 5	27.08	0.65	127.29
Image 6	27.05	0.86	128.17
Image 7	27.15	0.80	125.34
Image 8	27.74	0.89	123.86
Image 9	27.90	0.88	124.74
Image 10	27.86	0.88	127.86
Average	27.34	0.82	125.85

The table 2 evaluates the performance of encryption and decryption processes based on different key sizes. The metrics used are the time taken for key generation (Key Gen Time), encryption time (Enc Time), and decryption time (Dec Time), all measured in seconds. As the key size increases, the time to generate the key increases as well. Encryption time also scales with key size, ranging from 1.348 seconds for a 64-bit key to 136.750 seconds for a 512-bit key. Similar to encryption, decryption time increases with key size, ranging from 1.033 seconds with a 64-bit key to 134.750 seconds with a 512-bit key. The average times are 0.12725 seconds for key generation, 42.7 seconds for encryption, and 41.6 seconds for decryption. As the key size increases, the security level also increases, but at the cost of speed. Larger keys take significantly more time for both encryption and decryption. However, this average may not be very informative given the wide range of times across different key sizes. Since both encryption and decryption times scale significantly with key size, optimizations could be beneficial, especially for larger key sizes. The choice of key size would likely depend on the specific requirements of an application, balancing the need for security against performance constraints. In summary, the table highlights important trade-offs between security and performance. Depending on the use-case, one may opt for higher security with a larger key size, or faster performance with a smaller key size.

Table 2. Performance Evaluation on Different Key Size

Key Size	Key Gen Time (in sec)	Enc Time (in Sec)	Dec Time (in Sec)
64	0.00080	1.348	1.033
128	0.00810	5.560	4.679
256	0.15500	27.140	25.960
512	0.34510	136.750	134.750
Average	0.12725	42.700	41.606

The table 3 evaluates the performance of cryptographic operations based on different image sizes. The metrics used are the time taken for key generation (Key Gen Time), encryption time (Enc Time), and decryption time (Dec Time), all measured in seconds. Encryption time increases with the size of the image, ranging from 5.64 seconds for a 64-pixel image to 165.86 seconds for a 512-pixel image. Decryption time also increases with the size of the image, ranging from 4.859 seconds for a 64-pixel image to 163.86 seconds for a 512-pixel image. The average times are 0.0083 seconds for key generation, 69.288 seconds for encryption, and 65.000 seconds for decryption. There's a clear trend that as the image size increases, both encryption and decryption times increase

substantially. This implies that for larger images, one should expect longer processing times. The average times could give an overall sense of what to expect in terms of processing times, but given the wide range of times and the apparent non-linear scaling with image size, this average may not be particularly informative for all use-cases. In summary, the table shows that encryption and decryption times scale substantially with image size, indicating that care must be taken when selecting image sizes for particular applications, especially those requiring real-time processing.

Table 3. Performance Evaluation on Different Image Size

Image Size	Key Gen Time (in sec)	Enc Time (in Sec)	Dec Time (in Sec)
64	0.002209	5.64	4.859
128	0.016	19.85	16.637
256	0.0105	85.80	74.6457
512	0.0045	165.86	163.86
Average	0.00830	69.288	65.000

The table 4 compares various techniques for secure image communication along three main parameters. improved image quality, enhanced security and reduced data transmission. Compressive Sensing [12] focuses solely on reducing data transmission but does not improve image quality or enhance security. Image Steganography [13] focuses on improving image quality but lacks in terms of enhanced security and reduced data transmission. Cybersecurity in PACS [14] designed primarily for enhanced security without addressing image quality or data transmission. Two-Phase Image Encryption [15] and Hyper-Chaotic Image Encryption [17], both improve image quality and enhance security but do not focus on reducing data transmission. Watermark Encryption [16] focuses only on enhancing security. Chaotic Attractors [18] does not offer any of the three mentioned benefits. Enhanced visual secret sharing [20] improves image quality and enhances security but doesn't reduce data transmission. The proposed method in this study improves image quality, enhances security, and reduces data transmission. Therefore, the proposed method offers a well-rounded solution that addresses all three major aspects of secure image communication. Most other techniques specialize in one or two aspects, thereby potentially leaving gaps in the overall secure image communication landscape. In summary, the proposed technique offers a comprehensive, multi-faceted approach to secure image communication, outperforming or matching most existing methods in the literature across key performance indicators.

Table 4. Comparison of Techniques for Secure Image Communication

Ref.	Technique Used	Improved Image Quality	Enhanced Security	Reduced Data Transmission
[12]	Compressive Sensing	x	x	√
[13]	Image Steganography	√	x	x
[14]	Cybersecurity in PACS	x	√	x
[15]	Two-Phase Image Encryption	√	√	x
[16]	Watermark Encryption	x	√	x
[17]	Hyper-Chaotic Image Encryption	√	√	x
[18]	Chaotic Attractors	x	x	x
[19]	Image Communication System	√	√	√
[20]	Enhanced Visual Secret Sharing	√	√	x
Ours		√	√	√

5. Conclusion

The increasing dependence on cloud services for data storage and transmission mandates a robust approach to ensure data security and intellectual property protection. This paper presented a secure image transmission methodology that ingeniously combines 2D-Discrete Wavelet Transform (2D-DWT) with FHE to address these challenges. The method allows for the secure encryption of image data and the embedding of watermarks without compromising the original image quality. Experimental results affirm the efficacy of the approach in maintaining data integrity while providing a strong layer of security.The extensive evaluation based on PSNR, SSIM, and MSE showcases the efficacy of the proposed method in maintaining high-quality image transmission. Interestingly, our algorithm does not suffer significant degradation in quality when evaluated under varying cryptographic key sizes and image dimensions. The time complexity for key generation, encryption, and decryption was also found to be acceptable, particularly for smaller image sizes. However, some challenges remain, such as the computational cost for larger images, which can be a point of focus for future research. The proposed algorithm bridges the gap between security and efficiency, making it a promising avenue for secure image communication in various applications, including healthcare, military, and social networks. Future research should aim at optimizing the algorithm for real-time applications and exploring additional layers of security to make it even more robust against potential cyber threats.

References

[1] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things," in IEEE Access, vol. 4, pp. 1222-1242, 2016, doi: 10.1109/ACCESS.2016.2542800.

[2] Ramalingam, B., Rengarajan, A., & Rayappan, J. B. B. (2017). Hybrid image crypto system for secure image communication–A VLSI approach. *Microprocessors and Microsystems*, *50*, 1-13. https://doi.org/10.1016/j.micpro.2017.02.003

[3] Simon Heron, Advanced Encryption Standard (AES), Network Security, Volume 2009, Issue 12, 2009, Pages 8-12, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(10)70006-4.

[4] Chen, J., Xue, D. & Lai, X. An analysis of international data encryption algorithm(IDEA) security against differential cryptanalysis. Wuhan Univ. J. Nat. Sci. 13, 697–701 (2008). https://doi.org/10.1007/s11859-008-0612-4

[5] Ritonga, A. R., Irmayani, D. ., & Ritonga, A. A. . (2022). Rivest Cipher 6 Algorithm Method to secure messages of Medical Record files at Perlayuan Health Center . Sinkron : Jurnal Dan Penelitian Teknik Informatika, 7(2), 586-594. https://doi.org/10.33395/sinkron.v7i2.11391

[6] Akshitha Vuppala, R Sai Roshan, Shaik Nawaz, JVR Ravindra, An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm, Procedia Computer Science, Volume 171, 2020, Pages 1054-1063, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.04.113.

[7] Sharma, A., Singh, G., Rehman, S. (2020). A Review of Big Data Challenges and Preserving Privacy in Big Data. In: Kolhe, M., Tiwari, S., Trivedi, M., Mishra, K. (eds) Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, vol 94. Springer, Singapore. https://doi.org/10.1007/978-981-15-0694-9_7

[8] Rounsefell, K, Gibson, S, McLean, S, et al. Social media, body image and food choices in healthy young adults: A mixed methods systematic review. Nutrition & Dietetics. 2020; 77: 19– 40. https://doi.org/10.1111/1747-0080.12581

[9] Ann E Schlosser, Self-disclosure versus self-presentation on social media, Current Opinion in Psychology, Volume 31, 2020, Pages 1-6, ISSN 2352-250X, https://doi.org/10.1016/j.copsyc.2019.06.025.

[10]Aiello M, Cavaliere C, D'Albore A, Salvatore M. The Challenges of Diagnostic Imaging in the Era of Big Data. *Journal of Clinical Medicine*. 2019; 8(3):316. https://doi.org/10.3390/jcm8030316

[11]O. Evsutin, A. Melman and R. Meshcheryakov, "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions," in IEEE Access, vol. 8, pp. 166589-166611, 2020, doi: 10.1109/ACCESS.2020.3022779.

[12]Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong and S. Guo, "Secure Wireless Communications Based on Compressive Sensing: A Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1093-1111, Secondquarter 2019, doi: 10.1109/COMST.2018.2878943.

[13]Mansi S. Subhedar, Vijay H. Mankar, Current status and key issues in image steganography: A survey Computer Science Review, Volumes 13–14, 2014, Pages 95-113, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2014.09.001

[14]Eichelberg, M., Kleber, K. & Kämmerer, M. Cybersecurity in PACS and Medical Imaging: an Overview. J Digit Imaging 33, 1527–1542 (2020). https://doi.org/10.1007/s10278-020-00393-3

[15]Patel, S.; Veeramalai, T. Image Encryption Using a Spectrally Efficient Halton Logistics Tent (HaLT) Map and DNA Encoding for Secured Image Communication. Entropy 2022, 24, 803. https://doi.org/10.3390/e24060803

[16]Bhaskar Mondal, Tarni Mandal, A light weight secure image encryption scheme based on chaos & DNA computing, Journal of King Saud University - Computer and Information Sciences, Volume 29, Issue 4, 2017, Pages 499-504, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2016.02.003.

[17]Norouzi, B., Mirzakuchaki, S., Seyedzadeh,. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 71, 1469–1497 (2014). https://doi.org/10.1007/s11042-012-1292-9

[18]Arumugham, S., Rajagopalan, S., Rethinam, S., Janakiraman, S., Lakshmi, C., Rengarajan, A. (2020). Synthetic Image and Strange Attractor: Two Folded Encryption Approach for Secure Image Communication. In: Pati, B., Panigrahi, C., Buyya, R., Li, KC. (eds) Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 1082. Springer, Singapore. https://doi.org/10.1007/978-981-15-1081-6_40

[19]L. Li, G. Wen, Z. Wang and Y. Yang, "Efficient and Secure Image Communication System Based on Compressed Sensing for IoT Monitoring Applications," in IEEE Transactions on Multimedia, vol. 22, no. 1, pp. 82-95, Jan. 2020, doi: 10.1109/TMM.2019.2923111.

[20]John Blesswin A, Raj, C., Sukumaran, R. et al. Enhanced semantic visual secret sharing scheme for the secure image communication. Multimed Tools Appl 79, 17057–17079 (2020). https://doi.org/10.1007/s11042-019-7535-2

[21] Kaissis, G.A., Makowski, M.R., Rückert, D. et al. Secure, privacy-preserving and federated machine learning in medical imaging. Nat Mach Intell 2, 305–311 (2020). https://doi.org/10.1038/s42256-020-0186-1

[22]Sample, K.L., Hagtvedt, H. & Brasel, S.A. Components of visual perception in marketing contexts: a conceptual framework and review. J. of the Acad. Mark. Sci. 48, 405–421 (2020). https://doi.org/10.1007

[23]Munjal, K., Bhatia, R. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex Intell. Syst. (2022). https://doi.org/10.1007/s40747-022-00756-z

[24]Pan Yang, Xiaolin Gui, Jian An, Feng Tian, "An Efficient Secret Key Homomorphic Encryption Used in Image Processing Service", Security and Communication Networks, vol. 2017, Article ID 7695751, 11 pages, 2017. https://doi.org/10.1155/2017/7695751

[25]R. Bellafqira, G. Coatrieux, D. Bouslimi and G. Quellec, "Content-based image retrieval in homomorphic encryption domain," 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy, 2015, pp. 2944-2947, doi: 10.1109/EMBC.2015.7319009.

[26]R. Challa, G. VijayaKumari and Sunny B, "Secure Image processing using LWE based Homomorphic encryption," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2015, pp. 1-6, doi: 10.1109/ICECCT.2015.7226064.

[27]Yang, H., Huang, Y., Yu, Y., Yao, M., Zhang, X. (2017). Privacy-Preserving Extraction of HOG Features Based on Integer Vector Homomorphic Encryption. In: Liu, J., Samarati, P. (eds) Information Security Practice and Experience. ISPEC 2017. Lecture Notes in Computer Science(), vol 10701. Springer, Cham. https://doi.org/10.1007/978-3-319-72359-4_6