Comparison of Image Encryption Methods Using Hybrid Frequency Domain Transforms and Chaotic Maps

Sergo Episkoposyan
National Polytechnic University of Armenia
Yerevan, Armenia
e-mail: sergo.episkoposyan@polytechnic.am

Davit Hovhannisyan
National Polytechnic University of Armenia
Yerevan, Armenia
e-mail: davithovhannisyan.mt040-1@polytechnic.am

***Abstract*—This paper presents a comparative study of hybrid image encryption algorithms combining frequency-domain transforms with chaotic scrambling. Three methods are analyzed: DCT + Arnold, WHT + Arnold, and DCT → WHT + Arnold. The Fast Walsh-Hadamard Transform (FWHT) is used to enhance computational efficiency. Cryptographic strength and reconstruction quality are evaluated using entropy, correlation coefficients, NPCR, UACI, MSE, and PSNR. Results show that WHT + Arnold (FWHT-based) offers the fastest processing with high security and lossless decryption, while the hybrid DCT → WHT + Arnold also demonstrates strong cryptographic characteristics.**

***Keywords*—Image encryption, chaos, DCT, WHT, FWHT, Arnold Cat Map, cryptanalytic metrics.**

I. Introduction

With the rapid growth of multimedia data in fields such as telemedicine, education, and defense, ensuring image confidentiality and integrity is a key challenge. Traditional ciphers like DES, AES, or RSA are applicable but computationally costly for real-time applications [1], [2], motivating specialized image encryption methods based on frequency-domain transforms and chaos theory.

Orthogonal transforms such as the Discrete Cosine Transform (DCT) and Walsh–Hadamard Transform (WHT) are promising in this context. DCT efficiently compacts energy, while WHT and its fast implementation (FWHT) are lightweight and suitable for real-time systems. Combined with chaotic maps like the Arnold Cat Map, these transforms enable strong pixel shuffling and diffusion, providing both efficiency and security [3]–[6].

This paper presents a comparative analysis of three hybrid image encryption schemes: DCT + Arnold, WHT + Arnold, and DCT → WHT + Arnold, evaluating their cryptographic strength (entropy, correlation, NPCR, UACI) and computational efficiency, highlighting trade-offs between robustness, speed, and reconstruction quality.

II. Overview of Frequency-Domain Image Encryption Methods

A. Discrete Cosine Transform (DCT)

The Discrete Cosine Transform (DCT) is widely used in image processing, particularly in compression algorithms like JPEG. DCT concentrates the main visual information of an image in low-frequency coefficients, while high-frequency coefficients contain finer details. This property is exploited in frequency-domain image encryption.

The forward 2D DCT for an $M \times N$ image is:

$$C(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \times \cos\left(\frac{\pi(2x+1)u}{2M}\right) \cos\left(\frac{\pi(2y+1)v}{2N}\right) \tag{1}$$

with

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}}, & u = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le u \le M-1 \end{cases} \tag{2}$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{N}}, & v = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le v \le N-1 \end{cases} \tag{3}$$

The inverse 2D DCT is:

$$I(x,y) = \alpha_u \alpha_v \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} C(u,v) \times \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N}. \tag{4}$$

In our proposed methods, the standard 2D DCT and its inverse are used for forward and inverse transforms, respectively.

Rademacher Functions and Walsh Basis

Rademacher functions $r_k(t)$ are ± 1-valued building blocks for the Walsh basis. [7], [8]

$$r_k(t) = \operatorname{sgn}\big(\sin(2^k \pi t)\big), \quad t \in [0,1), \tag{5}$$

$$\operatorname{sgn}(x) = \begin{cases} 1, & x \ge 0, \\ -1, & x < 0. \end{cases} \tag{6}$$

Walsh functions $w_n(t)$ are formed as products of selected Rademacher functions according to the binary expansion of n. [8]

https://doi.org/10.51408/csit2025_33

Hadamard Matrix

The Hadamard matrix H_N is defined recursively and implements the discrete WHT [8].

$$H_1 = [1], \qquad H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{bmatrix}. \tag{7}$$

For example,

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{8}$$

B. Fast Walsh-Hadamard Transform (FWHT)

The FWHT leverages the Hadamard recursion to reduce computational cost compared with a direct $O(N^2)$ implementation; for a 1-D signal of length N, the FWHT runs in $O(N \log N)$ [9].

III. Direct and Inverse WHT

The forward discrete WHT is

$$X[k] = \sum_{n=0}^{N-1} x[n]\, W_k[n], \quad k = 0, \ldots, N-1, \tag{9}$$

and the inverse transform is

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k]\, W_k[n], \quad n = 0, \ldots, N-1. \tag{10}$$

Fast algorithms and implementation details are discussed in the literature on FWHT [10].

A. Arnold Cat Map

The Arnold Cat Map is a 2D chaotic mapping that effectively scrambles image pixels [6]. It is highly sensitive to initial conditions and can significantly change element positions within an image.

For a pixel (x_i, y_i) in an $N \times N$ image, the Arnold transform is:

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & b \\ c & bc+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \pmod N \tag{11}$$

where b and c are secret parameters. The inverse transform is:

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 1 & b \\ c & bc+1 \end{pmatrix}^{-1} \begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} \pmod N. \tag{12}$$

In our methods, the Arnold Cat Map is applied to frequency-domain coefficients after DCT or WHT, not directly to pixels [6]. The implemented parameters are $b = 1$ and $c = 2$.

IV. Proposed Hybrid Encryption Methods

We investigate three hybrid image encryption algorithms combining frequency-domain transforms with the Arnold chaotic map. All methods use a secret key comprising Arnold map parameters (b, c) and the number of iterations m. Input images are square, scaled to 256×256 pixels.

A. DCT + Arnold Method

The image is transformed using 2D DCT, then the DCT coefficients are scrambled by the Arnold Cat Map for m iterations. Finally, inverse 2D DCT produces the encrypted image.

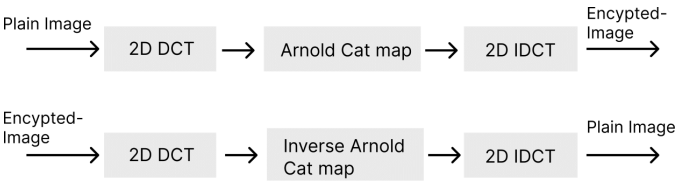

Figure 1. Scheme of the DCT + Arnold encryption algorithm

B. WHT + Arnold Method

The image is transformed using 2D WHT (FWHT), coefficients are scrambled by the Arnold map for m iterations, then the inverse 2D WHT reconstructs the encrypted image.

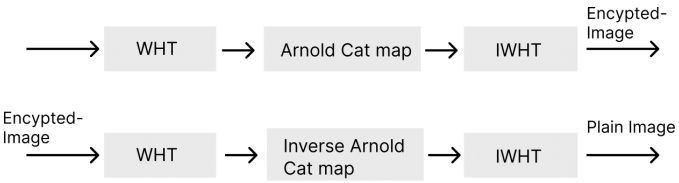

Figure 2. Scheme of the WHT + Arnold encryption algorithm

C. DCT → WHT + Arnold Method

The image undergoes 2D DCT, followed by 2D WHT (FWHT). The WHT coefficients are scrambled with the Arnold map, then inverse transforms are applied in reverse order: first inverse WHT, then inverse DCT.

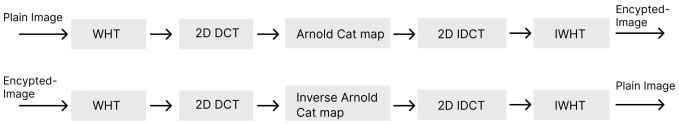

Figure 3. Scheme of the DCT → WHT + Arnold encryption algorithm

V. Experimental Setup and Cryptanalysis Metrics

Experiments were conducted on the 256×256 grayscale "Barbara" image. The Arnold Cat Map was iterated $m = 15$ times as part of the secret key.

The following metrics were used to evaluate cryptographic strength and decryption quality. Entropy measures pixel-value randomness; for an 8-bit image, values close to 8 indicate effective diffusion and resistance to statistical attacks. Entropy change is the difference between the encrypted and original image entropy; larger positive values indicate better concealment of original statistics. The Correlation coefficient quantifies the dependence of neighboring pixels. Effective encryption reduces correlations in horizontal, vertical, and diagonal directions close to zero.

NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) assess sensitivity to small input changes. High NPCR (close to 99.6%) and UACI (close to 33.4%) values indicate strong resistance to differential attacks. MSE (Mean Squared Error) evaluates the average squared difference between original and decrypted images; ideal lossless encryption yields MSE = 0. PSNR (Peak Signal-to-Noise Ratio) measures reconstruction quality; higher PSNR indicates better decrypted image quality. PSNR is computed as:

$$PSNR = 20 \times \log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{13}$$

For MSE = 0, PSNR is infinite.

VI. Results and Discussion

Figures 4, 5, and 6 show the original and encrypted "Barbara" images for the three methods. All experiments used $m = 15$ iterations of the Arnold Cat Map. In each figure, the original image is on the left and the encrypted image on the right.

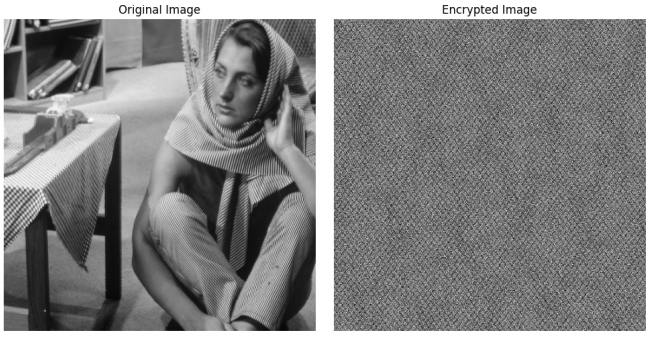

Figure 4. Original (left) and encrypted (right) images for the DCT + Arnold method

Figure 5. Original (left) and encrypted (right) images for the WHT + Arnold method

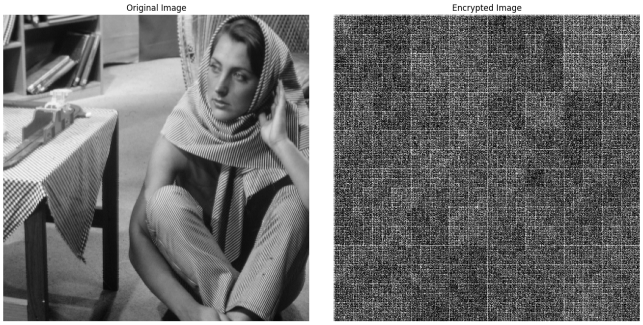

Figure 6. Original (left) and encrypted (right) images for the DCT → WHT + Arnold method

Table I compares cryptographic metrics, and Table II reports execution times for the three methods.

A. Execution Time Analysis

Table II shows significant performance differences. The WHT + Arnold method (FWHT) has the lowest encryption (0.2241 s) and decryption (0.2698 s) times due to FWHT's lower computational complexity making it suitable for real-time processing. DCT + Arnold is moderate, while the hybrid DCT → WHT + Arnold is slowest due to the sequential application of two transforms.

B. Entropy Analysis

Encrypted image entropy reflects randomness; values near 8 (for 8-bit images) indicate strong resistance to statistical attacks. Table I shows the highest entropy for WHT + Arnold (7.7181), while DCT + Arnold (7.7003) and DCT → WHT + Arnold (7.6631) also have high values. Positive entropy changes confirm increased randomness compared to the original image.

C. Correlation Analysis

Effective encryption minimizes correlations between neighboring pixels. Table I shows that all methods retain relatively high correlations, with the hybrid DCT → WHT + Arnold having the highest values (0.9550 horiz., 0.8813 vert., 0.8765 diag.), indicating less effectiveness in removing statistical dependencies. DCT + Arnold and WHT + Arnold perform slightly better.

D. NPCR and UACI Analysis

NPCR and UACI measure sensitivity to small input changes. High NPCR values (close to 99.48–99.49%) indicate that a single-pixel change significantly affects the encrypted image. UACI values (24.18% for DCT + Arnold, 22.72% for WHT + Arnold, 22.70% for DCT → WHT + Arnold) are below the ideal 33.4%, suggesting room for improvement in pixel intensity variation.

Table I
CRYPTOGRAPHIC METRICS OF THREE ENCRYPTION METHODS

Metric	DCT + Arnold	WHT + Arnold	DCT → WHT + Arnold
Entropy (Encrypted)	7.7003	7.7181	7.6631
Entropy Change	+0.0682	+0.0860	+0.0309
Correlation (Horiz.)	0.7401	0.8268	0.9550
Correlation (Vert.)	0.8091	0.8306	0.8813
Correlation (Diag.)	0.7387	0.7997	0.8765
NPCR (%)	99.49	99.48	99.48
UACI (%)	24.18	22.72	22.70
MSE	0.1071	0.0000	0.4292
PSNR (dB)	57.83	∞	51.80

Table II
ALGORITHM EXECUTION TIMES

Method	Encryption Time (s)	Decryption Time (s)
DCT + Arnold	0.6371	0.6646
WHT + Arnold (FWHT)	0.2241	0.2698
DCT → WHT + Arnold	0.8620	0.8631

E. MSE and PSNR Analysis

MSE and PSNR assess reconstruction quality after decryption. Ideal lossless decryption yields MSE = 0 and PSNR = ∞. Table I shows that WHT + Arnold achieves MSE = 0.0000 and PSNR = ∞, indicating perfect reconstruction. DCT + Arnold also has low MSE (0.1071) and high PSNR (57.83 dB). The hybrid DCT → WHT + Arnold shows slightly higher MSE (0.4292) and lower PSNR (51.80 dB), indicating minor information loss.

VII. CONCLUSION

This paper presented a comparative analysis of three hybrid image encryption algorithms combining frequency-domain transforms (DCT, WHT, FWHT) with the Arnold map. We extended prior work by investigating new hybrid combinations and evaluating their effectiveness.

Experimental results show that WHT + Arnold (FWHT-based) achieves the best performance, offering high encryption/decryption speed and perfect lossless reconstruction. All methods demonstrate high NPCR and good entropy, confirming strong information concealment. However, correlation coefficients indicate that statistical dependencies between neighboring pixels could be further reduced, particularly in the hybrid DCT → WHT + Arnold method, which, despite longer execution and minor reconstruction loss, exhibits similar statistical characteristics.

The optimal method depends on application needs: WHT + Arnold is preferable for speed and lossless reconstruction, while hybrid methods suit tasks requiring sequential processing in multiple frequency domains, with awareness of their computational cost. Future work includes optimizing transform and chaotic map parameters, enhancing resistance to attacks, applying the methods to other multimedia types, and reducing residual correlations in encrypted images.

REFERENCES

[1] S. A. Episkoposian and S. A. Grigoryan, "Hybrid Cryptographic Algorithm Based on AES, RSA and Walsh Transform," *Proc. Int. Conf. on Artificial Intelligence and Technology in Academia and Profession (CAPCDR-8th Conf.)*, Center for Academic & Professional Career Development and Research (CAPCDR), Virtual Conference, Dec. 25–26, 2024.

[2] M. A. W. Shalaby, A. A. Wahba, and M. M. Ibrahim, "Enhanced Arnold's Cat Map-AES encryption technique for medical images", in *Proc. 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, Giza, Egypt, pp. 157123–157136, 2020. DOI: 10.1109/NILES50944.2020.9257876.

[3] H. Wen, L. Ma, L. Liu, Y. Huang, Z. Chen, R. Li, Z. Liu, W. Lin, J. Wu, Y. Li, and C. Zhang, "High-quality restoration image encryption using DCT frequency-domain compression coding and chaos", *Sci. Rep.*, Nature Publishing Group, London, UK, vol. 12, art. no. 16523, 2022. DOI: 10.1038/s41598-022-20145-3.

[4] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image encryption using DCT and stream cipher", *European Journal of Scientific Research*, London, UK, vol. 32, no. 1, pp. 48–58, Jan. 2009.

[5] Ö. Kasim, "Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography algorithm", *Med. Biol. Eng. Comput.*, Springer, Heidelberg, Germany, vol. 60, pp. 1585–1594, 2022. DOI: 10.1007/s11517-022-02565-5.

[6] N. A. AbdulMohsin Abbas, "Image encryption based on Independent Component Analysis and Arnold's Cat Map", *Egyptian Informatics Journal*, Elsevier, Amsterdam, Netherlands, vol. 17, no. 1, pp. 139–146, Mar. 2016. DOI: 10.1016/j.eij.2015.10.001.

[7] S. V. Astashkin, "Rademacher System in Function Spaces", *Springer Nature Switzerland AG*, Cham, Switzerland, 2020. DOI: 10.1007/978-3-030-47890-2.

[8] A. Hedayat and W. D. Wallis, "Hadamard matrices and their applications", *Ann. Statist.*, Institute of Mathematical Statistics, Beachwood, OH, USA, vol. 6, pp. 1184–1238, 1978.

[9] J. R. Johnson and M. Püschel, "In search of the optimal Walsh–Hadamard transform", *Proc. IEEE ICASSP*, IEEE, Hilton Hotel and Convention Center, Istanbul, Turkey, pp. 3347–3350, 2000. DOI: 10.1109/ICASSP.2000.860117.

[10] M. H. Lee and M. Kaveh, "Fast Hadamard transform based on a simple factorization," *IEEE Trans. Acoust., Speech, Signal Process.*, IEEE, Piscataway, NJ, USA, vol. 34, no. 6, pp. 1666–1667, Dec. 1986.