Enhancing AES Security with the Integration of the Orthogonal Haar Transform

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

Spartak Sirakanyan
National Polytechnic University of
Armenia, Yerevan, Armenia
e-mail: sevospart@gmail.com

***Abstract*—This paper presents a hybrid encryption algorithm that integrates the orthogonal Haar Transform into the Advanced Encryption Standard (AES) framework to enhance cryptographic strength. By inserting the Haar Transform between the *SubBytes* and *ShiftRows* stages in AES-128, the proposed scheme increases confusion and diffusion, thereby improving resistance to cryptanalytic attacks. Experimental results were obtained using a fixed 128-bit key and multiple plaintext samples of varying lengths, demonstrating notable improvements in key security metrics. The avalanche effect increased from 61.0% to 73.44%, and the bitwise correlation coefficient decreased from 0.17 to 0.02, indicating near-randomness in the ciphertext. While the Shannon entropy slightly declined from 3.70 to 3.20 bits per byte due to the orthogonal nature of the transform, the overall unpredictability and structural complexity of the output were enhanced. The integration introduces a modest 7% performance overhead, which remains acceptable for applications prioritizing security, such as embedded systems, IoT devices, and secure cloud storage. The proposed AES-H algorithm offers a practical balance between computational efficiency and enhanced cryptographic robustness.**

***Keywords*—Advanced encryption standard (AES), Haar transform, hybrid cryptography, data security, avalanche effect, bit correlation, cryptographic performance, IoT security.**

I. Introduction

The need to protect confidential information has existed since ancient times. Early civilizations, such as those in Egypt and Mesopotamia, developed basic encryption schemes based on character substitution to secure military and political communications. A well-known historical method is the "Caesar cipher," which utilized a fixed shift in the Latin alphabet to obscure messages.

In the modern digital era, encryption plays a critical role in ensuring the confidentiality, integrity, and authenticity of data. Encryption algorithms are generally categorized into three main types:

- Hash functions: Convert input of arbitrary size into fixed-length outputs commonly used for password storage [1].
- Symmetric-key encryption: Use the same secret key for encryption and decryption. Examples include AES and DES [2].
- Asymmetric-key encryption: Utilize a pair of public and private keys. RSA and ECC are notable examples used for secure key exchange [3].

Among these, AES has emerged as a leading symmetric encryption standard due to its efficiency and resilience against known cryptographic attacks [4]. Nevertheless, as computational power increases and new attack strategies are developed, enhancements to existing algorithms are required.

Recent studies have explored hybrid encryption techniques that combine classical ciphers with mathematical transforms to improve security. Notable examples include the integration of Walsh transforms and RSA methods [5–8], as well as wavelet-based schemes for audio data [9]. Other works investigate combining AES with RSA or DES to harness the strengths of both symmetric and asymmetric systems [10]. In this context, the Haar Transform-a fast, orthogonal, and energy-compacting transform-offers promising cryptographic properties. Its ability to disperse and scramble data makes it a strong candidate for integration into symmetric algorithms. The research in [11] also highlights improvements to AES through nonlinear components for enhanced security in medical IoT systems. Additional studies, such as [12], have specifically investigated the use of the orthogonal Haar Transform in text information encryption, further confirming its practical relevance.

II. Haar System and Discrete Matrix

The Haar system, introduced by Alfred Haar in 1910 [13], forms a complete orthonormal basis in $L_2[0,1]$ and is widely used in signal processing and numerical analysis. The basic Haar functions $X(k,x)$ are defined as:

$$X(0,\mathrm{x}) \equiv 1$$

$$X(2^m + j, \mathrm{x}) = \begin{cases} 2^{m/2}, & \mathrm{x} \in \left[\frac{\mathrm{j}}{2^{\mathrm{m}}}, \frac{\mathrm{j}+0.5}{2^{\mathrm{m}}}\right) \\ -2^{m/2}, & \mathrm{x} \in \left[\frac{\mathrm{j}+0.5}{2^{\mathrm{m}}}, \frac{\mathrm{j}+1}{2^{\mathrm{m}}}\right) \\ 0 & \text{otherwise} \end{cases}$$

where $m = 0, 1, \dots,$ $j = 0, 1, \dots, 2^{\mathrm{m}-1}$. This system satisfies the orthonormality condition in $L_2[0,1]$:

https://doi.org/10.51408/csit2025_47

$$\int_0^1 X_n(t)\, X_m(t)\ dt = \begin{cases} 0, & n \neq m \\ 1, & n = m \end{cases}$$

Any function $f(x) \in L_2[0,1]$ can be expressed as a Haar series:

$$f(x) = \sum_{k=0}^{\infty} C_k X(k,x), \qquad C_k = \int_0^1 f(t)\, X(k,t)\ dt$$

For practical applications, especially in encryption, the Haar system is discretized into a matrix form. The discrete Haar matrix of order 2^n is denoted by $Haar_{2^n}$ and satisfies the orthogonality condition:

$$Haar_{2^n} * Haar_{2^n}^T = 2^n I_n$$

where I_n is the identity matrix. This matrix is used to implement the Haar Transform in encryption processes [14].

III. Encryption via Haar Transform

Haar-based encryption utilizes matrix multiplication for both encryption and decryption, making it symmetric and lightweight. Given a normalized and padded input vector $x \in R^{2^n}$, the transformation is defined as:

- Forward transform:

$$\mathrm{y} = Haar_{2^n}\ \mathrm{x}$$

- Inverse transform:

$$\mathrm{x} = \frac{1}{2^n}\ Haar_{2^n}^T\ \mathrm{y}$$

Due to the orthogonality, the inverse is easily computed, and no key scheduling is needed (unlike asymmetric methods).

IV. Advanced Encryption Standard (AES)

AES is a symmetric block cipher standardized by NIST, operating on 128-bit data blocks using key sizes of 128, 192, or 256 bits. The number of transformation rounds depends on the key length (Table 1).

Table 1: AES Key Sizes and Corresponding Rounds

Key Size (bits)	*Number of rounds*
128 bit	*10*
192 bit	*12*
256 bit	*14*

Each AES round includes the following operations:

- SubBytes - Byte substitution using an S-Box constructed from an inverse in GF(2^8) followed by an affine transformation.
- ShiftRows - Cyclic shifting of the rows in the 4x4 byte matrix.
- MixColumns - Column-wise transformation using a fixed matrix in GF(2^8).
- AddRoundKey - Bitwise XOR of the state matrix with a round key derived from the main key.

Table 2 summarizes the transformations per round.

Table 2: AES Transformations by Round (128-bit Key)

Round	*Transformation*
0	*AddRoundKey*
1–9	*SubBytes, ShiftRows, MixColumns, AddRoundKey*
10	*SubBytes, ShiftRows, AddRoundKey*

V. Hybrid Encryption Algorithm (AES-H)

The proposed hybrid algorithm (AES-H) integrates the Haar Transform between the SubBytes and ShiftRows stages in each AES round. This modification aims to enhance diffusion and disrupt statistical structures in intermediate states. The transformation order for AES-128 is updated as shown in Table 3.

Table 3: AES-H Transformations by Round

Round	*Transformation*
0	*AddRoundKey*
1–9	*SubBytes, Haar Transform, ShiftRows, MixColumns, AddRoundKey*
10	*SubBytes, Haar Transform, ShiftRows, AddRoundKey*

VI. Experimental Setup and Evaluation

The proposed AES-H algorithm was evaluated using the input message “Hello Armenia” (13 ASCII characters, padded to 128 bits) and a fixed AES-128 key. Several key cryptographic metrics were analyzed and compared with those of the standard AES algorithm.

In terms of entropy, the results showed that AES produced a value of 3.70 bits per byte, while AES-H achieved 3.20 bits per byte. Although slightly lower, this reduction is explained by the orthogonal nature of the Haar transform, which introduces structured patterns in the ciphertext without reducing its overall unpredictability.

When analyzing the avalanche effect, a small change in the plaintext, such as replacing the character ‘H’ with ‘J,’ caused 61.0% of the output bits to change in AES, while the proposed AES-H algorithm produced 73.44% changes. This indicates a stronger diffusion effect and a higher resistance to differential attacks.

The evaluation of bit correlation further confirmed these improvements. While the standard AES algorithm exhibited a correlation coefficient of 0.17 between plaintext and ciphertext, AES-H reduced this value to 0.02, which is very close to the properties of random data. This demonstrates that the proposed algorithm significantly increases the independence of the ciphertext from the input message.

The integration of the Haar transform introduced only a modest performance overhead of about 7% in encryption time. Despite this increase, the performance remains suitable for practical applications, particularly in IoT and embedded systems where enhanced security is often prioritized over minimal latency.

Finally, brute-force resistance was also tested on a standard personal computer (Intel i7, 16 GB RAM). The system was unable to recover the 128-bit key even after several hours of exhaustive attempts. The attack led to maximum CPU utilization and eventual system freeze, confirming that brute-force approaches are computationally infeasible against the proposed AES-H algorithm within realistic time constraints.

An experiment was conducted using data of different sizes (10 KB, 50 KB, and 100 KB), which were encrypted using both AES and AES-H (Haar Transform + AES) algorithms. Each data block was encrypted in 128-bit (16-byte) blocks. The results show that the AES-H algorithm introduces approximately a 7% increase in encryption time compared to AES, due to the inclusion of the Haar Transform. It should be noted that encryption speed depends not only on the algorithm but also on the computer, operating system, and hardware used. These results are important for evaluating the trade-off between security and performance, especially in IoT and embedded system applications.

VII. Conclusion

This paper proposed a structural enhancement to the AES-128 algorithm by inserting an orthogonal Haar Transform between the SubBytes and ShiftRows stages in each round. The primary goal was to increase the cryptographic strength of AES by enhancing diffusion and disrupting predictable byte patterns in intermediate encryption states. Experimental evaluation using a fixed 128-bit key and the input text “Hello Armenia” demonstrated measurable improvements across multiple metrics. The avalanche effect increased from 61% to 73.44%, indicating a more effective propagation of input changes throughout the ciphertext. The bitwise correlation between adjacent ciphertext bits decreased from 0.17 to 0.02, suggesting near-randomness and elimination of structural patterns. Although Shannon entropy slightly decreased from 3.70 to 3.20 bits per byte due to the orthogonal nature of the Haar Transform, this did not correspond to reduced security, as other diffusion-oriented metrics improved significantly. The hybrid implementation introduced a modest performance overhead of approximately 7%, which is acceptable for applications prioritizing cryptanalytic resistance over minimal latency. These characteristics make the proposed AES-H approach suitable for security-critical environments such as embedded systems, IoT devices, and secure cloud-based data storage. Future work may extend this approach by exploring other orthogonal transforms (e.g., Walsh–Hadamard, Daubechies), applying the method to AES-256, and evaluating resistance against advanced attack models such as differential cryptanalysis and side-channel attacks. Additionally, performance optimization and hardware-level implementations are promising directions for achieving real-time secure communication.

VIII. Funding

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

IX. Conflict of Interests

The process of writing and the content of this article do not give grounds for raising the issue of a conflict of interest.

References

[1] D. R. Stinson and M. B. Peterson, “Chapter 5”, *Cryptography Theory and Practice*, 4th ed., CRC Press, New York, NY, USA, pp. 135–176, 2018.

[2] W. Stallings, “Chapter 1”, *Cryptography and Network Security Principles and Practice*, 6th ed., Pearson, Boston, MA, USA, pp. 27–60, 2014.

[3] C. Paar and J. Pelzl, “Chapter 6”, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, Berlin, Germany, pp. 149–168, 2010.

[4] A. M. Abdullah, “Advanced encryption standard (AES) algorithm to encrypt and decrypt data”, *Cryptography and Network Security*, vol. 16, no. 11, 2017.

[5] S. A. Episkoposian, “Securing information with the Walsh transform”, *Proc. III Int. Sci. Pract. Conf.: Questions, Hypotheses, Answers – Science XXI Century*, Toronto, Canada, Sep. 2023, pp. 10–14.

[6] S. A. Episkoposian, “Application of Walsh system in data encryption”, *Tuijin Jishu/Journal of Propulsion Technology*, vol. 44, no. 3, pp. 494–502, 2023.

[7] A. S. Yepiskoposyan, “Improvement of information encryption with secret key generation using the Walsh-Hadamard transform”, *Proc. XI Int. Sci. Conf. Mathematical Sciences*, Dortmund, Germany, p. 67 Jan. 2024. DOI: 10.5281/zenodo.10564951.

[8] S. A. Episkoposian and S. A. Grigoryan, “Hybrid cryptographic algorithm based on AES, RSA, and Walsh transform”, *Int. Conf. Artificial Intelligence and Technology in Academia and Profession (CAPCDR-8th Conf.)*, 2024.

[9] D. S. Hovhannisyan and S. A. Episkoposian, “Application of Walsh transformations for encryption and decryption of audio signals”, *Int. Conf. Artificial Intelligence and Technology in Academia and Profession (CAPCDR-8th Conf.)*, 2024.

[10] V. Verma, P. Kumar, R. K. Verma, and S. Priya, “A novel approach for security in cloud data storage using AES-DES-RSA hybrid cryptography”, *Emerging Trends in Industry 4.0 (ETI 4.0)*, Raigarh, India, pp. 1–6, 2021. DOI: 10.1109/ETI4.051663.2021.9619274.

[11] X. Zhang and Y. Zhang, “Intelligent medical system data encryption based on improved AES algorithm”, *2024 7th International Conference on Computer Information Science and Application Technology (CISAT)*, Hangzhou, China, Jul. 12–14, 2024. DOI: 10.1109/CISAT62382.2024.10695219.

[12] S. Sirakanyan, “Encryption of text information using orthogonal Haar transforms”, *Modern Science: Actual Problems. Proceedings of the XVIII International Scientific and Practical Conference*, Manchester, 11–12.02.2025, ISBN 978-91-65424-07-4.

[13] A. Haar, “Zur Theorie der orthogonalen Funktionensysteme”, *Mathematische Annalen*, vol. 69, pp. 331–371, 1910.

[14] N. Ahmed and K. R. Rao, *Orthogonal Transform for Digital Signal Processing*, Springer, New York, NY, USA, 1975.