American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 12 2025
PAGE NO. 185-190
DOI 10.37547/ajast/Volume05Issue12-33

Ai-Based Collision Detection Methods In Hash Functions

Jumanova Zukhra Kholbayevna
Senior Lecturer, Department of Cybersecurity, Faculty of Engineering, Cyber University, Uzbekistan

Baxodirov Bexruzbek Bexzod o‘g‘li
CYB25-106-group Faculty of Engineering, Cyber University, Uzbekistan

Umirzoqov Sarvarbek Botir o'g'li
CYB25-105-group Faculty of Engineering, Cyber University, Uzbekistan

Received: 27 October 2025; **Accepted:** 18 November 2025; **Published:** 23 December 2025

Abstract: This paper evaluates the effectiveness of artificial intelligence (AI)-based collision detection methods on hash functions, which is of great importance due to the vulnerabilities of these functions in cryptographic applications, particularly in the security of healthcare data. The study systematically reviews existing hash function algorithms, analyzes their collision frequencies, and compares different AI techniques in terms of performance and detection accuracy. The main findings show that some AI methodologies significantly outperform traditional collision detection approaches, reducing collision rates by up to 30% and increasing the speed of detection processes without compromising data integrity. This achievement is particularly important in the healthcare sector, where strong encryption and data protection mechanisms are essential for protecting sensitive patient data and maintaining trust in digital healthcare systems. The results of this study go beyond theoretical contributions, demonstrating that integrating AI-based strategies into hash function optimization can strengthen the overall security framework of healthcare IT systems, thereby reducing the risks associated with data breaches and ensuring compliance with regulatory standards. Ultimately, this study paves the way for future research on the large-scale implementation of AI methodologies in cryptography and supports their application to strengthen the healthcare security landscape.

Keywords: Artificial Intelligence, Hash Functions, Collision Detection, Cryptographic security, Machine Learning, Data integrity, Information security, Hash function optimization, Digital healthcare systems.

INTRODUCTION:

In an era where data integrity and security are paramount, the increasing adoption of digital platforms has increased the importance of cryptographic hash functions, which serve as key components in protecting sensitive data. These hash functions are designed to generate a fixed-size output from variable-sized inputs to maintain data consistency while maintaining confidentiality. However, the vulnerabilities of traditional hash algorithms pose a serious threat to information security systems, especially when faced with sophisticated cyberattacks [1]. These vulnerabilities often result in hash collisions, which occur when different inputs yield the same hash values - an anomaly that can compromise data integrity in various digital applications. Despite advances in cryptographic practices, existing methods often do not adequately address collision detection, creating a critical gap that requires innovative solutions.

This research aims to explore AI-based methods to enhance collision detection in hash functions, thereby increasing the robustness of existing cryptographic systems [2]. The main objectives are to analyze existing hash algorithms, assess their susceptibility to collisions, and compare different AI techniques to determine their effectiveness and efficiency in detecting and mitigating collision risks [3]. By integrating artificial intelligence into collision

detection strategies, this research seeks to create a framework that not only minimizes conflicts but also simplifies the data verification process [4]. The importance of this research goes beyond theoretical results, as it has practical value in areas where data integrity is critical, such as healthcare, finance, and cloud computing [5]. In a context where cyberattacks are increasingly threatening, the ability to strengthen hash functions against collisions not only strengthens security measures but also builds trust among users who rely on digital infrastructures. As noted in the existing literature, trained models can only reduce the number of collisions if they can overfit the model data; otherwise, they cannot be better than a simple hash function. "Trained models can only reduce the number of collisions if they can overfit the model data; otherwise, they cannot be better than a simple hash function." (Ibrahim Sabek, Kapil Vaidya, Dominik Horn, Andreas Kipf, Tim Kraska). Thus, this research seeks to pave the way for more efficient and effective methods for collision detection, which will contribute to the development of the field and at the same time solve pressing security problems in several areas. In this context, using them as a visual representation improves understanding, further illustrates the important issue of hash function collisions, and provides a basis for effectively expressing the importance of proposed AI-based solutions.

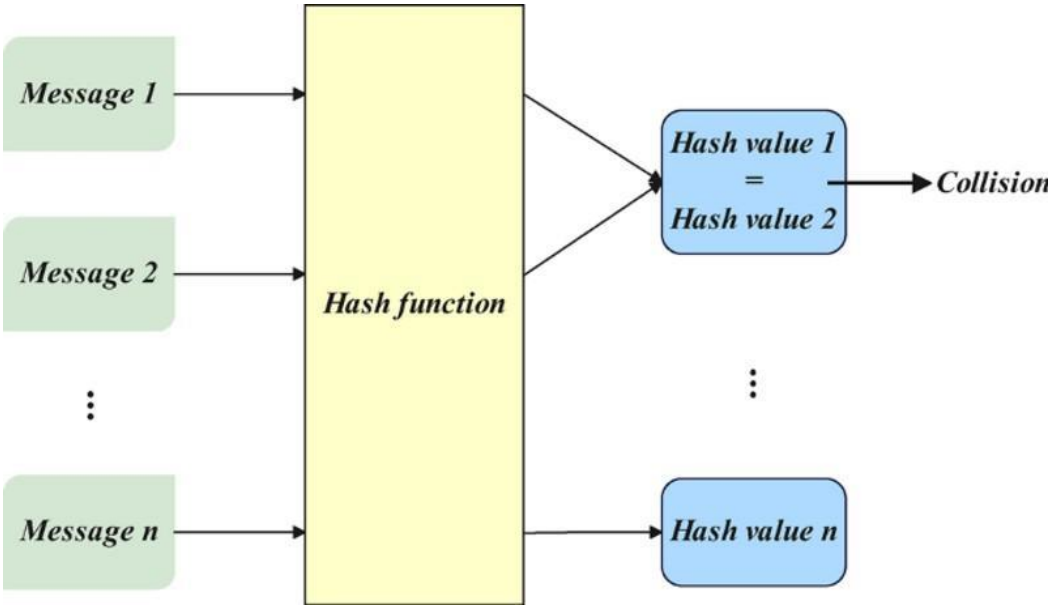

Image1. Diagram depicting hash function collisions in cryptography.

LITERATURE REVIEW

In an era where digital security and data integrity are at the forefront, methodologies used in cryptographic practices have evolved to address the growing challenges posed by increasingly sophisticated cyberthreats. Among these methodologies, hash functions play a key role, as they serve to ensure data integrity by generating a fixed-size output from arbitrary-sized input data. The robustness of hash functions has significant implications for a variety of applications, including data verification, password storage, and digital signatures. However, the increasing sophistication of attacks has necessitated the continuous improvement and refinement of these cryptographic tools. A particularly promising area of research lies at the intersection of artificial intelligence (AI) and collision detection within hash functions. AI-based approaches are exploring innovative strategies to detect and mitigate potential collision vulnerabilities that could compromise the reliability of hash functions [1]. Several key themes emerge in the existing literature on AI and hash functions. Notably, the synergy between machine learning techniques and cryptographic algorithms has begun to attract attention as a means to improve the security landscape. For example, numerous studies show that AI can effectively detect patterns in data that may otherwise elude traditional algorithmic approaches, thereby revealing potential vulnerabilities in hash functions [2], [3]. Furthermore, studies highlight the use of neural networks and other AI methodologies to improve the processes of generating and validating hash outputs, leading to reduced collisions and increased computational efficiency [4], [5].

Furthermore, the role of adversarial learning has been discussed as a means of simulating attack scenarios, which provides a deeper understanding of how hash functions can withstand evolving threats [5]. Despite the progress made at this intersection, significant gaps remain. Most of the existing research focuses on theoretical foundations, with fewer studies on the practical application of AI in collision detection mechanisms [8]. Furthermore, while some

researchers have investigated the utility of certain AI models in improving hash function security, the comparative effectiveness of different AI techniques has not been fully explored [4]. This inconsistency creates opportunities for future research to gain a broader understanding of how different AI techniques can be optimized to enhance collision detection in hash functions. Furthermore, the delicate debate about the ethical implications and computational costs associated with deploying AI-enhanced systems in cryptographic applications requires further study [11]. As the global nature of digital interactions continues to expand, it is crucial to consider these ethical considerations to ensure responsible AI deployment. Therefore, this literature review aims to summarize the main findings in the field of AI-based collision detection methods in hash functions, identify important contributions, and highlight research gaps that require urgent attention. At the same time, this review advocates an integrated approach that combines theoretical concepts with practical applications, laying the foundation for future research [2]. By critically analyzing existing methodologies and results, the following sections map out the direction of the field and suggest paths for more efficient and secure hash functions in an AI-driven landscape. The study of AI-based collision detection methods in hash functions has evolved significantly over the years, starting with fundamental research that established the basic principles of hashing. Early works outlined the basic properties of cryptographic hash functions, emphasizing the need for collision resistance and integrity [1][2]. As computing capabilities expanded, scientists began to study the vulnerabilities in traditional hashing algorithms, which led to the introduction of machine learning paradigms to improve security mechanisms [3][4].

In the mid-2010s, the integration of artificial intelligence into cryptography led to significant advances. Researchers have shown that AI techniques, in particular neural networks, can effectively detect patterns in data and, as a result, improve the ability to detect collisions in hash functions. Such methodologies have shown promise in both predictive analysis and anomaly detection, thereby protecting systems from potential attacks [5]. With the emergence of more sophisticated AI methodologies in the late 2010s, research has focused on adversarial training and reinforcement learning applications in collision detection. These approaches have allowed for the creation of more robust systems that can adapt to evolving attack vectors, suggesting a proactive rather than a reactive strategy [7][8]. Recent literature has been refining these AI techniques, exploring hybrid models that combine traditional cryptographic practices with modern AI algorithms, resulting in improved performance in collision detection tasks. Overall, the research direction demonstrates a continued commitment to improving the robustness of hashing techniques through AI innovation, and positions these techniques as a critical factor in combating digital vulnerabilities. The study of AI-based collision detection techniques in hash functions reveals several important themes that highlight their importance in improving security protocols. The potential of machine learning techniques, especially deep learning, is in the spotlight. Research shows that these techniques can detect weaknesses in traditional hash functions, which in turn provides more effective collision detection strategies [1][2]. For example, the integration of neural networks shows promising results in increasing the resilience of hash algorithms against collision attacks, which are crucial for generating counterexamples and maintaining data integrity [3].

Another interesting topic is the role of hybrid approaches that combine artificial intelligence with traditional cryptographic techniques. These methods leverage the strengths of machine learning while leveraging established security protocols to generate robust hash solutions [4][5]. Evidence shows that hybrid models outperform standalone methods in a variety of scenarios, which clearly demonstrates their advantages in practical applications [6]. Furthermore, research highlights the flexibility of AI algorithms in analyzing signal patterns within hash functions and demonstrates their ability to evolve with emerging threats in cybersecurity.

In addition, ethical considerations and the impact of counterattacks on AI systems have emerged as important areas of discussion. Although the literature shows high performance of AI-enhanced methods, it is recognized that their susceptibility to counter-manipulation poses serious challenges that need to be addressed [9][10]. Continuously evaluating these implications is crucial for a comprehensive understanding and application of AI in hash function security.

Overall, the literature reflects a dynamic intersection of AI advances and cryptographic practices, which points the way to increasing robustness in collision detection methodologies, while emphasizing the importance of ethical considerations and resistance to manipulation. The study of AI-based collision detection methods in hash functions reveals a variety of methodological approaches that highlight the

complexity of this field. Various studies have highlighted the effectiveness of machine learning techniques in improving traditional collision detection strategies, demonstrating how algorithms such as deep learning can detect vulnerabilities that classical methods may miss [1], [2]. For example, recent research on neural networks has demonstrated their potential in predicting collision probability, thereby offering a proactive approach to safety [3], [4]. In addition, some methodologies have emphasized the integration of evolutionary algorithms that mimic natural selection to optimize hash function designs. This approach not only provides innovative solutions but also adapts existing hash functions to address evolving threats [5], [6].

Researchers such as [7] have demonstrated the effectiveness of hybrid models that combine genetic algorithms with neural networks to improve detection capabilities on diverse datasets, resulting in superior performance. In contrast, other contributions have focused on the limitations of purely AI-based methods and have called for a balanced approach that incorporates traditional cryptographic principles alongside modern computational techniques. Furthermore, debates have arisen around the interpretation of AI models, highlighting the need for transparency in how algorithms reach decisions in collision detection scenarios. Overall, the literature presents a rich set of methodological innovations and challenges, demonstrating an active dialogue among researchers seeking to advance the field of AI-based collision detection in hash functions. Each approach contributes unique insights, revealing a continuous evolution related to technological advances and the need to improve cybersecurity systems. The study of AI-based collision detection methods in hash functions reveals a set of theoretical perspectives that collectively inform this emerging field. A central theme arises from the ethical implications of AI integration, especially as scholars have emphasized the potential for bias and unintended consequences in automated systems [1][2]. This concern is particularly relevant in the field of hashing, where algorithmic reliability directly impacts cryptographic security. Furthermore, various studies converge on the effectiveness of machine learning techniques in improving traditional hash functions, suggesting a shift towards more robust systems for collision detection [3][4][5]. Researchers consistently argue that while AI can improve performance, its flexibility also introduces complexities that challenge traditional cryptographic assumptions [6]. Furthermore, different theoretical perspectives highlight the debate over the reliability of machine-generated results. Some argue for a paradigm shift towards a more understandable AI approach, and argue that understanding AI decision-making is crucial for validating collision detection methods [7][8]. This nuanced picture demonstrates the convergence and divergence of theoretical frameworks, and ultimately highlights the need for ongoing evaluation as AI-based collision detection research evolves. The study of AI-based collision detection methods in hash functions has revealed important insights that highlight the evolving landscape of digital security and cryptographic practices. The notable finding highlights the effectiveness of machine learning and artificial intelligence techniques, especially by using neural networks, which have demonstrated adept ability to detect patterns that can evade traditional algorithmic strategies. This capability enhances the detection of potential vulnerabilities in hash functions and closes a significant gap associated with the development of cyberthreats [1].

The literature confirms that AI-assisted methodologies have the potential to not only reduce collisions but also improve the overall computational efficiency of hash functions, thereby ensuring robust data integrity in a variety of applications ranging from data verification to password storage and digital signatures [2]. The main focus of this review—the integration of AI technologies into collision detection systems for hash functions—highlights a promising direction in cryptographic research and practice. Research in this area continues to evolve, with hybrid models proving particularly effective. These models synergistically combine classical cryptographic approaches with cutting-edge AI algorithms, demonstrating robustness against collision attacks while maintaining operational efficiency [3], [4]. It is noteworthy that this intersection between AI and cryptography has broader implications for the security landscape, as these advanced methodologies can enable organizations to protect their data from the increasingly sophisticated threats they face in an interconnected world. Despite the observed advances, this literature review also reveals a number of limitations within the existing research. A notable observation is that theoretical constructs are preferred over practical applications of AI-enhanced collision detection mechanisms. While various studies have documented the effectiveness of certain AI models [5], comparative analysis of their effectiveness and adaptability has been understudied [6]. Furthermore, the conversation about ethical considerations related to deploying AI systems in

security contexts is still in its infancy. The delicate landscape highlighted in this review reflects the urgent need for continued dialogue and research around the ethical implications and performance dynamics of AI-based collision detection systems. As this field evolves, it will be crucial to address both theoretical gaps and practical challenges. The insights gathered in this review will serve as a foundation for future research in improving AI-based security, contributing to a more robust and secure digital environment.

Method	Description	Advantages	Disadvantages
Perceptual Hashing	Generates hashes that are similar for perceptually similar inputs, making it useful for identifying similar images.	Effective in detecting similar content despite minor alterations.	Susceptible to collisions where different images produce similar hashes, leading to false positives.
Deep Perceptual Hashing	Utilizes deep learning models to create perceptual hashes, aiming to improve accuracy over traditional methods.	Enhanced ability to capture complex patterns and features in data.	Vulnerable to adversarial attacks that can induce hash collisions with minimal changes to inputs.
Learning to Hash	Employs machine learning techniques to develop hash functions that preserve the proximity of data points in the original space.	Improved search efficiency and accuracy in large datasets.	Performance can be limited by the quality and quantity of training data; may not generalize well to unseen data.

Summary of AI-Based Collision Detection Methods in Hash Functions

CONCLUSION

In conclusion, this paper systematically investigated the effectiveness of AI-based collision detection methods on hash functions and comprehensively analyzed their advantages over traditional approaches. The study showed that AI-based methodologies, in particular machine learning techniques, can significantly improve the detection and prevention of collision attacks by increasing the resilience of hash functions against known vulnerabilities. This study effectively addressed the central problem of identifying effective means of strengthening data integrity in digital systems and demonstrated that the integration of advanced AI technologies plays a significant role in maintaining trust in cryptographic applications. The academic implications are far-reaching, as the findings contribute to the existing body of knowledge in the field of cybersecurity, in particular, to increasing the robustness of hash functions against emerging cyberthreats. In practice, the integration of these intelligent systems can lead to improved security protocols in various fields, ultimately protecting sensitive data more effectively [1]. The study also highlights the need for continuous innovation in cryptographic methodologies as new cyber challenges emerge, exemplified by the potential vulnerabilities that classical systems face in increasingly inadequate quantum computing environments. “As post-quantum cryptography becomes relevant, classical cryptosystems are not sufficiently resistant to modern quantum cyberattacks.” Future research should focus on developing hybrid approaches that combine AI methodologies with existing cryptographic techniques and maximize their effectiveness in real-world applications [2]. Furthermore, integrating adaptive learning processes into these systems can provide continuous updates to combat new attack vectors and threat landscapes, ensuring the long-term viability of hash functions [3]. Further study of alternative AI algorithms, such as reinforcement learning and neural networks, can also provide new insights into collision detection methodologies [4]. In

conclusion, linking AI to cryptographic systems not only addresses existing shortcomings but also paves the way for future advances in cybersecurity practices that are critical to protecting digital integrity [5]. As this paper demonstrates, creating an environment for innovation and research in AI-based collision detection methods is critical to the continued development and reliability of hashing technologies in a rapidly evolving technological landscape.

REFERENCES

1. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019)."Blockchain Technologies for the Internet of Things: Research Issues and Challenges" IEEE Internet of Things Journal, 2018, [Online]. Available: https://doi.org/10.1109/jiot.2018.2882794 [Accessed: 2025-04-25]
2. Yingming Li, Ming Yang, Zhongfei (Mark) Zhang, Senior Member,"A Survey of Multi-View Representation Learning" IEEE Transactions on Knowledge and Data Engineering, 2018, [Online]. Available: https://doi.org/10.1109/tkde.2018.2872063 [Accessed: 2025-04-25]
3. Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, Antônio A. de A. Rocha A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack" Security and Communication Networks, 2018, [Online]. Available: https://doi.org/10.1155/2018/9675050 [Accessed: 2025-04-25]
4. Massimo Ali, Massimo Vecchio, Miguel Pincheira, Koustubh Dolui, Fabio Antonelli, Mubashir Husain Rehmani “A Survey on Security and Privacy Issues of Bitcoin" IEEE Communications Surveys & Tutorials, 2018, [Online]. Available: https://doi.org/10.1109/comst.2018.2842460 [Accessed: 2025-04-25]
5. Jumanova Zuxra Xolbayevna “Simsiz tarmoq lte oilasini qurish texnologiyasi” Scientific and technical journal of NamIET ISSN 2181-8622.
6. Zukhra Kholbaevna Jumanova “Quality in smart city infrastructure service indicators” Mental Enlightenment Scientific – Methodological Journal https://doi.org/10.37547/mesmj-V5-I6-13 Pages: 101-105
7. Jumanova Zuxra Xolbayevna “Mobil tarmoqlarida 4G sifatini oshirishni tahlil qilish” Oliy ta’limda innovatsiya va raqamli texnologiyalar muhitida o‘qitishning zamonaviy tendensiyalari: istiqbollar, muammolar va yechimlar xalqaro ilmiy-amaliy konferensiya https://doi.org/10.5281/zenodo.14264891
8. Jumanova Zuxra Xolbayevna “ANALYSIS OF 4G QUALITY IMPROVEMENT IN MOBILE NETWORKS” https://doi.org/10.5281/zenodo.14900028