Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 3 (2023)

Application of Walsh System in Data Encryption

Sergo A. Episkoposian
Faculty of Applied Mathematics and Physics,
National Polytechnic University of Armenia, Armenia

Abstract: This article explores the application of the Walsh system in modern data encryption methods. The advantages and limitations of this system are reviewed and its effectiveness is analyzed in comparison to other encryption schemes. The article describes the mathematical basis of the Walsh transform, its use for encryption and decryption, and its practical applications. In conclusion, prospects for further research in this area are considered.

Keywords: *Cryptography, Walsh Hadamard Transform, Data Encryption , Data Security*

I. Introduction

Data encryption is an important field of information security, which aims to ensure the confidentiality and integrity of information during transmission and storage. In the modern digital world, the issue of encryption is becoming more and more important as technology develops and new threats constantly emerge. Various methods and algorithms have been used to solve this problem, including methods based on mathematical transformations such as the Walsh transform. The Walsh transform, also known as the Walsh-Hadamard transform, is a powerful tool in the fields of signal processing, information theory, and cryptography. It allows you to represent data as a combination of basic Walsh functions, which have the properties of orthogonality and normalization. These properties make the Walsh transform useful for both data analysis and encryption. Over the past decades, the Walsh transform has been the subject of active research in cryptography and data encryption. A lot of research is focused on the analysis and application of this transformation to ensure the security and confidentiality of information. The studies present a variety of approaches and methods using the Walsh system to encrypt various types of data. However, despite numerous studies, there are open questions and directions for further research. The security, attack resistance, and effectiveness of Walsh-based encryption methods still require further analysis and research. The scope of the Walsh system can also be extended to other areas of information security and cryptography.

In this paper, we examine the main aspects of the Walsh system, consider encryption methods based on this transformation and analyze their strengths and weaknesses. We will also review examples of research and publications in this field to support our analysis and conclusions. The Walsh transform is a linear transform that can be used for signal analysis, data processing, and information encryption. It is based on the Walsh matrix, which is orthogonal and contains elements equal to 1 and -1. The Walsh transform allows you to decompose the original data into basis functions that have the properties of orthogonality and normalization. These properties make it a useful tool for data processing and presentation. There has been a lot of research and development in the area of application of the Walsh Transform in data encryption ([1]-[9]). An important direction is the analysis of the effectiveness of the Walsh system in comparison with other encryption methods. These studies demonstrate multiple data encryption methods and approaches based on the Walsh system and evaluate their effectiveness and security. However, despite extensive research efforts, further research is still needed to improve encryption methods and their applications in various fields. The purpose of this paper is to consider the application of the Walsh system to data encryption and to identify its advantages and limitations. We will first study the properties of the Walsh system and its mathematical basis and then describe encryption methods based on this system. Next, we consider the pros and cons of using the Walsh system for

data encryption and provide examples of its application. Finally, we summarize our findings and discuss prospects for further research in this area.

Ii. Orthonormal Walsh System

Walsh functions have been introduced in mathematics in 1923 by Joseph L. Walsh [1]. They constitute a complete set of orthogonal func-tions which assume only the values +1 and –1. The Walsh system is an orthonormal set of functions that finds wide application in signal process-ing, including encryption tasks. Consider the main properties of the Walsh system and their mathematical justification.

Orthonormal: The Walsh system consists of Walsh functions that are orthonormal on the interval [−1,1]. Orthonormal means that the product of the scalar products of two different Walsh functions is equal to zero, and for the same function this product is equal to 1:

$$\langle W_m, W_n \rangle = \int_{-1}^{1} W_m(x) \cdot W_n(x) dx = \begin{cases} 1, & \text{если } m=n, \\ 0, & \text{если } m \neq n, \end{cases}$$

Normalization: Each Walsh function is normalized, which means that the square of the integral over its square is 1:

$$\int_{-1}^{1} W_n^2(x) dx = 1.$$

Orthogonality concerning other features: The Walsh functions are orthogonal concerning other orthonormal systems, such as the Legendre, Chebyshev and others functions.

Walsh transform: The Walsh transform allows you to represent a function as a sum of Walsh functions. For a continuous function f(x) on [−1,1], the Walsh transform is defined as follows:

$$W[f](n) = \int_{-1}^{1} f(x) \cdot W_n(x) dx.$$

Inverse Walsh transform: The inverse Walsh transform allows you to restore the original function from its Walsh transform:

$$f(x) = \sum_{n=0}^{\infty} W[f](n) \cdot W_n(x).$$

Discrete Walsh transform: For discrete data with N elements, the Walsh transform has the form:

$$f(x) = \sum_{n=0}^{\infty} W[f](n) \cdot W_n(x).$$

Orthogonality in the discrete case: In the discrete case, Walsh functions form an orthonormal basis, and they can be used to represent data as a linear combination of Walsh coefficients.

$$W[f](n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N} f(k) \cdot W_n\left(\frac{2k}{N} - 1\right).$$

The Walsh system, due to its mathematical properties, finds application in various fields, including data encryption.

Walsh matrix: In mathematics, a **Walsh matrix** is a specific square mat-rix of dimensions 2^n, where n is some particular natural number. The entries of the matrix are either +1 or −1 and its rows as well as columns are orthogonal, i.e. dot product is zero. The Walsh matrix was proposed by Joseph L. Walsh in 1923 [1]. Each row of a Walsh matrix corresponds to a Walsh function. The Walsh matrices are a special case of Hadamard matrices. The naturally ordered Hadamard matrix is defined by the recur-sive formula below, and the

sequencyordered Hadamard matrix is formed by rearranging the rows so that the number of sign changes in a row is in increasing order [2]. Walsh-Hadamard matrices can be determined by the following simple rule:

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \; H_8 = \begin{bmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{bmatrix} \text{ etc.}$$

Iii. Encryption Methods. Pros And Cons, Disadvantage

There are several encryption methods ([3] – [9]). Let's consider some of them:

1. Symmetric encryption (Caesar cipher):

When encrypting with a Caesar cipher, each letter in the message is shifted to a certain number of places in the alphabet. For example, if you move 3 positions, "A" will become "D", "B" will become "E", and so on. Decryption is performed with a reverse shift.

Pros:

- Speed: Symmetric encryption is faster because it requires fewer compu-ting resources.
- Simplicity: Easy to implement and use, making it a popular choice for fast encryption.

Cons and disadvantages:

-Key exchange: Requires the exchange of aprivate key between the sender and receiver.

-Security: If the key is compromised,anattacker can easily decrypt the data.

2. Asymmetric (public) encryption (RSA):

In RSA, each user has a pair of public and private keys. The public key is used to encrypt data and the private key is used to decrypt data. The sen-der encrypts the message using the recipient's public key, and only the recipient with the corresponding private keycan decrypt it.

Pros:

- No Key Exchange: Allows secure communication without the need to exchange secret keys.
- Digital Signatures: Used to create digital signatures that provide authentication and non-repudiation.

Cons and disadvantages:

- Computational complexity: Asymmetric encryption requires more computational resources than symmetric encryption.
- Slower: Compared to symmetric encryption, asymmetric encryption is slower.

3. Hash-based encryption (HMAC):

HMAC uses hash functions to generate a message authentication code, which is a short hash computed from a key and data. A message authen-tication code is added to the message and ensures the authenticity and integrity of the data.

Pros:

- Data Integrity: Hash functions are used to check the integrity of data.

- Fast: The generation of hash values is fast.

Cons and disadvantages:

- Irreversibility: Hash functions are one-way, making it impossible to recover the original data.
- Collisions: Collisions can occur when different inputs match the same hash value.

4. Quantum Encryption:

Quantum cryptography is a new approach, completely different from classical cryptography, which uses the quantum nature of particles to guarantee the secure transmission of information. The main idea of quantum cryptography is to use the principles of continuity and unpre-dictability of quantum states to generate keys and transmit data.

Pros:

- Real-time protection: Allows you to detect any eavesdropping or hacking attempts.
- Quantum Authentication: Provides authentication without the possibility of key interception.

Cons and disadvantages:

- Complexity: Requires specialized hardware and software solutions.
- Computational requirements: Quantum encryption requires high computing power.

Encryption methods using the Walsh system are based on applying a Walsh transform to the original data, which results in an encrypted repre-sentation of the data in terms of Walsh coefficients. These methods provide an uncorrelated transformation of the data, which makes it resistant to frequency attacks.

Iv. Aoolication Of The Walsh-Hadamard Transform

The Walsh transform, as a mathematical method, can be catego-rized as symmetric encryption. This is because the Walsh transform is based on the use of an orthonormal system of functions that is common to both sides (sender and receiver). Both parties use the same system of functions to encrypt and decrypt data.

The Walsh transform does not require asymmetric keys and can be applied on both the sender and receiver side using a shared key to trans-form and detransform the data. This makes the Walsh transformation easier to implement and less computationally demanding than asymmetric methods. However, it is worth noting that the Walsh system also has its limitations and vulnerabilities, like any other encryption method.

When data is encrypted using the Walsh transform, the original data is represented as a vector of values. The Walsh transform is performed by multiplying the Walsh matrix by the original data vector. The resulting Walsh coefficients are encrypted data.

Text message encryption:

The application of the Walsh system for encrypting text data is based on converting the text into a number format, which is then sub-jected to a Walsh transform.

Consider a text message M , consisting of characters m_i , Where i - character index. Each character can be associated with its ASCII code (integer), let's denote it as $a_i = \mathbf{ord}(m_i)$.

Example:

Let's say we have the message "Hello, World!". Assign each character to its ASCII code:

H ->72, e ->101,l ->108,l ->108, o ->111, , ->32, W ->87, o ->111, r ->114,l ->108, d ->100, ! -> 33

Let's create a vector X = [72, 101, 108, 108, 111, 32, 87, 111, 114, 108, 100, 33], which will represent our text message.

Applying the Walsh Transform to a Vector x happens like this:

Let us have the original vector $X = \{x_1, x_2, ..., x_n\}$ length n, which contains data, such as a text message, that we want to encrypt. Applying the Walsh Transform to a Vector X reduces to multiplying the original vector by the Walsh transformation matrix. The result of this multiplication will be a new vector of coefficients $W = \{w_1, w_2, ..., w_n\}$ which will represent the encrypted message.

Let H - Walsh-Hadamard matrix, size $n \times n$. The Walsh transform is performed as follows: $W = H \cdot X$, where the symbol «$\cdot$» denotes the matrix multiplication. In the context of data encryption, the resulting vector of coefficients W represents an encrypted message. Since the Walsh matrix has certain properties of orthogonality and normalization, the encryption and decryption process can be efficiently implemented using the inverse Walsh transform.

It is important to note that in real encryption applications, applying the Walsh transform may be accompanied by additional steps such as choosing meaningful coefficients, adding a key to improve security, and so on.

Text message decryption:

To decrypt an encrypted message, an inverse Walsh transform must be performed. The

inverse transform allows you to recover the original data from the encrypted coefficients

obtained after applying the Walsh transform.

Let us have an encrypted vector of coefficients $W = \{w_1, w_2, ..., w_n\}$, which is the result of applying the Walsh transform to the original data vector. To decrypt, we need to follow the following steps:

1. Inverse Walsh Transform: For coefficient vector W perform the inverse Walsh transform. For this we need the inverse matrix H^{-1} to the Walsh matrix H. The inverse matrix allows you to perform the inverse transformation and restore the original data.

The inverse Walsh transform can be written as follows:

$$m = H^{-1} \cdot W$$

Where $m = \{m_1, m_2, ..., m_n\}$ is a vector of decrypted characters representing the original message.

2. calculation m: Calculate vector of decoded characters m done by inverse matrix multiplication H^{-1} to the vector of coefficients. This restores the original characters that were encrypted using the Walsh transform.

Thus, after performing the inverse Walsh transform, we get a vector of decrypted characters m that contains the original message, which can be interpreted and read.

It is important to note that in real encryption applications, the inverse Walsh transform can also be accompanied by additional steps, such as removing additional characters, restoring the original message length, and so on.

V. An Example Of Decryption

Let's understand in detail how the program for encrypting and decrypting text messages using the Walsh system works. To do this, imagine two users, Alice (sender) and Bob (receiver), located in different cities, and explain how they can exchange encrypted messages.

Prior Knowledge:

1. Users must have access to the executable version of the program with code for encryption and decryption.
2. They must know how to exchange encrypted and decrypted messages.

Messaging process:

1. **Alice (Sender):**

- Alice has access to the executable version of the program, including functions for encrypting and decrypting text messages using the Walsh system.
- She types her text message like "Hallo Armenia".
- Using the encrypt_message() function, similar to the code we provided earlier, Alice encrypts her message into a binary format using the Walsh system.
- The encrypted data is ready to be sent.

For example, the following Python code:

Code of Alice

```
import numpy as np
# Walsh transform
def walsh_transform(data):
    n = len(data)
    transform_matrix = np.zeros((n, n), dtype=int)
    for i in range(n):
        for j in range(n):
            transform_matrix[i, j] = (-1) ** (bin(i & j).count('1'))
    return np.dot(transform_matrix, data)
# Text Message Encryption
def encrypt_message(message):
    message = message.lower()
    message_length = len(message)
    padded_length = 2 ** int(np.ceil(np.log2(message_length)))
    padded_message = message.ljust(padded_length, ' ')
    binary_message = np.array([ord(char) for char in padded_message], dtype=int)
    encrypted_data = walsh_transform(binary_message)
    return encrypted_data
# Usage example
original_message = "Hallo Armenia"
encrypted_message = encrypt_message(original_message)
print("Original message:", original_message)
print("Encrypted message:", encrypted_message)
```

Original Post: Hallo Armenia

Encrypted message: [1389 147 -23 171 295 -107 -17 -151 153 -9 -143 35 -169 -3 123 -27]

1. **Bob (Recipient):**

- Bob also has access to an executable version of the program to encrypt and decrypt using the Walsh system.
- He expects to receive encrypted data from Alice.

2. **Encrypted data exchange:**

Alice sends the data received from encryption to Bob:[1389, 147, -23, 171, 295, -107, -17, -151, 153, -9, -143, 35, -169, -3, 123, -27]

- This could be through the Internet, email, instant messengers, etc.

3. **Bob (Recipient):**

- Bob receives encrypted data from Alice.
- It uses the decrypt_message() function similar to the code you provided earlier to decrypt the data. This function will perform the inverse Walsh transform and restore the original text message.

The code for Bob will decrypt the encrypted data that was sent to him by Alice. Here's what the code for Bob might look like:

Code of Bob

```
import numpy as np
# Inverse Walsh Transform
def inverse_walsh_transform(data):
    n = len(data)
    transform_matrix = np.zeros((n, n), dtype=int)
    for i in range(n):
        for j in range(n):
            transform_matrix[i, j] = (-1) ** (bin(i & j).count('1'))
    return np.dot(transform_matrix, data) / n
# Decrypt Text Message
def decrypt_message(encrypted_data):
    decrypted_data = inverse_walsh_transform(encrypted_data)
    decrypted_message = ''.join([chr(int(round(val))) for val in decrypted_data])
    return decrypted_message.strip()
# Encrypted message received from Alice
encrypted_message_from_alice = np.array(
    [1389, 147, -23, 171, 295, -107, -17, -151, 153, -9, -143, 35, -169, -3, 123, -27],
    dtype=int)
# Decrypt and message output
decrypted_message = decrypt_message(encrypted_message_from_alice)
print("Decrypted message:", decrypted_message)
```

- The decrypted message will "Hallo Armenia".

Thus, Alice and Bob can exchange encrypted and decrypted messages using a program for encryption and decryption based on the Walsh system. For successful messaging, both users must know how to use the program and how to transfer encrypted data between them.

V. Conclusion

In this review scientific article, the principles of using the orthonormal Walsh system in data encryption were considered. We have studied the basic mathematical aspects of the Walsh system, including its definition, the properties of orthogonality and normalization of basis functions, and Walsh transform and inverse transform methods.

The Walsh system provides an efficient way to represent data as transform coefficients, which makes it useful for data encryption. The use of encryption methods based on the Walsh system has its advantages, such as speed, mathematical properties and the absence of feedback between the coefficients. However, some drawbacks should be taken into account, such as vulnerability to statistical analysis, the need for key exchange, and sensitivity to errors.

Outlook:

Further research into the use of the Walsh system in data encryption may lead to the development of more sophisticated and efficient encryption methods that are resistant to modern attacks. The following prospects and directions of research are possible:

1. **Security improvement:** Research aimed at increasing the resistance of the Walsh system to attacks, including the development of new encryption algorithms and data processing methods.
2. **Research into new areas of application:** The application of the Walsh system can be extended to other areas such as image, video and sound encryption, as well as in the field of quantum cryptography.
3. **Research of hybrid methods:** Research on hybrid encryption methods that combine the Walsh system with other modern encryption methods to achieve a higher level of security and efficiency.
4. **Adaptation to new technologies:** Application of the Walsh system in the context of modern technologies such as cloud computing, mobile applications and the Internet of things.
5. **Development of tools and libraries:** Creation of software tools and libraries that simplify the implementation and use of the Walsh system in various applications.

In conclusion, the Walsh system remains an interesting and relevant topic for research in cryptography and information security. Its mathematical properties and potential for developing new encryption methods make it an important tool for data privacy and security.

References

[1]. J. Walsh, A closed set of normal orthogonal functions, Amer. J. Math., vol. 45, no 1, pp. 5– 24, 1923.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[2]. P. P. Kanjilal, Adaptive Prediction and Predictive Control, IET., 1995.R. Nicole, “Title of paper with only first word capitalized,” Journal name, in press.
[3]. KJ . Horadam, Hadamard Matrices and Their Applications, Princeton University Press, 2007.
[4]. Yi . Lu, Y. Desmedt, Walsh transforms and cryptographic applications in bias computing, Cryptography and communications, vol.8, no 3, pp. 435–453, 2016.
[5]. G. Sharma, A. Kakkar, Cryptography Algorithms and approaches used for data security, International Journal of Scientific & Engineering Research, vol. 3, no. 6, pp. 1-6, 2012.
[6]. A. Tushar, P.,KulhalliK, Symmetric Key Cryptography Algorithm for Data Security, International Journal of Trend in Scientific Research and Development, vol. 2, no 2, pp. 586 - 589, 2018.

[7]. L. Bertram, D. Gunther van, et al. (Eds.), Nomenclatura: Encyclopedia of modern Cryptography and Internet Security - From Auto Crypt and Exponential Encryption to Zero-Knowledge-Proof Keys, Books on Demand: Paris, France, 2019.
[8]. F. Piper, S. Murphy, Cryptography: A Very Short Introduction, Oxford University Press, 2002.
[9]. W. Diffie, M. Hellman, New Directions in Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 22, no. 6, pp. 644 – 654, 1976.