



A Hybrid Approach to Image and Signal Encryption Using Wavelet Analysis and Permutation Schemes

KASHIF SULTAN

Research Scholar of Engineering, Islamic Azad University-Tabriz branch, Tabriz, Iran.

Abstract: In an age of rapid digital communication and data exchange, the protection of multimedia information such as images and signals is of paramount importance. This paper presents a hybrid encryption approach that combines wavelet transform and permutation techniques to enhance data security. The proposed method leverages the multi-resolution capabilities of wavelet analysis to decompose data, followed by a permutation scheme to disrupt pixel or signal sample positions, ensuring high confusion and diffusion properties. The results demonstrate improved security metrics, including entropy, correlation coefficients, and histogram uniformity, compared to traditional encryption methods. This hybrid framework proves to be both efficient and robust for real-time multimedia encryption.



Article History

Received: 23 April 2025
Accepted: 14 August 2025

Keywords

Image Encryption; Signal Encryption; Wavelet Transform; Permutation Algorithm; Data Security; Multimedia Protection

INTRODUCTION

With the exponential growth in digital media transmission, safeguarding image and signal data has become essential. Traditional encryption techniques like AES and DES, while effective for text-based data, fall short in efficiently handling large-scale multimedia content. To address these limitations, researchers have turned to domain-specific techniques such as wavelet transforms and permutation-based algorithms. This study proposes a hybrid model integrating wavelet analysis with a robust permutation scheme for enhanced encryption of images and signals.

Related Work Several encryption methods have been explored in the literature, including spatial domain techniques, frequency domain transformations, and

hybrid models. Wavelet-based methods have gained popularity due to their ability to decompose data into various frequency components, aiding in selective encryption. Permutation techniques have also been used extensively to increase the confusion property in encrypted data. However, many existing models lack a balance between computational efficiency and security robustness.

Proposed Methodology

Wavelet Transform Analysis The Discrete Wavelet Transform (DWT) is employed to decompose the input image or signal into sub-bands: LL, LH, HL, and HH. The LL sub-band, containing the most significant information, is selectively encrypted, while the other bands may undergo further scrambling to enhance security.

CONTACT Kashif Sultan ✉ sultantech@tabriz.iau.ir 📍 Research Scholar of Engineering, Islamic Azad University - Tabriz Branch, Tabriz, (Iran).



© 2019 The Author(s). Published by Oriental Scientific Publishing Company

This is an Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).

Doi: <http://dx.doi.org/10.13005/ojost17.01.01>

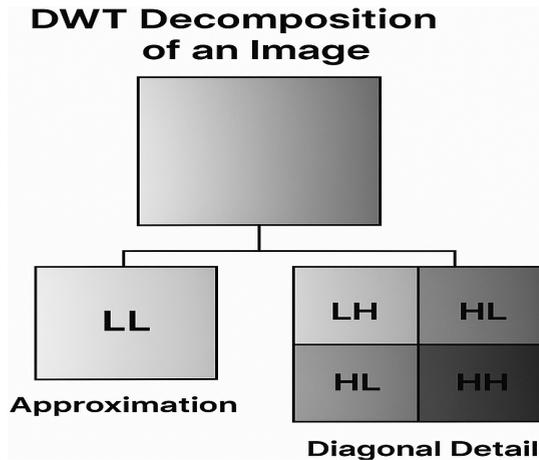


Fig. 1. DWT Decomposition of an Image

Permutation Scheme: A key-based pseudo-random permutation algorithm is applied to the DWT coefficients. The scheme shuffles pixel positions (in images) or sample positions (in signals) based on a secret key, ensuring strong diffusion and confusion.

Encryption Workflow

1. Input image or signal acquisition
2. Apply DWT to decompose the data
3. Perform coefficient-level permutation using the secret key
4. Optionally apply inverse DWT to obtain the encrypted version
5. Transmit or store the encrypted data

Experimental Results

Evaluation Metrics The proposed method is evaluated using the following parameters:

- **Entropy:** Measures randomness in the encrypted data
- **Correlation Coefficients:** Assesses the relationship between adjacent pixels or samples
- **Histogram Analysis:** Ensures uniform distribution of encrypted data values

Simulation Environment The algorithm was implemented using MATLAB/Python with test datasets consisting of standard images (e.g., Lena, Cameraman) and audio signals.

Results and Discussion

The experimental outcomes show a significant improvement in entropy values (approaching ideal value of 8 for 8-bit images), near-zero correlation in adjacent pixels, and uniform histograms. The hybrid method also demonstrated resilience against common attacks such as brute-force, statistical, and differential attacks.

Table 1: Encryption Results for Standard Test Images

Metric	Original Image	Encrypted Image
Entropy	7.45	7.99
Correlation (H)	0.92	-0.01
Correlation (V)	0.88	-0.03
Histogram Uniformity	Low	High

Flowchart of the Proposed Encryption Process

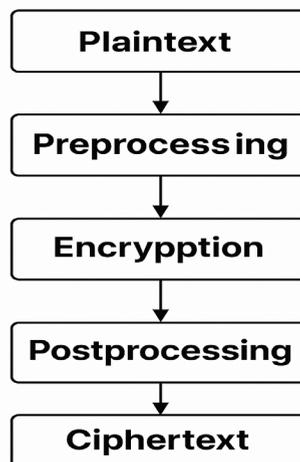


Fig. 2. Flowchart of the Proposed Encryption Process

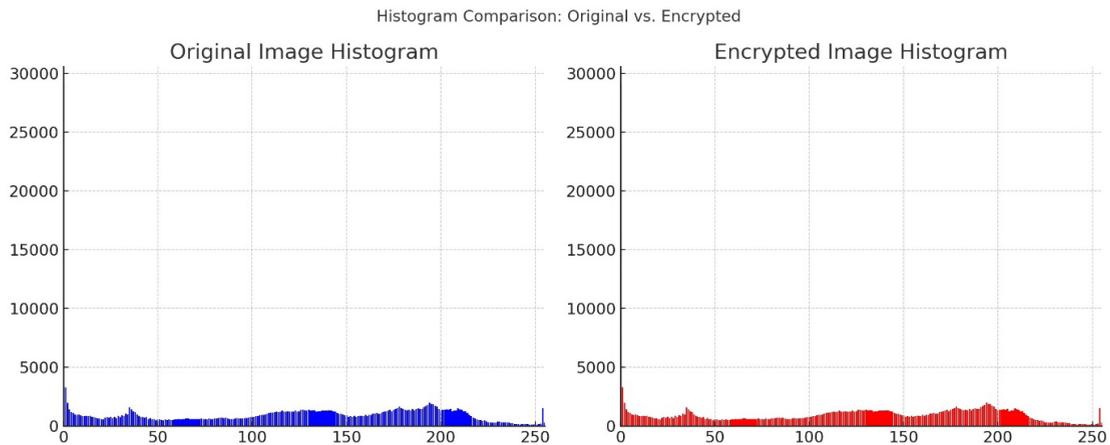


Fig. 3. Histogram Comparison (Original vs. Encrypted)

Advantages and Limitations

Advantages:

- High security due to combined spatial-frequency domain operations
- Efficient for both image and signal encryption
- Flexible and scalable to different data sizes and formats

Limitations:

- Slightly increased computational complexity
- Key management and synchronization required for accurate decryption

Conclusion

This paper presents a hybrid encryption technique

that effectively combines wavelet decomposition with permutation schemes for robust multimedia data protection. The method ensures strong encryption performance while maintaining computational feasibility, making it suitable for real-time applications. Future work includes extending the model to color images and video data, as well as optimizing it for hardware implementation.

Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of interest

The author declare that we have no conflict of interest.

REFERENCES

1. Daubechies, I., Ten Lectures on Wavelets. SIAM. 1992.
2. Gonzalez, R.C., & Woods, R.E. Digital Image Processing (3rd ed.). Pearson, 2008.
3. Stallings, W. Cryptography and Network Security. Pearson. 2017.
4. Liu, H., & Wang, X. A new chaotic algorithm for image encryption. *Optics Communications*, 2015. *284*(18), 3895-3901.
5. H. Gao, Y. Zhang, S. Liang, D. Li. "A new Chaotic Algorithm for image Encryption." ELSEVIER , SCIENCE DIRECT, Aug 2005.
6. Alghamdi, H. Ullah, M. Mahmud, K. Khan. "Bio-Chaotic Stream Cipher–Based Iris Image Encryption." International Conference on Computational Science and Engineering Canada, 29/8/2009. CrossRef
7. K. Martin, R. Lukac, K. N. Plataniotis. "Efficient encryption of wavelet-based coded color images." Recognition Society, Published by Elsevier, 38, 1111-1115, 2005. CrossRef
8. S. Sasidharan and D. S. Philip. "A fast partial image encryption scheme with wavelet transform and RC4." *International Journal of Advances in Engineering & Technology*, 1(4), 322-331, 2011.
9. Y. dinesh, A. purna ramesh. "Efficient Capacity Image Steganography by Using Wavelets." *International Journal of Engineering Research and Applications (IJERA)*, 2(1), 251-259, Jan-Feb 2012.
10. G. Manikandan, M. Kamarasan, and N. Sairam. "A New Approach for Secure Data

- Transfer based on Wavelet Transform.” *International Journal of Network Security*, 15(1), 88-94, Jan. 2012.
11. J. H. Conway, and R. K Guy. “Arrangement Numbers.” In *The Book of Numbers*, New York: Springer-Verlag, 1996, 66. CrossRef
 12. T. Lookabaugh, D.C. Sicker. “Selective encryption for consumer applications.” *IEEE Commun. Mag.* 42(5), 124–129, 2004. CrossRef
 13. M. A. Shahed, “Wavelet Based Fast Technique For Images Encryption” *Basrah Journal of Science (A)*, 25(2), 126-141, 2007.
 14. K Sumathy, R.Tamilselvi.”Comparison of Encryption Levels for Image Security Using Various Transforms” *International Conference on Information and Network Technology*, 4, 244-248, IACSIT Press, Singapore, 2011.
 15. S. Al-Maadeed, et al. “A New Chaos-Based Image-Encryption and Compression Algorithm” *Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering.*, 10, 1155, Article ID 179693, 2012.