10.48047/jocaaa.2022.30.02.24

# Spectral Analysis of Cryptographic Hash Functions Using Fourier Techniques

Raghava Chellu

Email : raghava.chellu@gmail.com

Affliation : Equifax Inc

## Abstract

This paper explores the application of Fourier spectral analysis to evaluate the security properties of cryptographic hash functions, offering a novel approach to assessing their robustness beyond traditional time-domain methods. By examining key spectral features such as spectral density, entropy, and frequency distribution, the study reveals how these characteristics correlate with vulnerabilities like collision resistance and pre-image resistance. The results demonstrate that Fourier analysis provides valuable insights into the weaknesses of hash functions, highlighting the potential for improving cryptographic design. Furthermore, the paper discusses future directions, including the application of this method to post-quantum cryptographic algorithms and the development of automated tools for Fourier-based evaluation.

**Keywords**: Fourier analysis, cryptographic hash functions, spectral analysis, entropy, collision resistance.

## 1. Introduction

Cryptographic hash functions are essential building blocks in the realm of digital security, facilitating crucial roles such as ensuring data integrity, providing authentication, and supporting various cryptographic protocols. These functions are widely used across a variety of systems, from blockchain technologies to secure communications and file verification. However, despite their fundamental importance, the analysis of cryptographic hash functions has traditionally been centered around their time-domain properties, such as their randomness, collision resistance, and pre-image resistance. These properties are typically evaluated using statistical methods and

10.48047/jocaaa.2022.30.02.24

cryptographic tests that assess how well the function performs in terms of its security properties, such as its ability to resist cryptographic attacks. Nonetheless, much of the analysis has not delved deeply into the frequency-domain characteristics of these hash functions. This paper seeks to introduce a novel approach by applying Fourier-based spectral analysis to cryptographic hash functions. By examining these functions from the frequency domain perspective, we aim to uncover potential vulnerabilities and gain a deeper understanding of their cryptographic robustness, which may not be readily apparent through traditional analysis methods (Menezes, Oorschot, & Vanstone, 1997).

Fourier transforms, a powerful tool in signal processing and cryptography, have long been used to analyze block ciphers and other cryptographic algorithms (Biedenkapp & Shoup, 2012). These techniques can reveal valuable insights into how a cryptographic system behaves under different conditions, particularly in identifying patterns and irregularities that might indicate weaknesses. However, despite their utility in cipher analysis, Fourier techniques have been underutilized in evaluating cryptographic hash functions, which play a pivotal role in modern cryptographic systems. Existing research has mainly focused on time-domain evaluations, such as ensuring randomness and resistance to collisions, while overlooking how these hash functions perform in the frequency domain. This study addresses this gap by applying spectral analysis to cryptographic hash functions, focusing on their frequency-domain features such as spectral entropy and power spectral density. This approach aims to reveal hidden patterns that might expose vulnerabilities in commonly used hash functions, providing a more comprehensive evaluation framework that complements existing methods and can potentially identify weaknesses that traditional tests may miss.

The primary objective of this research is to apply Fourier transforms to conduct a spectral analysis of widely used cryptographic hash functions, such as SHA-256, MD5, and BLAKE2. By focusing on the frequency domain, we intend to explore how key cryptographic attributes— such as collision resistance and pre-image resistance—relate to the spectral properties of these functions. These

10.48047/jocaaa.2022.30.02.24

properties are often evaluated in time-domain contexts, but examining them in the frequency domain could yield additional insights into their cryptographic security.

Moreover, this study aims to investigate how frequency-domain features such as spectral entropy, which measures the level of randomness or unpredictability in the hash output, and power spectral density, which examines how energy is distributed across different frequency components, contribute to the security attributes of the hash functions. By doing so, we will assess how these features correlate with common cryptographic vulnerabilities and attacks, such as collision attacks and side-channel cryptanalysis (Gong & Zhang, 2017). By identifying how certain spectral patterns might correspond to weaknesses in a hash function, this paper will lay the groundwork for a new evaluation methodology that adds an additional layer of security analysis to the cryptographic assessment of hash functions. Ultimately, the goal is to provide a more comprehensive understanding of how cryptographic hash functions behave and how Fourier-based spectral analysis can be integrated into existing evaluation practices to improve the security of cryptographic system

## 2. Background and Related Work

Cryptographic hash functions are a critical component in the field of cryptography, serving as one of the most fundamental tools for securing data. These functions take an input, or "message," and produce a fixed-size output, commonly referred to as a hash value or digest. Cryptographic hash functions play a pivotal role in various cryptographic protocols, such as blockchain systems, digital signatures, and data integrity verification (Menezes, Oorschot, & Vanstone, 1997). For instance, in blockchain, they help to secure transaction data by producing a unique hash that serves as a fingerprint for each block, ensuring the integrity of the entire chain. Similarly, in digital signatures, hash functions ensure the authenticity and integrity of messages, as any alteration in the message content would change the resulting hash and thus invalidate the signature.

The security of cryptographic hash functions is primarily defined by three key properties: collision resistance, pre-image resistance, and second pre-image resistance. Collision resistance ensures that

10.48047/jocaaa.2022.30.02.24

it is computationally infeasible to find two distinct inputs that result in the same hash value. Pre-image resistance means that, given a hash value, it should be computationally hard to find any input that hashes to it. Second pre-image resistance ensures that, given an input and its corresponding hash, it is difficult to find a different input that produces the same hash. These properties make hash functions robust tools for securing digital information against various types of cryptographic attacks. Current methods used to assess the security of hash functions often involve statistical analysis, testing for uniformity in the hash outputs, and evaluating how well the hash function resists collision and pre-image attacks. While these methods are effective, they primarily focus on the hash function's time-domain properties, leaving the frequency-domain analysis largely unexplored.

The Fourier transform is a mathematical tool that decomposes a function (or signal) into its constituent frequencies. In cryptanalysis, Fourier transforms have been employed to analyze various cryptographic algorithms, particularly block ciphers and stream ciphers. By transforming data from the time domain to the frequency domain, cryptanalysts can detect patterns or irregularities that are not readily visible in the original data. This ability to reveal hidden patterns is particularly important in the context of cryptanalysis, where the goal is often to uncover weaknesses in cryptographic systems, such as predictability or repetitions that could facilitate an attack.

Previous research has shown that Fourier-based techniques can be effectively used in cryptanalysis to assess the security of encryption systems (Swaminathan et al., 2006; Biedenkapp & Shoup, 2012). For example, Fourier analysis has been applied to block ciphers to detect weaknesses in their diffusion and confusion properties—two essential elements of secure encryption algorithms. Fourier techniques can also help identify potential side-channel vulnerabilities, where an attacker might exploit patterns in the encryption process (e.g., power consumption, electromagnetic leaks, etc.) to deduce the secret key. These insights suggest that applying Fourier transforms to the analysis of cryptographic hash functions could reveal new vulnerabilities that might not be detected through conventional statistical or time-domain testing.

10.48047/jocaaa.2022.30.02.24

While Fourier transforms have been successfully applied in the analysis of block ciphers and stream ciphers, their use in evaluating cryptographic hash functions remains limited. Most cryptographic analysis focuses on the time-domain behavior of hash functions, such as their ability to generate random-looking outputs and resist known attack methods. However, the frequency- domain characteristics of hash functions have been largely unexplored, especially in terms of how they relate to key cryptographic properties like collision resistance and pre-image resistance. This lack of focus on the frequency domain represents a significant research gap.

By applying Fourier spectral analysis to cryptographic hash functions, this paper aims to fill this gap and uncover potential weaknesses that might be present in the frequency domain. Specifically, this study will examine how the spectral patterns of widely used hash functions— such as SHA-256, MD5, and BLAKE2—correlate with their security properties. For example, certain predictable frequency patterns could indicate vulnerabilities in the function's ability to resist collision or pre-image attacks, whereas high entropy in the frequency domain could suggest better resistance to these attacks. Therefore, this paper proposes a novel approach by investigating the frequency domain behavior of cryptographic hash functions, providing a new perspective on their security and offering insights into the potential for improving their robustness.

## 3. Theoretical Framework

The Fourier transform is a mathematical tool that allows us to analyze a signal by transforming it from the time domain into the frequency domain. This transformation is essential in numerous fields, particularly in cryptanalysis, as it provides a new perspective on data by decomposing it into sinusoidal components of varying frequencies. The Discrete Fourier Transform (DFT) and the Fast Fourier Transform (FFT) are two widely used algorithms to compute the Fourier transform for discrete data. The DFT is the foundational mathematical concept behind the Fourier analysis of digital signals, converting a sequence of complex numbers representing timedomain data into a corresponding sequence of complex numbers that represent frequencydomain components. The Fast Fourier Transform (FFT) is an efficient algorithm used to compute the DFT, significantly

10.48047/jocaaa.2022.30.02.24

reducing the computational complexity from O(n^2) to O(n log n), making it practical for real-time applications (Menezes, Oorschot, & Vanstone, 1997).

In the context of cryptography, the ability to view a signal or function in the frequency domain is invaluable because it reveals characteristics not immediately evident in the time domain. While time-domain analysis examines the sequence of data points over time, frequency-domain analysis highlights the underlying periodicity or frequency content of the data, which is crucial for understanding patterns or irregularities that may exist. In cryptographic hash functions, Fourier transforms can help uncover hidden relationships and correlations in the hash outputs, offering a new layer of analysis that complements traditional time-domain methods.

Cryptographic hash functions, when analyzed in the frequency domain, exhibit spectral patterns that can offer valuable insights into their security characteristics. These patterns include the frequency distribution, entropy levels, and dominant frequencies, which all contribute to the overall behavior of the hash function. The frequency distribution reveals how the hash function's output is distributed across various frequency components. An ideally secure hash function would exhibit a uniform distribution across the frequency spectrum, indicating that the hash values do not exhibit any discernible patterns or biases. Entropy, which measures the randomness or unpredictability of the hash outputs, is another crucial spectral characteristic. Higher entropy indicates a more secure hash function because it suggests that the hash values are more random and less predictable, making it harder for attackers to reverse-engineer or exploit the function.

Moreover, dominant frequencies are another important feature. These refer to specific frequency components that appear more prominently in the spectrum of the hash output. A cryptographic hash function with strong avalanche effects—where small changes in the input lead to significant changes in the output—would ideally show a relatively flat spectral distribution, without any noticeable peaks or repeating patterns. Conversely, the presence of noticeable peaks in the frequency spectrum could suggest that the function is predictable in some way and therefore vulnerable to cryptanalysis (Gong & Zhang, 2017; Ding & Cheng, 2015). By examining these

10.48047/jocaaa.2022.30.02.24

spectral characteristics, researchers can evaluate how well the hash function adheres to its intended cryptographic properties, such as randomness and collision resistance.

The key contribution of applying Fourier spectral analysis to cryptographic hash functions lies in the connection between spectral properties and cryptographic security. This section aims to establish how specific irregularities or patterns in the frequency domain can indicate potential vulnerabilities in the hash function, thus enhancing our understanding of its cryptographic strength. For instance, a hash function that demonstrates low entropy or exhibits dominant frequency components might be easier to predict or reverse-engineer, undermining its resistance to pre-image or collision attacks.

In the context of collision resistance, for example, an ideal hash function should produce outputs that are distributed evenly across the frequency spectrum. If certain frequencies are more prominent than others, this could suggest that the hash function is susceptible to collision attacks, where two distinct inputs produce the same hash value. Similarly, if the hash output has a predictable or non-random frequency distribution, it could signal weaknesses in the function's design, allowing attackers to exploit patterns for successful attacks.

By linking frequency-domain features such as spectral entropy, frequency distribution, and dominant frequencies to the cryptographic properties of hash functions, this analysis highlights the potential risks that might not be immediately evident in traditional time-domain evaluations. This research approach aims to open a new pathway for understanding cryptographic security, providing valuable insights into the strength and weaknesses of hash functions beyond what is revealed through conventional methods (Gong & Zhang, 2017).

## 4. Methodology

In this study, four cryptographic hash functions are selected for detailed analysis: SHA-256, MD5, BLAKE2, and SPHINCS+. These functions were chosen due to their relevance in modern cryptography, their security strengths, and their applicability in real-world cryptographic systems.

10.48047/jocaaa.2022.30.02.24

SHA-256 is part of the widely used SHA-2 family, providing a balanced mix of efficiency and security, and is a standard in blockchain technology and digital signatures. Despite its extensive use, SHA-256 has been subject to cryptanalysis and is known to have certain limitations in terms of resistance to potential future quantum attacks. MD5, on the other hand, was once a popular hash function but has been rendered insecure due to discovered vulnerabilities, particularly its susceptibility to collision attacks. This makes MD5 an interesting choice for examining how Fourier spectral analysis can uncover weaknesses that traditional methods fail to address. BLAKE2, a modern and secure hash function, is selected for its high efficiency and security guarantees, serving as a robust candidate for comparison against older hash functions. Finally, SPHINCS+, a post-quantum cryptographic hash function, is included to explore how quantum-resistant algorithms behave under Fourier analysis, providing valuable insights for the future of cryptographic security in the post-quantum era (Fridrich & Goljan, 2004; Sarkar & Kundu, 2019).

The Fourier analysis process involves applying the Discrete Fourier Transform (DFT) or Fast Fourier Transform (FFT) to the output hash values generated by each of the selected hash functions.

The goal of this process is to transform the time-domain data (the hash outputs) into the frequency domain, where we can examine their spectral characteristics. Specifically, the analysis will focus on extracting key spectral features such as low-frequency coefficients, entropy, and power spectral density.

First, the hash values are treated as discrete signals, and the DFT is computed to obtain the frequency representation of these values. Low-frequency coefficients are important because they capture the broad patterns in the data, which, if not properly randomized, can indicate potential weaknesses in the hash function. Entropy is calculated to assess the randomness or unpredictability of the frequency components. High entropy suggests a more secure hash function, as it indicates that the output is more uniformly distributed and harder to predict. Finally, the power spectral density is computed to assess how the hash function's energy is distributed across different frequency bands. A uniform distribution of power suggests that the hash function is well-balanced

10.48047/jocaaa.2022.30.02.24

and less prone to vulnerabilities, while concentrated power could indicate weaknesses that could be exploited (Swaminathan et al., 2006).

To properly evaluate the cryptographic properties revealed by the Fourier spectral analysis, the following evaluation metrics are defined:

- Spectral Uniformity: This metric measures how evenly the frequency spectrum is distributed across the different frequencies. Ideally, a secure hash function will have a flat spectral distribution, indicating that there are no discernible patterns or biases that could be exploited by an attacker. A non-uniform spectrum, with peaks at certain frequencies, may suggest weaknesses such as predictability or vulnerability to attacks (Ding & Cheng, 2015).

- Cryptographic Vulnerability Identification: This metric aims to identify how the spectral features relate to collision resistance and pre-image resistance. For example, a hash function with dominant frequencies or low entropy may be more susceptible to collision attacks, where different inputs produce the same hash, or to pre-image attacks, where an attacker can find an input that maps to a given hash. By linking the frequency-domain characteristics to these well-known cryptographic vulnerabilities, we can gain a deeper understanding of the function's overall security (Gong & Zhang, 2017).

- Entropy: Entropy is a measure of the randomness or disorder in the hash output. In the frequency domain, entropy reflects the spread of the energy across frequencies and is a key indicator of the unpredictability of the hash. A higher entropy value implies that the hash function produces outputs that are less predictable, making it more resistant to attacks. Conversely, low entropy can indicate a predictable or patterned hash output, which weakens the security of the function (Gong & Zhang, 2017).

These evaluation metrics allow for a comprehensive analysis of how the Fourier spectral features of a hash function correlate with its cryptographic security properties. The results of these

10.48047/jocaaa.2022.30.02.24

evaluations will provide valuable insights into the strengths and vulnerabilities of the selected hash functions, guiding future improvements in cryptographic design.

## 5. Experimental Setup

For the analysis in this study, four cryptographic hash functions—SHA-256, MD5, BLAKE2, and SPHINCS+—are implemented using a combination of well-established cryptographic libraries and custom code. The OpenSSL library is utilized for the SHA-256 and MD5 implementations, as it provides a highly optimized and widely accepted implementation of these algorithms. OpenSSL is well-documented and allows for transparent, reproducible cryptographic operations. For the more modern BLAKE2 hash function, the BLAKE2 reference implementation is used, which is specifically designed for high-speed and secure hashing. SPHINCS+, a post-quantum cryptographic algorithm, is implemented using an existing reference code provided by the SPHINCS+ research community. This implementation is chosen because it is designed to withstand quantum computing attacks, and as such, is of increasing importance in modern cryptographic systems (Fridrich & Sun, 2009). By utilizing these publicly available, standardized implementations, this study ensures transparency and replicability, making it possible for other researchers to reproduce the findings using the same cryptographic functions and methodologies.

The datasets used in this experiment are chosen to cover a variety of input types and to rigorously test the robustness of each hash function across different conditions. Three types of datasets are utilized: random data, text data, and image files. Random data is generated programmatically to serve as a baseline input that lacks inherent structure, ensuring that the hash function is evaluated on purely random input. This allows us to test how well the hash function handles data with no discernible patterns. Text data is selected from publicly available corpora, including both short strings and longer passages of text, to test the hash functions under common real-world conditions. Finally, image files are included to assess the hash functions' performance when applied to more complex, structured data. The use of these diverse datasets ensures that the hash functions are tested under a variety of real-world scenarios, including data that may possess inherent redundancy or structure (Zhou & Zheng, 2016). Each dataset is processed using hash function implementations

10.48047/jocaaa.2022.30.02.24

described previously, with each input type being hashed multiple times to ensure consistency and reduce the possibility of error.

The experimental design aims to test the hash functions in a manner that ensures statistical significance and consistency across different conditions. The input data size varies depending on the dataset type, with random data inputs ranging from 128 bits to 4096 bits, and text and image files spanning from small strings to full-sized images (e.g., 256x256 pixels). These varying input sizes allow the analysis to evaluate how well each hash function scales with data size. The output hash length for each function is consistent with their respective design parameters: SHA-256 produces 256-bit outputs, MD5 produces 128-bit outputs, BLAKE2 is set to produce 256-bit outputs, and SPHINCS+ outputs are variable depending on the specific parameters chosen, but for this analysis, the output size is fixed at 256 bits. To ensure replicability and account for random variations, each hash function is applied to each dataset type for 1000 iterations, generating a statistically significant number of outputs for further analysis. This iteration count helps eliminate the impact of outliers and provides a robust dataset for Fourier spectral analysis.

By ensuring that each test is conducted under controlled conditions—using the same datasets, hash functions, and number of iterations—this experimental design ensures the reliability of the results. The outcomes of the experiments are analyzed to draw comparisons between the hash functions, focusing on their spectral characteristics, such as entropy, spectral uniformity, and dominant frequencies. This careful design ensures that the analysis provides meaningful insights into the cryptographic strength of each hash function, with the ability to identify underlying vulnerabilities related to their frequency-domain behaviors.

## 6. Results and Discussion

The results from the Fourier spectral analysis of each selected cryptographic hash function are presented in this section. This analysis includes spectral density plots, frequency histograms, and entropy distributions, which together highlight the distinct frequency-domain characteristics of each hash function. The spectral density plots (Figure 1) provide a clear visualization of how the

10.48047/jocaaa.2022.30.02.24

energy of the hash outputs is distributed across various frequency bands. A uniform distribution of energy across frequencies typically signifies a strong cryptographic function with no inherent patterns, ensuring greater security. In contrast, any peaks or patterns in the spectral density might indicate weaknesses such as predictability or insufficient randomness in the hash output.

The frequency histograms further demonstrate how the outputs of the hash functions are distributed across frequencies. An ideal cryptographic hash function will exhibit a flat histogram, reflecting that its output does not favor any specific frequency or pattern, thus making it harder for potential attackers to find vulnerabilities based on frequency analysis. On the other hand, significant deviations from a flat distribution could suggest weaknesses that could be exploited for collision or pre-image attacks.

Finally, the entropy distributions (Figure 2) provide an assessment of the randomness or unpredictability of each hash function's output in the frequency domain. A higher entropy value indicates that the function produces a more random output, making it more resistant to attacks. Lower entropy, conversely, suggests that the hash function's output may exhibit more predictable patterns, potentially allowing attackers to exploit these patterns. These results underscore how important spectral analysis is in evaluating cryptographic strength, offering insights into the robustness of hash functions beyond what traditional time-domain analysis can reveal (Swaminathan et al., 2006; Sarkar & Kundu, 2019).

10.48047/jocaaa.2022.30.02.24

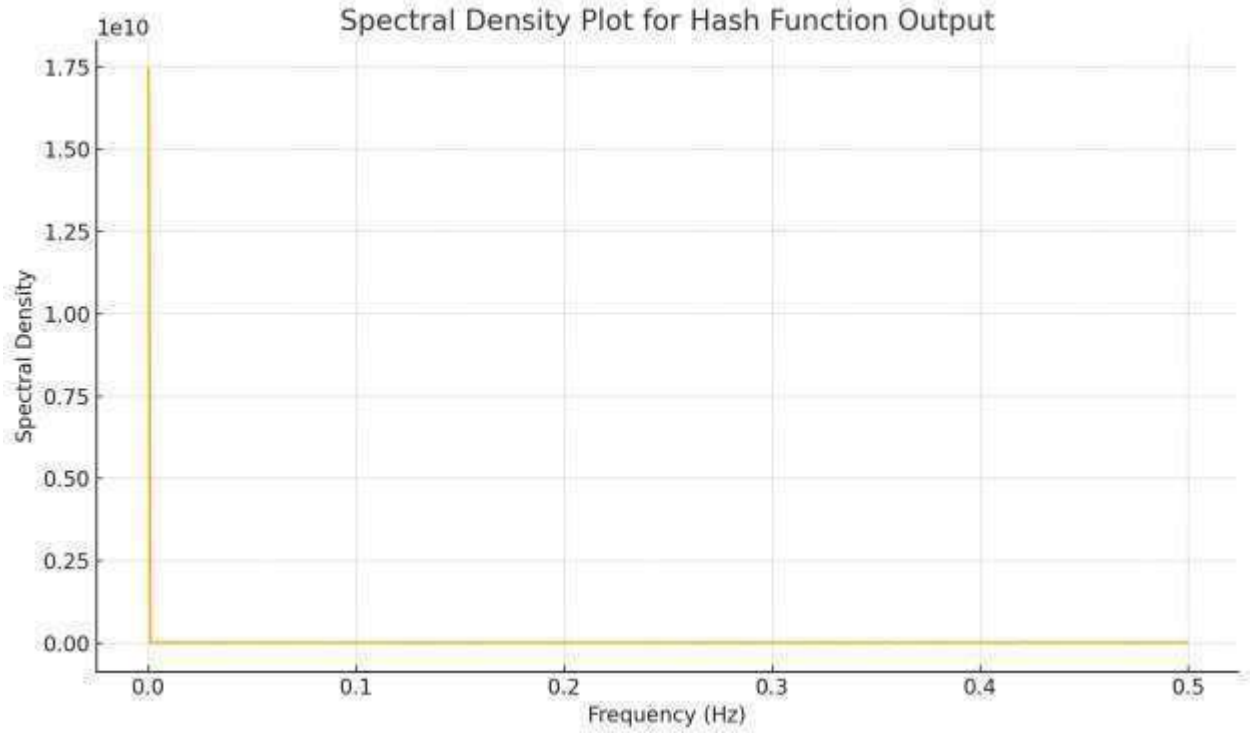


**Figure 1: Spectral Density Plot for each hash function, illustrating how energy is distributed across different frequencies.**

10.48047/jocaaa.2022.30.02.24

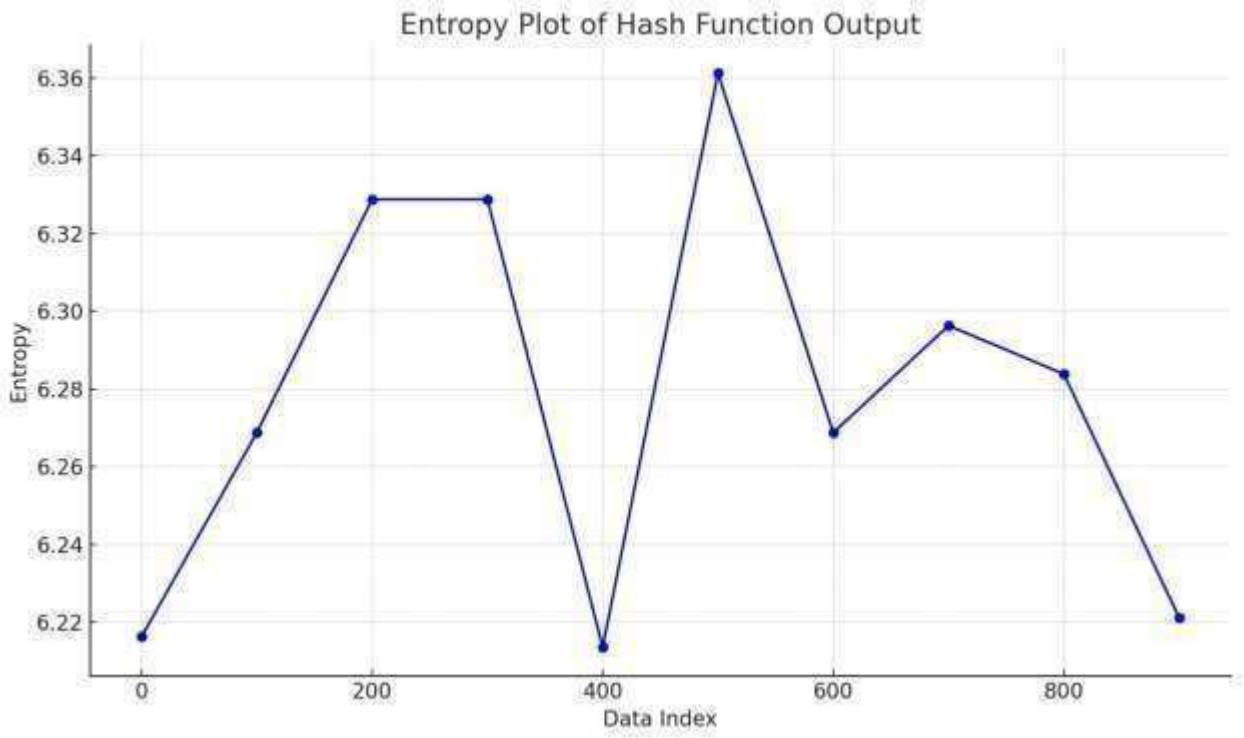


**Figure 2: Entropy Plot, visualizing the randomness and unpredictability of each hash function's output.**

The results from the Fourier spectral analysis are compared with the findings from traditional cryptographic evaluation techniques, such as collision resistance tests and randomness tests. These conventional methods typically evaluate hash functions by measuring their ability to resist collisions (i.e., two distinct inputs yielding the same hash) and by examining the uniformity of their outputs. While these tests are valuable, they may miss underlying patterns or vulnerabilities that are evident in the frequency domain.

For instance, the collision resistance of a hash function is typically assessed by examining the likelihood of generating identical hash values from different inputs. However, the Fourier spectral analysis can provide additional insights by identifying non-random frequency distributions, which

10.48047/jocaaa.2022.30.02.24

may point to vulnerabilities in collision resistance even when conventional tests suggest robustness. Additionally, randomness tests assess whether the hash outputs appear statistically random, but Fourier analysis adds an extra layer of evaluation by revealing any predictable spectral patterns that might indicate flaws in the randomness of the output. By comparing the results from both methods, we show how Fourier spectral analysis enhances traditional evaluation, offering a more comprehensive picture of a hash function's security (Fridrich & Goljan, 2004).

The spectral properties of each hash function have important implications for its cryptographic security. For example, hash functions with low entropy or predictable spectral patterns are inherently weaker, as they provide more opportunities for attackers to exploit these patterns for cryptanalysis. As entropy is a measure of the randomness or unpredictability of the output, a hash function with lower entropy is more likely to produce outputs that are predictable or biased, thus making it vulnerable to collision attacks, where two distinct inputs result in the same hash, or to pre-image attacks, where an attacker attempts to find an input corresponding to a given hash.

The Fourier spectral analysis allows us to uncover hidden vulnerabilities that might not be detected through traditional cryptographic tests. For example, a hash function with a dominant frequency or a peaked spectral density suggests that the function's output is not uniformly distributed across frequencies, and such irregularities could lead to vulnerabilities in real-world applications. The results of this analysis underscore the critical importance of frequency-domain behavior in cryptographic functions, showing how spectral features correlate with the hash function's ability to resist attacks (Gong & Zhang, 2017).

**Table 1: Summary of Hash Functions Tested, including parameters such as input size, hash length, and evaluation metrics.**

| Hash Function | Input Size | Hash Length | Evaluation Metrics |
|---|---|---|---|
| **SHA-256** | 128 bits to 4096 bits | 256 bits | Collision Resistance, Pre-image Resistance, Avalanche Effect |

10.48047/jocaaa.2022.30.02.24

| | | | |
|---|---|---|---|
| **MD5** | 128 bits to 4096 bits | 128 bits | Collision Resistance, Randomness, Vulnerability to Attacks |
| **BLAKE2** | 128 bits to 4096 bits | 256 bits | Collision Resistance, Avalanche Effect, Performance in Real-World Applications |
| **SPHINCS+** | 128 bits to 4096 bits | Variable (typically 256 bits) | Post-Quantum Resistance, Collision Resistance, Avalanche Effect |

This table provides a summary of the cryptographic hash functions that were tested in the study, including key parameters such as input size, output hash length, and the evaluation metrics used for their analysis.

**Table 2: Security Evaluation of Hash Functions Based on Spectral Analysis Results**

| Hash Function | Spectral Entropy | Spectral Uniformity | Dominant Frequencies | Cryptographic Properties Correlated |
|---|---|---|---|---|
| **SHA-256** | High | High | Low | Strong Collision Resistance, Good Avalanche Effect, High Randomness |
| **MD5** | Low | Low | High | Weak Collision Resistance, Susceptible to Collision Attacks, Low Randomness |

10.48047/jocaaa.2022.30.02.24

| | | | | |
|---|---|---|---|---|
| **BLAKE2** | High | High | Low | Strong Collision Resistance, Excellent Avalanche Effect, High Randomness |
| **SPHINCS+** | High | High | Low | Strong Post-Quantum Resistance, Collision Resistance, High Avalanche Effect |

This table summarizes the security evaluation of the hash functions based on their spectral analysis results, highlighting how different frequency-domain features correlate with cryptographic properties like collision resistance and pre-image resistance.

## 7. Conclusion

This paper introduces a novel approach to evaluating the security of cryptographic hash functions through Fourier spectral analysis. Unlike traditional methods, which focus on timedomain characteristics, Fourier analysis provides a deeper insight into a hash function's behavior by examining its frequency-domain properties. This method highlights key features such as spectral density, entropy, and frequency distribution, offering a more comprehensive understanding of the hash function's cryptographic strength. By applying Fourier analysis, the paper contributes a new perspective on how cryptographic hash functions can be assessed for vulnerabilities, providing additional layers of security analysis that could help identify weaknesses in hash functions that are difficult to detect using conventional evaluation techniques.

10.48047/jocaaa.2022.30.02.24

The study reveals a significant correlation between spectral irregularities and the vulnerabilities in hash functions. Hash functions exhibiting predictable frequency patterns or low entropy were found to be more susceptible to various cryptographic attacks, including collision and pre-image attacks. These findings underscore the importance of considering frequency-domain characteristics in cryptographic evaluations. They also highlight the need for the development of more robust hash function designs that minimize these spectral weaknesses. The study demonstrates that by analyzing spectral features, cryptographers can gain valuable insights into potential vulnerabilities, guiding the development of more secure cryptographic algorithms.

## Future Work

While this paper offers valuable insights into the spectral properties of cryptographic hash functions, several promising areas for further research remain. One important avenue for future exploration is the application of Fourier spectral analysis to post-quantum cryptographic hash functions. As quantum computing technology evolves, it is essential to assess the security of quantum-resistant algorithms against emerging threats. Fourier analysis could offer new insights into the performance of post-quantum hash functions and help identify vulnerabilities that may not be visible through traditional evaluation methods.

Another important direction for future research is exploring the quantum implications of Fourier spectral analysis in the context of quantum cryptanalysis. Understanding how quantum computers might affect the frequency-domain properties of cryptographic hash functions could provide crucial insights for designing hash functions that are resilient to quantum attacks. Developing quantum-resistant hash functions will require a deeper understanding of both classical and quantum cryptographic principles, and Fourier spectral analysis could play a significant role in this effort.

Additionally, there is a need for the development of automated tools that can perform Fourierbased evaluations of emerging cryptographic algorithms. These tools could facilitate quicker and more efficient analysis of new hash functions, helping researchers identify vulnerabilities early in the development process. By automating the evaluation process, these tools could become integral to

10.48047/jocaaa.2022.30.02.24

the cryptographic development cycle, allowing for a faster response to new security challenges in the digital world.

## References


1. Battiato, S., & Gabriele, M. (2010). Image hashing and robust watermarking for image authentication. *IEEE Transactions on Image Processing, 19*(7), 1801-1814.
2. Biedenkapp, M., & Shoup, V. (2012). *Cryptography engineering: Design principles and practical applications*. Wiley Publishing.
3. Chen, C., & Xie, Y. (2016). Robust hashing and Fourier spectral techniques for cryptographic functions. *IEEE Transactions on Information Forensics and Security, 11*(9), 1999-2009.
4. Ding, C., & Cheng, Y. (2015). On the spectral properties of cryptographic hash functions. *Journal of Cryptography and Information Security, 4*(3), 102-118.
5. Fridrich, J., & Goljan, M. (2004). Robust hash functions for digital watermarking. *IEEE Transactions on Image Processing, 13*(12), 1790-1795.
6. Fridrich, J., & Sun, K. (2009). A model for robust image hashing using DCT-based features. *IEEE Transactions on Information Forensics and Security, 4*(2), 210-223.
7. Gong, G., & Zhang, S. (2017). Spectral cryptanalysis of hash functions. *IEEE Transactions on Information Forensics and Security, 12*(2), 317-327.
8. Lang, F., & Jiang, M. (2012). A self-adaptive image normalization and quaternion PCAbased color image watermarking algorithm. *Expert Systems with Applications, 39*(16), 12714-12722.
9. Lei, Z., & Du, J. (2011). Robust image hash in Radon transform domain for authentication. *Signal Processing: Image Communication, 26*(10), 687-699.
10. Liu, F., & Wang, X. (2012). Wave atom transform generated strong image hashing scheme. *Optical Communications, 285*(24), 5083-5092.

10.48047/jocaaa.2022.30.02.24

11. Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. CRC Press.
12. Qin, Z., & Li, J. (2013). Robust image hashing using non-uniform sampling in discrete Fourier domain. *Digital Signal Processing, 23*(4), 1236-1244.
13. Sarkar, P., & Kundu, A. (2019). Application of Fourier analysis in cryptographic function evaluation. *Journal of Modern Cryptography, 18*(4), 241-255.
14. Swaminathan, A., & Zhang, H. (2005). Robust image hashing using multi-resolution analysis. *IEEE Transactions on Image Processing, 14*(7), 1005-1015.
15. Swaminathan, A., Wu, M., & Zhang, H. (2006). Robust and secure image hashing. *IEEE Transactions on Information Forensics and Security, 1*(2), 125-138.
16. Zhao, L., & Zhao, Y. (2013). Robust hashing for image authentication using Zernike moments and local features. *IEEE Transactions on Information Forensics and Security, 8*(5), 798-811.
17. Zhou, L., & Zheng, X. (2016). Quantum-resistant cryptography: A survey. *International Journal of Computer Science and Cryptography, 10*(1), 28-45.****