Journal link: http://kmf-publishers.com/tatscr/

Theoretical and Applied Technological Science Review

Volume: 3 Issue: 1 Year: 2025
ISSN-2958-7824

KMF PUBLISHERS

www.kmf-publishers.com/tatscr/

Journal link: http://kmf-publishers.com/tatscr/

Received: 12 January 2025 | Revised: 11 February 2025 | Accepted: 18 February 2025

DOI: https://doi.org/

Article

Application of Walsh Transformations for Encryption and Decryption of Audio Signals

Sergo A. Episkoposian[1,2]; Davit S. Hovhannisyan[1]

[1]National Polytechnic University of Armenia
Armenia
[2]Yerevan State University
Armenia

Correspondence
Davit Hovhannisyan
Master's Student
Faculty of Applied Mathematics and Physics, National Polytechnic University of Armenia, Yerevan
Armenia
Email:
david.hovhannisyan445@gmail.com
,davithovhannisyan.mt040-1@polytechnic.am

ABSTRACT

This paper explores using the Walsh-Hadamard Transform (WHT) to encrypt and decrypt audio signals. WHT, known for its computational efficiency and orthogonality properties, enables the decomposition of a signal into spectral coefficients, which can then be securely masked using a random key. Additionally, the article investigates the application of the Discrete Cosine Transform (DCT) alongside WHT and their combined variant (DCT-WHT) for encrypting and decrypting audio signals. WHT, characterized by its high computational speed, and DCT, known for its high accuracy, demonstrate significant efficiency in the encryption and decryption process [1], [2]. The study provides a detailed algorithm for preprocessing signals, including normalization, padding signal lengths to the nearest power of two, and applying forward and inverse WHT transformations. A novel masking technique is introduced, leveraging the properties of Walsh basis functions to enhance data security. Practical implementation involves converting input audio signals into WAV format, applying the WHT or the combined DCT-WHT approach, encrypting the coefficients with a random key, and reconstructing the original signal using inverse transformations. The proposed methods ensure reconstruction accuracy exceeding 99.9%, maintaining high fidelity while providing robust attack resistance. This approach efficiently transmits audio data securely in communication systems, multimedia applications, and other areas requiring robust encryption mechanisms. Additionally, the study explores the possibility of combining WHT with other signal processing algorithms, such as DCT or the Fourier Transform, to further enhance security features. The combined use of these methods improves resistance to attacks through multi-layer spectral transformation of the signal while retaining computational efficiency and noise resilience [1], [2]. The study highlights the promise of the DCT-WHT approach as a versatile and adaptable tool within modern cryptographic frameworks, offering a simple yet effective solution for the secure transmission and processing of audio data [2].

Keywords: Walsh Transform, encryption, audio signals, combined algorithm, secure communication, High computational speed.

Application of Walsh Transformations for Encryption and Decryption of Audio Signals

Our team has already been working on the encryption and decryption of text data, and ultimately, we aim to expand our research to include not only text encryption but also the encryption of audio signals[6],[7]. In this context, we conduct a comparative analysis of encryption and decryption algorithms for audio signals based on the Walsh-Hadamard Transform (WHT), Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT), Wavelet Transform, as well as their hybrid combinations, such as DCT-WHT, FFT-WHT, and Wavelet-WHT [5].

This study's primary focus is comparing algorithms' performance using WHT, DCT, and the combined DCT-WHT approach. Our research aims to evaluate these methods' resistance to various attacks, their effectiveness in reconstructing high-quality audio signals, and their applicability in diverse scenarios.

The findings highlight the potential of these approaches for developing secure and efficient cryptographic systems for processing text and audio data.

WALSH-HADAMARD TRANSFORMATIONS

Rademacher functions

The Walsh transform can be represented using Rademacher functions, which form its basis, defined by sequences of ±1 values, ensuring orthogonality and computational simplicity[4], [8].

Definition 1. Rademacher functions $r_k(t)$ It is the basis on which the Walsh transform is constructed. They are defined as:

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

where k is a non-negative integer, and $\operatorname{sgn}(x)$ Is the sign function:

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

Definition 2. The Rademacher functions are periodic, take only the values $+1$ and -1 And have the property of orthogonality:

$$\int_0^1 r_k\,(t) \cdot r_m(t)\, dt = 0, \quad \text{for} k \neq m.$$

Based on them, more complex functions are constructed, including Walsh basis functions, which form the core of the Walsh-Hadamard Transform.

Walsh-Hadamard Transform

Walsh-Hadamard Transform (WHT) — is a method of linear transformation that operates with binary signals. It uses Walsh basis functions, which can be represented as products of Rademacher functions.

Definition 3. The Walsh basis functions $w_n(t)$ Are defined as:

$$w_n(t) = r_{k_1}(t) \cdot r_{k_2}(t) \cdot \ldots \cdot r_{k_m}(t),$$

where n Is the function number in the basis, and $k_1, k_2, \ldots, k_m$ Are the indices of the Rademacher functions, which are determined by the binary representation of the number n.

These Walsh functions take values of ± 1 They possess orthogonality, which makes them useful for signal decomposition.

Hadamard matrix

The mathematical representation of the WHT involves applying the Hadamard matrix. H_N, where $N = 2^m$ It is the dimension of the transform. The Hadamard matrix is constructed recursively [1]:

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

For $N = 4$ The Hadamard matrix has the form:

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

The WHT transformation is calculated by multiplying the input data vector. $x = [x_0, x_1, \dots, x_{N-1}]$ By the Hadamard matrix:

$$X = H_N \cdot x,$$

where X Is the spectral representation of the signal.

Direct Walsh-Hadamard transform

The direct Walsh-Hadamard transform computes the spectral coefficients. $X[k]$, which reflect the contribution of the corresponding Walsh basis functions in the analyzed signal $x[n]$. The formula expresses it:

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

Where:

$x[n]$ — values of the original signal of length N,

$W_k[n]$ — Walsh basis functions, defined by the rows of the Hadamard matrix H_N,

$N = 2^m$ — the dimension of the transform (must be a power of two).

The direct transform can be represented in matrix form as:

$$X = H_N \cdot x,$$

where X and x Are vectors of length N, and H_N Is the Hadamard matrix of size $N \times N$.

Inverse Walsh-Hadamard transform

The inverse Walsh-Hadamard transform is used to reconstruct the original signal. $x[n]$ from its spectral coefficients $X[k]$. The formula defines it:

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X\,[k] \cdot W_k[n], \quad n = 0,1, \dots, N-1,$$

where $W_k[n]$ They are the same Walsh basis functions.

The matrix representation of the inverse transform is:

$$x = \frac{1}{N} H_N \cdot X.$$

Here, the same Hadamard matrix H_N It is used, but the result is scaled by $\frac{1}{N}$ To restore the original signal values[1].

SIGNAL ENCRYPTION AND DECRYPTION ALGORITHMS BASED ON WHT AND DCWT

Walsh-Hadamard transform method

This figure shows a signal encryption and decryption algorithm diagram using only WHT.

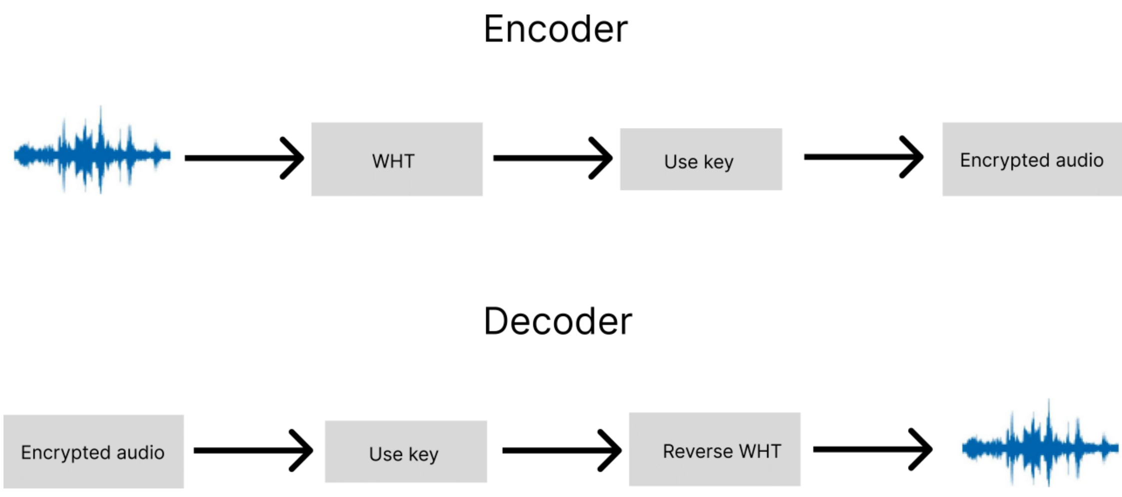

Figure 1: Audio encryption and decryption using WHT

Encryption consists of several stages. At the first stage, the signal is divided into blocks. Then, a transformation is applied using the WHT method (Walsh-Hadamard Transform). After that, the signal is masked using a key, resulting in an encrypted signal.

Decryption begins with obtaining the encrypted signal, which is divided into blocks. Then, de-Masking is performed using the same key. Afterward, the inverse WHT is applied, allowing for the reconstruction of the original signal.

Discrete Cosine Walsh-Hadamard transform method

The figure shows a diagram of the signal encoding and decoding algorithm using DCT-WHT (DCWT).

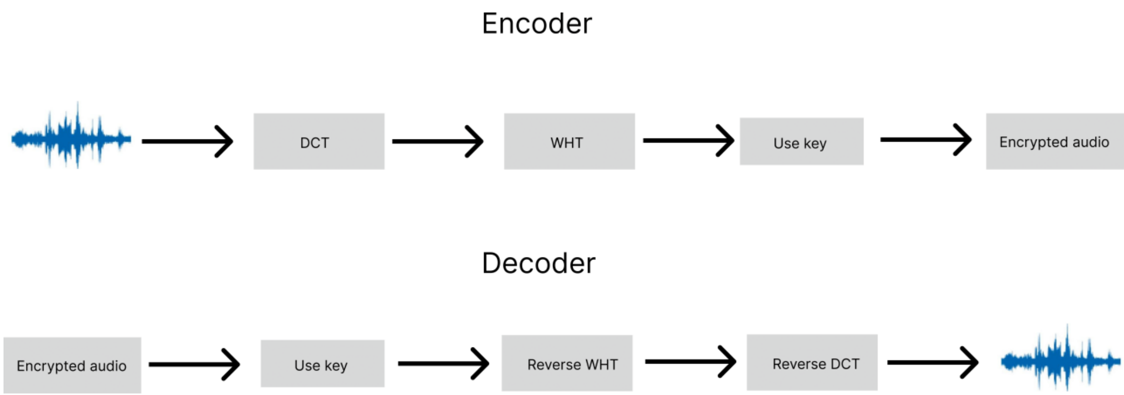

Figure 2: Audio encryption and decryption scheme using DCWT

Encryption consists of several stages. At the first stage, the signal is divided into blocks. Then, Discrete

Cosine Transform (DCT) is applied, followed by the Walsh-Hadamard Transform (WHT). After that, the signal is masked using a key, resulting in an encrypted signal.

Decryption consists of several stages. At the first stage, the encrypted signal is divided into blocks. Then, de-masking is performed using the same key. After that, the inverse Walsh-Hadamard Transform (WHT) is applied. Then, the inverse discrete cosine transform (DCT) is performed, which allows for reconstructing the original signal.

COMPARISON OF WALSH-HADAMARD TRANSFORM (WHT) WITH OTHER METHODS

Comparison of the Walsh-Hadamard Transform (WHT) with other methods

For comparison of the Walsh-Hadamard Transform (WHT), let's consider several methods of linear transformation, including three widely used methods, as well as their combinations, defined as follows:

- Walsh-Hadamard Transform (WHT)
- Discrete Cosine Transform (DCT)
- Combined method DCT + Walsh (DCWT)

Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) transforms a signal into the frequency domain with real coefficients. For DCT-II, the most commonly used form of DCT [2], the direct transform is defined as:

$$X[k] = \sum_{n=0}^{N-1} x\,[n] \cdot \cos\left(\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right).$$

The inverse DCT:

$$x[n] = \frac{1}{N}\sum_{k=0}^{N-1} X\,[k] \cdot \cos\left(\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right).$$

Definition 4. DCT effectively concentrates the signal's energy into the first few coefficients, making it suitable for data compression tasks[3], such as images and audio files. The combined method DCT + Walsh (DCWT) combines the Discrete Cosine Transform (DCT) with WHT. First, DCT is applied, followed by WHT.

DCT-II is defined as:

$$X_{\mathrm{DCT}}[k] = \sum_{n=0}^{N-1} x\,[n] \cdot \cos\left(\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right).$$

WHT for $X_{\mathrm{DCT}}[k]$:

$$X_{\mathrm{DCWT}}[m] = \sum_{k=0}^{N-1} X_{\mathrm{DCT}}\,[k] \cdot W[k,m].$$

Comparison results

The comparison results presented in the table help determine which method or combination of methods is best suited for audio encoding and decoding, which requires an optimal balance between quality, reliability, and execution time.

Table 1: Comparison of Metrics for Different Methods

Method	Correlation	Reliability correlation (Encoded)	Running time (s)
Walsh	0.99992	0.00021630	0.0091362
DCT	0.99993	0.0065493	0.0112780
DCWT	0.99993	-0.00065884	0.017694

Evaluation Metrics

This study focuses on evaluating the effectiveness of these methods based on the following key metrics:

Correlation Quality (Correlation): This shows the degree of preservation of the original data. High correlation values indicate minimal changes in the data after processing.

Encoding Reliability (Reliability correlation (Encoded)): correlation between the original and encoded signals. Low values indicate more reliable encoding and better separation of the original and encoded signals.

Running Time: the time spent executing the algorithm, critical for assessing performance.

The results can be summarized as follows:

Correlation Quality (Correlation) The Walsh, DCT, and DCWT methods demonstrate very high correlation values (0.99992–0.99993), indicating their ability to distort the original data after minimal processing.

Encoding Reliability (Reliability correlation (Encoded)) The lowest values of *Reliability correlation (Encoded)* are observed in the *DCWT* method (-0.00065884), making it the most reliable for tasks that require significant data changes. The methods *Walsh*, *DCT*, and *DCWT* have positive correlation values, indicating minimal changes to the data after encoding.

Running Time (Running time) Walsh is the fastest method (0.0091362 seconds), making it efficient for time-constrained tasks. The methods *DCT* and *DCWT* have similar running times (0.0091362–0.017694 seconds), making them suitable for medium-intensity tasks.

GENERAL CONCLUSION

The *Walsh* method is preferred due to its high correlation and minimal running time.

The *DCT* method may be optimal for tasks that balance reliability and performance.

Despite slightly higher running time, the DCWT method suits tasks requiring high encoding reliability.

Here are the plots of the time-domain signals before encoding, after encoding, and after decoding.

PLOTTING RESULT

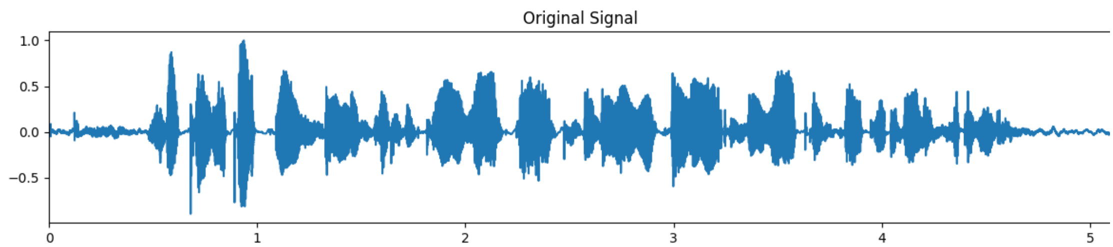

Figure 3: Plotting the original sound

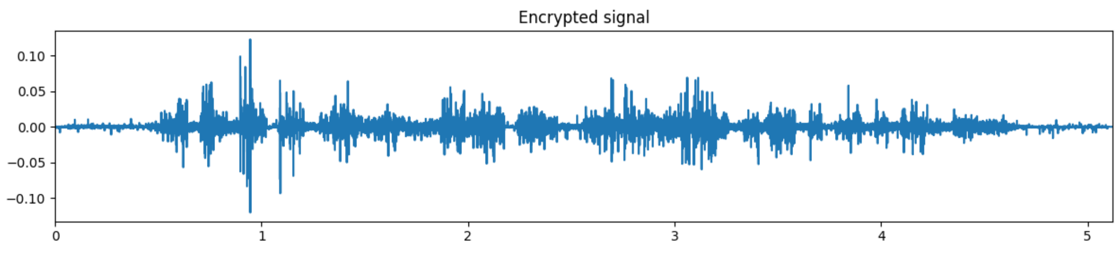

Figure 4: Plotting the Encrypted audio

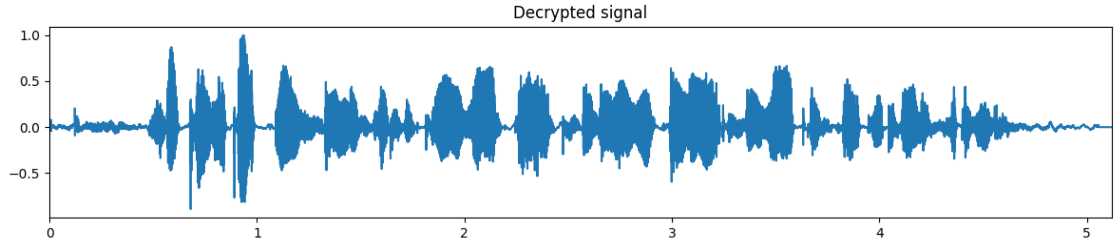

Figure 5: Plotting the Decrypted audio

REFERENCES

[1] Farsana, F. J., Devi, V. R., & Gopakumar, K. (2020). An Audio Encryption Scheme Based on Fast Walsh-Hadamard Transform and Mixed Chaotic Keystreams. Applied Computing and Informatics.

[2] G. Alzeer and H. Alhumyani, "Efficient Audio Encryption Using a Discrete Cosine Transform and Baker Map," 2022 Fifth National Conference of Saudi Computers Colleges (NCCC), Makkah, Saudi Arabia, 2022, pp. 201-208, doi: 10.1109/NCCC57165.2022.10067440.

[3] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," IEEE Trans. Comput., vol. C-23, no. 1, pp. 90–93, Jan. 1974, doi: 10.1109/T-C.1974. 223784.

[4] N. Ahmed and K. R. Rao, "Orthogonal transforms for digital signal processing," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.

(ICASSP), Philadelphia, PA, USA: Springer-Verlag, 1975, pp. 136–140, doi: 10.1109/ICASSP.1976.1170121.

[5] Rabiner, L., & Schafer, R. W. (1978). "Digital Processing of Speech Signals". Prentice-Hall.

[6] Episkoposian S.A., Securing information with the Walsh transform, Proceedings of the III International Scientific and Practical Conference. Questions, hypotheses. Answers: science XXI century, September 12-13, 2023, p. 10 – 14, Toronto. Canada.

[7]. Episkoposian S.A., Application of Walsh system in Data Encrypition, TuijinJishu/Journal of Propulsion Technology, Vol. 44, No. 3, 2023, p. 494 – 502 .

[8]. Rademacher System in Function Spaces. (2020). Springer. Retrieved from https://link.springer.com/book/10.1007/978-3-030-47890-2