www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-10, Issue-4, October 2022
Research Paper

Int. J. Sc. Res. in
Network Security
and Communication

E-ISSN:2321-3256

A Comparative Study Between RIPEMD160 and SHA256 Hash Functions On Digital Holy Quran Integrity Verification

N.M. Al-Aidroos[1], H.S. Baqtian[2*]

[1]Computer Science Department, College of Computers and Information Technology, Hadhramout University, Hadhramaut, Yemen
[2]Department of Information Technology, College of Computers and Information Technology, Ahgaff University, Hadhramaut, Yemen

[*]*Corresponding Author: eng.hanan.salem2020@gmail.com, Tel.: +00-967-738476040*

Received: 20/Jul/2022, Accepted: 15/Sept/2022, Published: 31/Oct/2022

Abstract— In Data Security and Cryptography areas, hash functions play a fundamental and important role in the field of Integrity, This paper presents a performance evaluation of two cryptographic hash functions SHA256 and RIPEMD160 which used to verify the integrity of digital holy Quran and determine which one is better. SHA256 and RIPEMD160 hash functions have been selected in this comparison because their characteristics speed and space characteristics, both hash functions have their own advantages and disadvantages what distinguishes them from others, which will be discuss in detail in Background section. This study focuses on security and performance analysis. Security analysis where many experiments be applied to find out the strength and effectiveness of each two hash functions and hash collisions be analysed. The performance analysis will be applied by measuring the speed of the proposed methods in this study. The results show that the RIPEMD160 hash function is faster than SHA256 hash function for the integrity verification on a digital copy of the Holy Quran.

Keywords—Integrity, Holy Quran, SHA256, RIPEMD160, Hash Function, Data Security, Verification

I. INTRODUCTION

On the planet Islam is the second biggest religion, and its followers utilize the Holy Quran as the fundamental wellspring of moral molarity rules and standards. Al-Quran is the holy book of Muslims which is written and read in Arabic language. Muslims believe that the Quran is neither adulterated nor changed this is essentially due to keeping up with its original text.

Integrity verification of sensitive online content field is very new and developing and requires devoting the efforts of researchers as far as distinguishing various strategies that are appropriate for checking and investigating the performance of various techniques appropriate for various formats like text and image, audio format...etc.

The users in internet are bound to disregard Internet content verification and bound to share the content. With regards to Islamic content like Quran verses, when someone share and spread fake or inaccurate content and this will cause a defect in religious and moral concepts. This ease of access and availability of online contents of the verses of the holy Quran from different and many sources. Thus, alterations and fabrications of fake Quran verses are possible and feasible, this is a primary motivation to do this study another motivation is that people use and share the verses of digital holy Quran without check and verify the correctness of this verses. Regardless of whether the verification process of Islamic content is becoming simpler consistently, the Internet users ignore the verification and check step and hop into sharing the content, and thus this is what leads to the distortion of the holy book, and this is inconsistent with the God promise that he pledged to preserve the verses of the Qur'an.

Where more than 1400 years ago the holy Quran text was revealed to the Holy Prophet Muhammad (PBUH) and has been protected from all possible ways of distortion until today and forever.

Content integrity refers to the process of managing and assuring the accurateness and correctness of the content being transferred or being made available to end users. [1]
Izzat Alsmadi has another definition where he say Integrity is about making sure that the document is not altered by any unauthorized person and hence is authenticated.[2]

An authentic text-based copy of digital Holy Quran will be used. Where Tanzil resource seeks to provide authenticated digital Holy Quran.[3]

Tanzil " site chosen as an authenticated source of digital copy of holy Quran because this site provides the ability to download text files of verses numbered according to the numbering in the Holy Qur'an. The paper is provide a comparison of a performance evaluation for two types of

hash functions SHA256 and RIPEMD160 on integrity verification of the verses of holy Quran with take into consideration the measurement of time , size, and security.
Figure1.illustrates the proposed method that was followed in this study, where a Table in database will be created here named as “T1” containing the Quranic verses all truncating according to the original numbering in the Quran, and T2, T3 containing the value of hash functions SHA256 and RIPEMD160 used in the hashing process then execution time, size will be measured.

II. Research Problem

A. Problem Specification

As we know Holy Quran is the main source of laws, legislation, rules and guidelines for Muslims to guide them in their lives. The integrity problem on internet have been increased because two reasons: The too much reliability on the internet content and the increase in users. The usage of the digital Holy Quran has been growing since the appearance of the first copy of digital Holy Quran in 2007[3].

Hakak et al. [4] said in his research that there are a lot of sensitive digital contents available online which can be accessed and downloaded from different sources, such as religious websites, social media websites and other online blogs~~.~~ Because holy Quran has highest sensitivity in its content then this sensitivity require a highly protection and integrity mechanisms.

Until now, there is no a procedure or way to make certain integrity of this sensitive content of holy Quran that we can say it is an optimal solution. Thus, there is no a system that can make sure of integrity and monitor the digital copies or verses of the Holy Quran to protect it from tampering or produce fake ones. Sensitivity on Quran content is means that any alteration of just one diacritics or symbol may change the meaning of a whole verse of holy Quran and may a lot of confusion in the minds of Muslims have been created if one single verse is misunderstood or misinterpreted, especially when Muslims do not know it any better. Hakak et al. [4] create a questionnaire and he obtain that Even though 73% of the participants confirmed that they used the internet for finding specific Quranic verses majority of them (71%) they did not concern about the authenticity or integrity of that content .On this problem of holy Quran integrity researchers produce several methods and approaches for solving this specific problems we can talk about them in brief in this section bearing in mind that this study's focus on text based formats where it is one of the easiest and user-friendly format. The first method we talk about is a simple SQL approach using select query which is not the most efficient approach as it needs a particular location to be specified first[5]. Hashing is another approach used by calculate the hash of the particular verse and compare the hash value with the hash value in the database, this approach is preferred to use.
Many researchers use hashing algorithms to make integrity verification on holy Quran such as in Izzat Alsmadi research a framework have been proposed to estimate digital Holy Quran integrity by using MD5 hash functions [2], but as it is known MD5 hash function is not secure anymore and it is severely compromised [6], Almazrooie [3] generate hash tables of the Holy Quran and chosen SHA256 and RIPEMD160 hash functions also a single compression technique used as a verification method and this method is specifically designed for the Quranic verses. But the cryptographic hash function used by Almazrooie study which are SHA256 and RIPEMD160 are vulnerable to attack [7] .Although SHA-2 provides stronger encryption, however, it is vulnerable to length extension attack[8].

Also Almazrooie et al. [3] gave a greater focus on memory resources than on execution time , but in this research, the focus will be on execution time more, as the most prominent feature of the BLAKE3 hash function is that it is the fastest among the hash functions.

Two different tables is generated containing the Quranic verses .One table will be generated by applying selected a cryptographic hash function (SHA256) on the Quranic verses one by one and store result in table. The second table will be generated applying a cryptographic hash function (RIPEMD160) on the Quranic verses one by one and store result in table , then the performance of them is evaluated and compared with another.

B. Research Objectives

The objective that this work aims to accomplish and achieve is to compare the speed and security of SHA256 hash function with, RIPEMD160 hash function.

III. Background

Data Integrity verification is one of the primary concept in information security concepts. Because holy Quran have a high position in Muslims and any tampering on its verses leads a huge problem in Muslims ideologies, so many researchers in the world attracted to Verifying the integrity of the digital Quranic verses and many works have been published in this area. Integrity verification of content refers to the process of managing and assuring the accurateness and correctness of the content being transferred or being made available to end users[1]. Based on online sensitive digital content format In this section we talk about integrity verification techniques used for digital holy Quran, take in your mind that there are text based and image based of available digital holy Quran copies on the internet but this work focus on text based format. There are different kinds of techniques used for checking the integrity of the images we talk about it in brief. Text-based formats: existing in different formats such as TXT, DOC, PDF, etc. and these are inside this study scope. Integrity verification approaches in text based format which include some approaches as discussed below:

A. Integrity verification approaches with text–based formats

Approaches for Content integrity protection from any alteration or tampering in text based formats is SQL Query approach, Hashing and compression all of them has its advantages and limitations the definition for each of them is discussed below:

- **SQL Query approach** : This approach depend on matching between Quran quote from online document and authentic database to detect tampering [5]. But it is not efficient enough because it can decide that there is tampering if the number or name of "surah" is wrong [1].
- **Hashing** : By using the cryptographic hash function and applying it to Quranic verses[2, 3], this approach is chosen in this work and other works because it has the following characteristics
  - Any little alteration can be detected immediately
  - Collision resistance property of a secure hash functions.
- **Compression** : By reduce the size of storing Quran verses to a half, the compression algorithm will be use which it proposed by Almazrooie and used as integrity verification method this will be happen by moving back the compression process and reproducing the genuine verses from the compressed ones [3].

Since in this research, text formats will be used, in addition to the choice to use the hash method, a simple introduction will be presented about the hash functions in the following sections.

B. Hash Functions Algorithms

Cryptography is the science used to maintain the security of the text, integrity is one of the primary objective of cryptography. Hash function means an algorithm which takes a variable length message as input and produces a fixed length string as output [9].This output is called hash value or message digest.

Cryptographic hash function is a one-way function, that is, a function for which it is practically infeasible to invert or reverse the computation[10].There are different families of hash algorithms each of them has its own hash value, message digest and its security properties.

The largest family of cryptographic hash functions Secure Hashing Algorithm (SHA) consists of four classes SHA0 -SHA1-SHA2-SHA3 where SHA-0 had many weaknesses and didn't become widely used. SHA-1 tried to fix this weaknesses, but got broken in 2005. Whereas today SHA-2 commonly used until SHA-3 proves itself as an even more secure function. The SHA-2 family consists of four members SHA-224, SHA-256, SHA-384, and SHA-512[11].

Another hash function such as RACE Integrity Primitives Evaluation Message Digest (RIPEMD) there are five hash functions in the RIPEMD family. RIPEMD-RIPEMD128-RIPEMD160-RIPEMD256-RIPEMD320. RIPEMD160 is the most common, In August 2004, a collision was reported for the original RIPEMD. This does not apply to RIPEMD-160 [12].

Also Whirlpool is one of hash algorithms that takes a message of any length less than 2256 bits and returns a 512-bit message digest .

In this research we focused on SHA256 and RIPEMD160 algorithms , the following sections highlight them.

1. SHA256

SHA 256 is a one of the SHA 2 family group of algorithms, where SHA is an acronym for Secure Hash Algorithm and SHA 256 published in 2001, The outputs value or message digest of SHA-256 is 256 bits long. Where The input of SHA256 algorithm is a message of arbitrary length that smaller than 264 bits [9]. However, SHA-256 has no multi-threading ability, and thus it is not fast enough for transactions [13]

2. RIPEMD160

Race Integrity Primitive Evaluation Message Digest (RIPEMD-160) first published in 1996, , which it is the most common version in the family. RIPEMD-160 was designed in the open academic community, in contrast to the NSA-designed SHA-1 and SHA-2 algorithms[14]. The main factors for choice the RIPEMD160 hash function are security, speed, and size to be adopted in the holy Quran integrity verification[3]

C. Related Works

It is noticeable that in recent times there has been an increased focus on data integrity verification in digital Quranic verse. Digital Quranic verses integrity verification has caught the attention of many researchers and many works have been published in this area. This researchers are listed below:

Alsmadi [2] was design a model to evaluate the integrity of the wording in the digital copy of the Quran ,this model is generating a Meta data related to all words in the Quran preserving the counts and locations. Such model can be used in security as hash algorithms are used where any small change in the data will result in a different hash value.

Almazrooie et al. [3] proposed two methods for digital Holy Quran verses integrity verification. The first method uses cryptographic hash functions SHA256 and RIPEMD160 and generate the hash table of the Holy Quran. The second method is a single compression technique.

Yaakub Bin Idris et al. [15] proposed an integrity verification technique to protect data during processing from incorrectness that leads to false decisions, MD5 and SHA1 cryptographic hash functions are used. Where Hadoop User Experience (Hue). is not equipped with any integrity verification technique to evaluate whether the downloaded data has changed or not .

Tayan and Alginahi [16] proposed an approach based on zero-watermarking and digital-signature for sensitive text documents like holy quran verses to achieve integrity verification and content originality. Where Zero watermarking is an approach for verification and authentication purpose. To authenticated a document by embed it with a specific data sequence obtained from a watermark logo. Then, generate a specific key by using logical XOR operation.

Laouamer [17] proposed an approach to confirm the authenticity of published online digital-Quran text-images this approach based on singular value decomposition (SVD) for watermarking the data .

Ping et al. [18] proposed a public data integrity verification scheme for cloud storage based on the algebraic signature and elliptic curve cryptography. In addition to that this method is used to verify the outsourced data integrity, it is used in resists malicious attacks such as replay attacks, replacing attack and forgery attacks.

Hilal et al. [19] focused on English Text and proposed another integrity verification technique using Watermarking and Natural Language Processing Approach based on first level order of Markov model to improve the accuracy of tampering detection of sensitive English text.
There are many studies that have discussed the comparison between cryptographic hash functions from different aspects, some in terms of speed performance and the other in terms of the ability to resist attacks, some of them will be mentioned below:

A comparative study of MD5 and SHA256 algorithms which determine which is better. The parameters which used to compare in this study are the running time and complexity[9] .

Another study compares different hashing encryption algorithms like MD5, SHA-1, and SHA-512 and provides several suggestions about how to choose different hashing encryption algorithms for particular cases [20].

Prashant Pittalia makes a comparison between SHA-1, SHA-2, SHA-3, MD4, MD5 and Whirlpool hash functions. importance and analysis of various hash algorithms are focused [21].

Alfrhan et al. [22] presented a study on evaluating the performance of SHA-2, SHA-3 candidate called Keccak and PHOTON which is a lightweight hash function , these functions can be used for lightweight blockchain-based Internet of Things (IoT).

IV. Experimental Results

The aims of this paper is to find the better algorithm, where hashing achieved high security and high performance, by comparing among several hashing algorithms over holy Quran verses. This study it recorded execution time for several operations like truncating verses or searching/matching on tables or hashing process that effect the performance.

A. Security Analysis and Results

Here, the results of each experiment will be limited with a description of what was done within each experiment

- ***Experiment1*** : This experiment determine the large change of hash value result if small modification do on the verse. In the verse 77 at Albaqra Sura or chapter ,ya'a character has the diacritic of damma (يُ) in the original reliable verse if diacritic is changing to fatha (يَ) instead of damma in the altered verse , there is a large change in hash value and the hash values for both verses were taken, and this is what the following *Table1* shows.

Table1. The message digests of an original and altered verse are produced by sha256, ripemd160.

Original Verse		((أَوَلَا يَعْلَمُونَ أَنَّ اللَّهَ يَعْلَمُ مَا يُسِرُّونَ وَمَا يُعْلِنُونَ)) البقرة [77]
Hash Algorithms	SHA256	6745235b872bb2eb8ef439d4de3352119eea4a26e8e63e4748387e8d14b2cefe
	RIPEMD160	9add9f21df1f5ab2815add3032e814d1e6f5d405
Altered Verse		((أَوَلَا يَعْلَمُونَ أَنَّ اللَّهَ يَعْلَمُ مَا يَسِرُّونَ وَمَا يُعْلِنُونَ)) البقرة [77]
Hash Algorithms	SHA256	cba16c7d50da453bd099ef238c94824189bd1af9e7b32169e4ad3d10eda5288e
	RIPEMD160	d0d3141ad5aec1cf69f0aa8c402ddf580dbaf3fe

So, if the data is missing due to any technical error or is done intentionally in the verses even though they are just one bit, it causes a big change in the hash value so that it can be easily detected.

- ***Experiment2*** : This experiment check collision resistance on any possible attack., All hash collision probabilities are analysed precisely and clearly as follows:

1. Birthday attack to find collision:

As is well known, birthday attack belongs to a class of brute force attacks. When same message digest are generated by using the two arbitrary messages this called birthday attack process. This attack largely depends upon the higher likelihood of collisions found between random attack attempts [23]. A birthday attack cannot be applied to compromise the hash tables produced in this study because the attacker has no control over the verses whose members must be uniformly distributed [3] ,meaning that the attacker's goal is to find words similar to the Quranic verse then collides it, not to find a collision between two arbitrary messages. Therefore Birthday attack is not applicable in holy Quran verses verification field [3].

2. Second pre-image attack to find collision :

Second-preimage resistance means that for any input x, it is computationally infeasible to find another input x' such that h(x)=h(x') [24].The second pre-image attack on Quranic verse works to find a sentence or fake verses whose message digest collided with a original verse of holy Quran . Almazrooie et al. [3] select CRC32 hash function because its message digest has a small size n= 32 to evaluate the potential of the second pre-image attack in practice and calculate elapsed time to find collision. So verify that this attack is almost infeasible to apply on RIPEMD160, SHA256. The CRC32 attack experiment took only 140 second to find the collision with parallel CPU-GPGPU computation platform [3] .

According to Almazrooie et al. [3] with a high-end computational power resources which capable to compute (6.4 × 1018) operations per second.by using RIPMD160 the attacker will need
((((2160/(6.4 × 1018)) ÷ 60)÷60)÷24) ÷ 365 = 7.24 × 1021 years (7,240 Quintillion years) to come up with a fake verse. Since the size of the message digest in function SHA256 is 256 bit ,it is logical that the resulting number of the time that the attacker need to come up with a fake verse using SHA256 will be greater than the number obtained by using RIPEMD160 . Therefore, the two hash functions are not vulnerable to second preimage attacks.

B. Performance Analysis and Results

Execution time in this work is mainly concerned. Figure1. shows an experiment of the performance analysis result in term of execution time elapsed to generating each tables. For an accurate and a fair comparison between the truncating algorithm and the other two algorithms, the parameters of all experiments are unified and all experiments were conducted under the same environments. The elapsed execution time result measurements were obtained by using the C# function “Stopwatch” where the measured time is in milliseconds (ms).

One of the meanings of the term execution time in our context this means the time elapsed in the process of applying algorithms, such as the first algorithm is the algorithm for cutting verses of the Holy Qur’an and saving them in a database table. This time is saved for each verse separately. Taking into account that the database management program used in this research is Microsoft SQL Server Management Studio v17.6 .

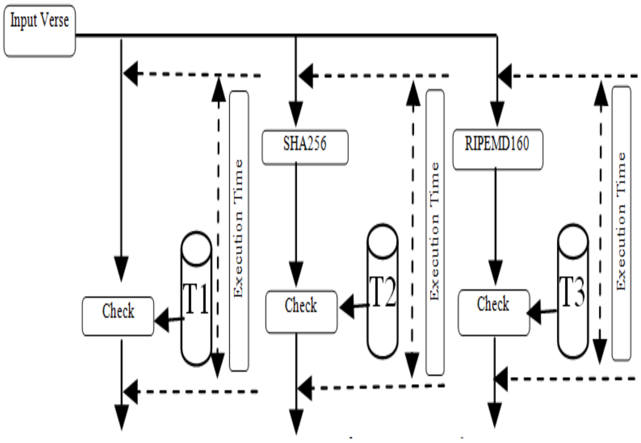

Figure1. Performance analysis

C. Actual Results

The first column in *Table2* indicates the number of rows in the digital Holy Quran database .The order of the rows matches the order of the verses in the hard copy of Holy Quran.

The results of the time elapsed in the process of applying the hash function to the verses of the Qur’an, which was called the term application time, for the application time, the application time of each of the two used hash functions was monitored, and therefore the difference in the results was compared and the following tables illustrate this. Expectedly, the results show that using and RIPEMD160 is faster than SHA256 hash function of the process of hashing digital Holy Quran. The listed results in *Table2* are the average of ten runs. The following results was ran on an Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz 2.60 GHz

Table 2. Performance analysis results of execution time. In milliseconds (ms) and the size is in bytes

Record No	Sura num	Verse num	Verse length	RIPEMD160_Average TimeElapsed	SHA256_Average TimeElapsed
1	1	1	41	0.00696	0.01135
289	2	282	1174	0.02572	0.02679
779	5	110	588	0.01436	0.01638
890	6	101	148	0.0046	0.00979
1406	10	42	98	0.00439	0.00886
2822	24	31	746	0.01874	0.02604
4647	50	17	75	0.00447	0.00684
4649	50	19	74	0.00476	0.00696
5156	60	6	156	0.00512	0.00917
6236	114	6	26	0.00308	0.00462

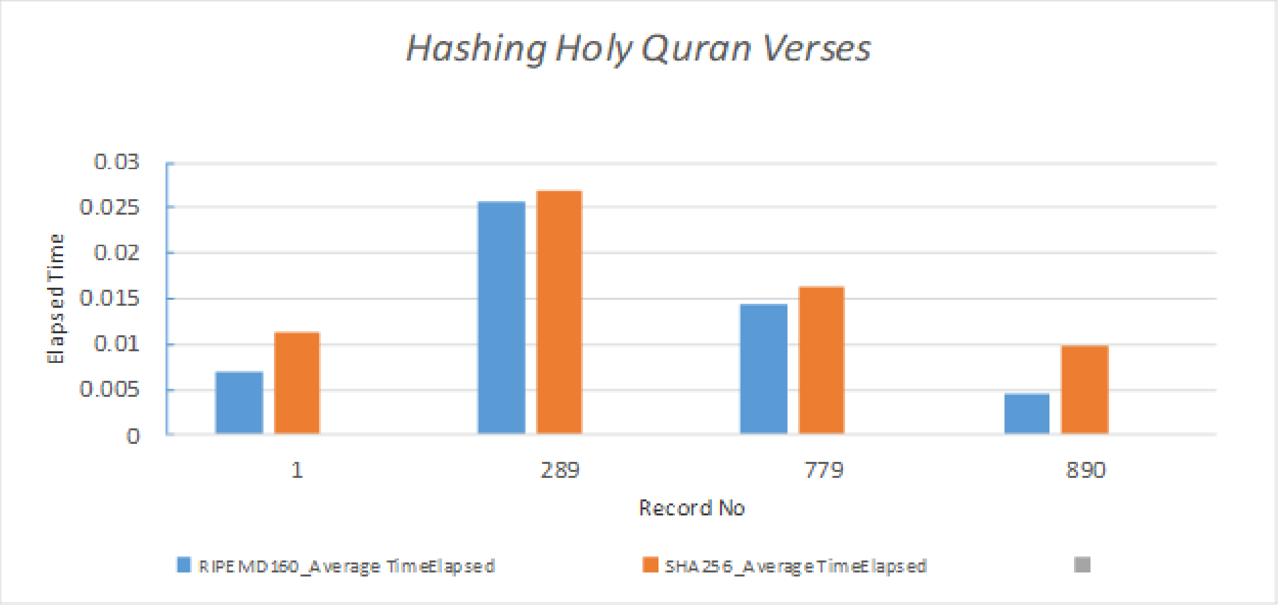

Figure2. Hashing Process Holy Quran Verses

In general, According to the specifications of the laptop used and the program language used, as the specifications of the computer used are Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz 2.60 GHz , and the language used are Microsoft Visual Studio 2022 ,Windows Forms App (.NET Framework) C# Project with GUI interfaces. The results shown in the above Figure2. were obtained, where the figure shows that the RIPEMD160 function is faster than the SHA256 hash function, as the execution time elapsed in the RIPEMD160 function is the shortest time. As for the RIPEMD160 hash function, it is noticeable that in most of the results it is the least in the execution time or the fastest, and this is attributed to the fact that the message digest value in the rate function is 160 bits, i.e. by 20 byte, which is the size of Less than the message digest size in the SHA256 which contain the message digest value 256 bit, which is a value greater than the RIPE message digest. Finally, Parameters used in Comparison between used two hash functions SHA256 and RIPEMD160 are discussed in the following *Table3.*

D. Conclusion

In this study, the performance of two hash functions in integrity verification of digital holy Quran are evaluated. Two tables were generated to evaluate them for the digital Holy Quran while the verification process is applying. The time that was taken in the generation process is termed in this research as the execution time. The results of the conducted experiments show that the RIPEMD160 hash function is faster than SHA256 hash function. Also results say that the size of verse or the length and the place of record number of verse have the main effect on it .

The two hash functions are not vulnerable to second preimage attacks where the resulting number of the time that the attacker need to come up with a fake verse using SHA256 will be greater than the number obtained by using RIPEMD160 .

Table 3. Hash algorithms comparisons

	Block size	**Digest size**	**Word size**	**Rounds**	**Operation**	**Reference**
RIPEMD160	512-bit	160-bit	32-bit	16	AND, NOT, OR, Exclusive-OR	[25]
SHA256	512 - bit	256-bit	32 - bit	64	ADD, XOR, OR, AND SHIFT, ROTATE	[21]

REFERENCES

[1] A. K. Saqib Hakak , Omar Tayan , Mohd Yamani Idna Idris , Gulshan Amin Gilkar, "Approaches for preserving content integrity of sensitive online Arabic content: A survey and research challenges," *Elsevier journal*, **2017**.

[2] M. Z. Izzat Alsmadi "Online integrity and authentication checking for Quran electronic versions," *Elsevier*, **2015**.

[3] A. S. Mishal Almazrooie , Adnan Abdul-Aziz Gutub , Muhammad Syukri Salleh ,Mohd Adib Omar , Shahir Akram Hassan, "Integrity verification for digital Holy Quran verses using cryptographic hash function and compression," *ScienceDirect - Journal of King Saud University – Computer and Information Sciences*, **vol. 32, 2018.**

[4] A. K. SAQIB HAKAK, OMAR TAYAN, MOHD. YAMANI IDNA IDRIS,ABDULLAH GANI, AND SABER ZERDOUMI, "Preserving Content Integrity of Digital Holy Quran: Survey and Open Challenges," *IEEE Access*, **2017**.

[5] O. T. Yasser M. Alginahi, Muhammed N. Kabir1, "Verification of Qur'anic Quotations Embedded in Online Arabic and Islamic Websites," *International Journal on Islamic*, **2013**.

[6] G. P. Reddy, A. Narayana, P. K. Keerthan, B. Vineetha, and P. Honnavalli, "Multiple Hashing Using SHA-256 and MD5," in *Advances in Computing and Network Communications*, ed: Springer, **pp. 643-655, 2021.**

[7] D. M. A. Cortez, A. M. Sison, and R. P. Medina, "Cryptographic randomness test of the modified hashing function of SHA256 to address length extension attack," in *Proceedings of the 2020 8th International Conference on Communications and Broadband Networking*, **pp. 24-28, 2020.**

[8] V. K. Sarker, T. N. Gia, H. Tenhunen, and T. Westerlund, "Lightweight security algorithms for resource-constrained IoT-based sensor nodes," in *ICC 2020-2020 IEEE International Conference on Communications (ICC),* **pp. 1-7, 2020.**

[9] J. T. T. D Rachmawati, A B C Ginting "A comparative study of Message Digest 5(MD5) and SHA256 algorithm," presented at the 2nd International Conference on Computing and Applied Informatics, Indonesia, **2017**.

[10] S. Halevi and H. Krawczyk, "Randomized Hashing and Digital Signatures," **2007**.

[11] H. J. K. Monika Parmar, "Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things," *International Journal of Advanced Computer Science and Applications,* **vol. 12, 2021.**

[12] N. P. Florian Mendel, Christian Rechberger, Vincent Rijmen, "On the Collision Resistance of RIPEMD-160," *Springer,* **2006**.

[13] S. M. D. Ali Maetouq, Noor Azurati Ahmad, Nurazean Maarop, Nilam Nur Amir Sjarif, Hafiza Abas, "*Comparison of Hash Function Algorithms Against Attacks: A Review*," *(IJACSA) International Journal of Advanced Computer Science and Applications,* **vol. 9, 2018.**

[14] S. S. K.Sriprasadh, "Multiple Securities for Cloud Computing Using RIPEMD-160," *SSRN journal,* **2017**.

[15] S. A. I. Yaakub Bin Idris, Nurulhuda Firdaus Mohd Azmi, Azri Azmi, Azizul Azizan, "Enhancement Data Integrity Checking Using Combination MD5 and SHA1 Algorithm in Hadoop Architecture," *Journal of Computer Science & Computational Mathematics,* **vol. 7, September 2017.**

[16] M. N. K. Omar Tayan, YasserM. Alginahi, "A Hybrid Digital-Signature and Zero-Watermarking Approach for Authentication and Protection of Sensitive Electronic Documents," *Hindawi - The Scientific World Journal,* **2014**.

[17] O. T. Lamri Laouamer "An Enhanced SVD Technique for Authentication and Protection of Text-Images using a Case Study on Digital Quran Content with Sensitivity Constraints," *Life Science Journal,* **2013**.

[18] Y. Z. Yuan Ping , Ke Lu , Baocang Wang, "Public Data Integrity Verification Scheme for Secure Cloud Storage," *MDPI journal,* **2020**.

[19] F. N. A.-W. Anwer Mustafa Hilal, Abdelzahir Abdelmaboud, Manar Ahmed Hamza,Mohammad Mahzari ,Abdulkhaleq Q.A. Hassan, "*A Hybrid Intelligent Text Watermarking and Natural Language Processing Approach for Transferring and Receiving an Authentic English Text Via Internet,*" *Computational Intelligence, Machine Learning and Data Analytics The Computer Journal,* **vol. 00, 7 May 2021.**

[20] S. Long, "A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512," *ICEMCE,* **2019**.

[21] P. Pittalia, "A Comparative Study of Hash Algorithms in Cryptography," *International Journal of Computer Science and Mobile Computing IJCSMC,* **vol. 8, pp. 147 – 152, 2019.**

[22] T. M. Aishah Alfrhan a, Abdulatif Alabdulatif "Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT)," *Blockchain: Research and Applications available at ScienceDirect,* **vol. 2, pp. 2096-7209, 2021.**

[23] N. G. Jibi Mariam Biju, Anju J Prakash "CYBER ATTACKS AND ITS DIFFERENT TYPES," *international Research Journal of Engineering and Technology (IRJET),* **2019**.

[24] G. W. Hongbo Yu, Guoyan Zhang, and Xiaoyun Wang, "The Second-Preimage Attack on MD4," presented at the National Natural Science Foundation of China, China, **2005**.

[25] H. D. Bart Preneel, Antoon Bosselaers, "The Cryptographic Hash Function RIPEMD-160," *CryptoBytes* **1997**.

AUTHORS PROFILE

Dr. Naziha Mohammed Al-Aidroos received the B.Sc. degree in Computer Science from Hadhramout University, Yemen in 2003, the M.Sc. degree in Computer Science from Assiut University, Egypt in 2009 and the Ph.D. degree in Data Security from Assuit University, Egypt in 2014. She is an Associate Professor in Department of Computer Science, College of Computers and Information Technology, Hadramout University, Hadhramout, Yemen from 2021until now .She is a Deputy Dean for Student Affairs, College of Computers and Information Technology, Hadramout University, Hadhramout, Yemen. Her interest focuses on the field of Data Security and Cyber Security; she has published a number of papers in Journals and conferences.