www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-11, Issue-1, February 2023
Research Paper

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

E-ISSN:2321-3256

Three Hash Functions Comparison on Digital Holy Quran Integrity Verification

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

[1]Dept. of Information Technology, College of Computers and Information Technology, Ahgaff University, Hadhramaut, Yemen

[2]Computer Science Dept., College of Computers and Information Technology, Hadhramout University, Hadhramaut, Yemen

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

Received: 22/Dec/2022, Accepted: 24/Jan/2023, Published: 28/Feb/2023

***Abstract*—** This paper provides a study of hash functions comparison on holy Quran integrity verification to ensure integrity of data in digital copy of holy Quran. There are many methods available in data security area for integrity verification. This study presents a comparison of three cryptographic hash functions SHA256, RIPEMD160 and Blake3 which used to verify the integrity of digital holy Quran and determine which one is better. Blake3 hash function is chosen in this proposed schema because it has many characteristics, the most important of which is the speed characteristic, and it will be mentioned in detail in Background section. Furthermore security analysis and performance analysis are focused on this study. In security analysis by apply four experiments to find out the strength and effectiveness of each three hash functions and all possible possibilities of hash collisions be carefully analysed and studied. Speed in term of execution time is measuring for all three hash function and this is under the umbrella of the performance analysis. The results that we have obtained say that the Blake3 hash function is the fastest function with the rest two hash functions. And the resulting number of the time that the attacker need to come up with a fake verse using SHA256/BLAKE3 will be greater than the number obtained by using RIPEMD160.

***Keywords*—**Integrity, Holy Quran, Hash functions, SHA256, RIPEMD160, Blake3**.**

I. INTRODUCTION

Verifying the integrity of sensitive texts available on the internet, such as the text of the verses of holy Quran, is an important field and requires more effort and focus on the part of researchers. It is necessary to provide techniques that are easy and accessible to all users and suitable for all types of formats available for digital texts of holy Quran copies.

Usually , internet users share content without verifying the content accurately ,especially Islamic texts , which are among the most sensitive texts ,and one of the visualizing is that any false or manipulated Quran verse may be shared , which may cause confusion in religious concepts , and all this is due to ignoring the verification process from the text of verse before it was shared .God has told us that his book is protected and preserved the Holy Quran from any tampering or alteration , and it is impossible to violate this promise .

In this research an authentic text-based copy of digital Holy Quran will be used. Most of the digital Quran sources come from well-known institutions sponsored by governments such as Tanzil (2021). This resource strive to provide authenticated digital Holy Quran[1]. "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 scope of this work is narrowed down to the performance evaluation of the three types of hash functions BLAKE3, SHA256, RIPEMD160 on integrity verification of the verses of holy Quran and taking into consideration measurement of time , size, and security . Note that, the term table is used to represent database and record of table represent the rows inside database.

This study is based on two hypotheses the first one is that the digital copy of holy Quran is from authenticated source, the second hypothesis is that the Blake3 hash function is the fastest function.

II. RESEARCH PROBLEM

A. Problem Specification

Religious websites, social media websites and other online blogs which may contain online sensitive digital contents can be accessed and downloaded [2]. The holy Quran book requires very capable techniques in protecting against tampering and verifying whether any part of it has been changed, because it is a very sensitive book in terms and hidden meaning as until now there is no specific procedure or method for verification and we can consider it the best solution, but in a field of security information many way that serve this field.

Hashing algorithms are used to make integrity verification on holy Quran such as in Izzat Alsmadi study a framework have been proposed to estimate digital Holy Quran integrity by using MD5 hash functions [3], but as it is known MD5 hash function is not secure anymore and it is severely compromised [4], Almazrooie et al. [1] 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 et al. study which are SHA256 and RIPEMD160 are vulnerable to attack [5] .Although SHA-2 provides stronger encryption, however, it is vulnerable to length extension attack[6]. All hash functions those built with the Merkle–Damgård construction are vulnerable to length extension include such as SHA-256 and RIPEMD-160. More recent hash functions, such as SHA-3 or BLAKE3, aren't vulnerable to length extension[7].

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.
In this proposed paper the BLAKE3 cryptographic hash function is selected to be included in the comparison and evaluation of performance with the functions SHA256 and RIPEMD160 hash functions. The selection of BLAKE3 because it is multithreaded and among the faster cryptographic hashing algorithms currently[8].
In addition, the researcher Kumar et al. [9] said about the BLAKE3 hash function the following characteristic:

- The world's fastest hashing function BLAKE3
- BLAKE3 targets 128-bit security strength against pre-image attack, collision attack or differentiability attacks

B. Research Objectives

This paper aims to:

- Evaluate the performance of Blake3 hash function on Holy Quran integrity verification and
- Compare the speed and security of Blake3 hash function with SHA256, RIPEMD160 hash functions.
- Analyze the security of hash functions by check collision resistance on any possible attack.
- Analyze the execution time of three hash functions

III. BACKGROUND

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[10]. In this section we talk about hash function algorithms used in this study, take in your mind that this work focus on text based format.

A. Hash Functions Algorithms

This research focused on three hash functions SHA256, RIPEMD160 and Blake3 algorithms, the following sections highlight them.

1. SHA stands for Secure Hash Algorithm. Published in 2001. The SHA256 algorithm takes as input a message of arbitrary length that smaller than 264 bits and produces as output a 256-bit message digest of the input. However, SHA-256 has no multi-threading ability, and thus it is not fast enough for transactions [11].
2. Race Integrity Primitive Evaluation Message Digest (RIPEMD-160) is an improved, 160-bit version of the original RIPEMD, and first published in 1996 and the most common version in the family. Security, speed, and space are the main factors while selecting the RIPEMD160 to be adopted in the holy Quran integrity verification[11].
3. BLAKE3 is a cryptographic hash function announced on January 9th, 2020. It is multithreaded and among the faster cryptographic hashing algorithms currently. it is considered safe for all security purpose[8].
   A benchmark published by the BLAKE3 authors on an Intel Cascade Lake-SP 8275CL processor showing it to be 5x faster than BLAKE2 and 15x faster than SHA3-256[12].
   The algorithm has proven much faster than standard algorithms like MD5, SHA-1, SHA-2, SHA-3, and BLAKE2.The performance improvement was achieved by reducing the number of rounds from 10 to 7 and dividing and hashing separately the input block into a contiguous chunk of 1KB This separation allows solving the problem of parallelizing data processing [9].
   Because of these many features of this hash function, it will be chosen in this research to hashing verses of the Holy Qur'an, and this is the first time that this function has been used in integrity verification of Holy Quran verses.

B. Related Works

Verifying the integrity of the digital Quranic verses has attracted many researchers and many works have been published in this area. This researchers are listed below:
Almazrooie et al. [1] have proposed an integrity verification methods for digital verses of the Holy Quran. The first method uses cryptographic hash functions and generate the hash table of the Holy Quran. SHA256 and RIPEMD160 hash functions are chosen. The second method is a single compression technique which manipulates data during the run time. Laouamer and Tayan [13] propose an approach based on singular value decomposition (SVD) for watermarking the data is proposed to confirm the authenticity of published online text-image content, and is applied on digital-Quran text-images as an ideal case study of content with challenging sensitivity constraints. Hilal et al. [14] propose another integrity verification technique used for English Text is Watermarking and Natural Language Processing Approach is proposed based on word mechanism and 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 algorithm which determine which is better. The parameters which used to compare in this study are the running time and complexity[15] .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 [16].

There are also many researchers who talked about the Blake3 function in the field of integrity verification and in other fields as well. Kumarv et al. [9] proposed a trusted third-party auditor (TPA) model which uses lightweight cryptographic system and lightweight hashing technique to ensure data security and data integrity to audit the cloud users outsourced data from cloud service providers. Blake3 is used as a lightweight hashing function in a proposed framework and store data into cloud storage safely.

Shobharam et al. [17] propose a model for Enhancing the Security and Performance of Cloud for E-Governance Infrastructure and BLAKE3 hashing function used as ultra-powerful hash function As he said in order to maintain the information security triad.

IV. Results and Analysis

Since in this study the focus has been on evaluating the performance of three hash functions in encoding verses of holy Quran , the topic has been studied from several aspects, the most important of which are security and performance analysis, and we will address them in the following paragraphs with the results we have reached.

A. Security Analysis and Results

In the study [11] ,experiments were carried out and the results were harvested by focusing on only two hash functions , namely SHA256 and RIPEMD160 .in this study the same experiments will be applied to Blake3 hash function in addition to the two previous functions .

- ***Experiment 1*** : In this experiment , many attacks were focused on and shed light on collision resistance , and if the attacker was able to find the collision , the hash function is vulnerable to this attack. In [11] the attacks on SHA2456 and RIPEMD160 are focused and in this study attacks on all three hash function means in addition Blake3 hash function attacks Is focused also.

a) *The holy Quran verses collisions or duplications*:

Ensure there are no duplications in the message digests of the Quranic verses .Almazrooie said that there are 278 duplicated verses in the Holy Quran. The results show that for any two different verses there is no duplication in the message digest[1]. As we know Surat Al-Rahman in the Holy Qur'an contains a verse that is repeated 31 times. This verse is

الرحمن (13) □□□□□□□□

Each has the same hash value, the Figure.1 below shows the result of the hash values for the same verse repeated in 13, 16 and 18 with the same hash values using the Blake3 hash function

55	13	70158a0b06518440befcf2dbcb2df740b76b4c79974f35719dccdf2f78d1bda3
55	14	2e656e0482ac211a45c1cfb822b67a1b3dc7068df22b6f4afeb146b1c59dcf5f
55	15	a6d7f93c611bf0574a75fe85080be236393ff9cb83701fa9042f67eea858520b
55	16	70158a0b06518440befcf2dbcb2df740b76b4c79974f35719dccdf2f78d1bda3
55	17	521fe1276028a43018e8445d9e236715640211285bf8541743035752b85cc9a5
55	18	70158a0b06518440befcf2dbcb2df740b76b4c79974f35719dccdf2f78d1bda3

Figure. 1. Duplications in the hash values using BLAKE3

If the searching process for this verse content. Logically, the true answer is returned when the first match is found. In integrity verification process the central task is not to provide information about the Surah or Ayah numbers but to confirm the identicalness of the verses content not verses place.

We are still on the subject of discussion about the duplications of the verses and the collisions, but now we will talk about it from another angle, which is the case in which we have two different verses. How likely we to get identical are hash values for these two different verses. The fact that common is that the checking collision experimentally is a hard problem, but for a small size database such as the digital Holy Quran the collision can be checked experimentally. Consider the following two verses: v1 = "بَلِ الْإِنسَانُ عَلَىٰ نَفْسِهِ بَصِيرَةٌ" and the second verse v2 = "ق ۚ وَالْقُرْآنِ الْمَجِيدِ". As it is noted, the two verses are different where |v1| ≠ |v2|. Mathematically it cannot be proved that H (v1) ≠ H (v2) but experimentally it does.

There is a possibility (Pr) for two different verses of different sizes to fall on the same hash value. where the probability of such a collision between verses may occur in that random space is very small (Pr = 1/ 2n) [1] where n is number of bits in message digest.

Therefore, when RIPEMD160 is used the probability of the collision is 1/ 2160, when SHA256 is used the probability is

1/ 2256 and when Blake3 is used the probability is 1/ 2256 where the message digest of Blake3 hash function is 256 bit default output size [18].The empirical results of this experiments show that Pr[∃(H(vi) =H(vj))] = 0, i.e. there is no collision between the verses of the Holy Quran when RIPEMD160 , SHA256 [1] or Blake3 hash functions are used.

b) Birthday attack to find collision:

As is well known, birthday attack is a type of cryptographic attack that belongs to a class of brute force attacks. It is the process of finding two arbitrary message that generate same message digest when processed by a hash function .The success of this attack largely depends upon the higher likelihood of collisions found between random attack attempts [19]. 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 [1] ,meaning that the goal of an attacker is not to find a collision between two arbitrary messages but to find message which collides with a known verse. Therefore Birthday attack is not applicable in holy Quran verses verification field [1].

c) 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')[20].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 . In [1] study CRC32 hash function was chosen 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 in [1] study and on Blake3in this study ,the time required to obtain the fake verse using these three hash function is measured in huge numbers of years .The CRC32 attack experiment took only 140 second to find the collision with parallel CPU-GPGPU computation platform[1] .

According to [1] study 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 both functions SHA256/BLAKE3 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/BLAKE3 will be greater than the number obtained by using RIPEMD160 . Therefore, the three hash functions are not vulnerable to second preimage attacks. When we talk about Blake3 security, it is said to be 128 bits secure for all security goals, including pre-image, collision, or differentiability attacks. Thus, Blake3 is secure like SHA3-256 and other hashes that also targets 128-bit security[12].

B. Performance Analysis and Results

In addiition to security , the performance analysis was also focused on. Figure.2 shows the performance analysis of the three hsh functions used and the methodology followed ,where the input verse which is stored in a separate row in T1 database . this verse enters in to the process of applying hash functions to them and obtaining the value of the hash. Time is calculated here and the result is saved in the database T2 for the values of the Blake 3 hash function and T3 for the values of the SHA256 hash functionand T4 for the values of the RIPEMD160 hash function . The elapsed execution time result measurements were obtained by using the C# function "Stopwatch" where the measured time is in milliseconds (ms).

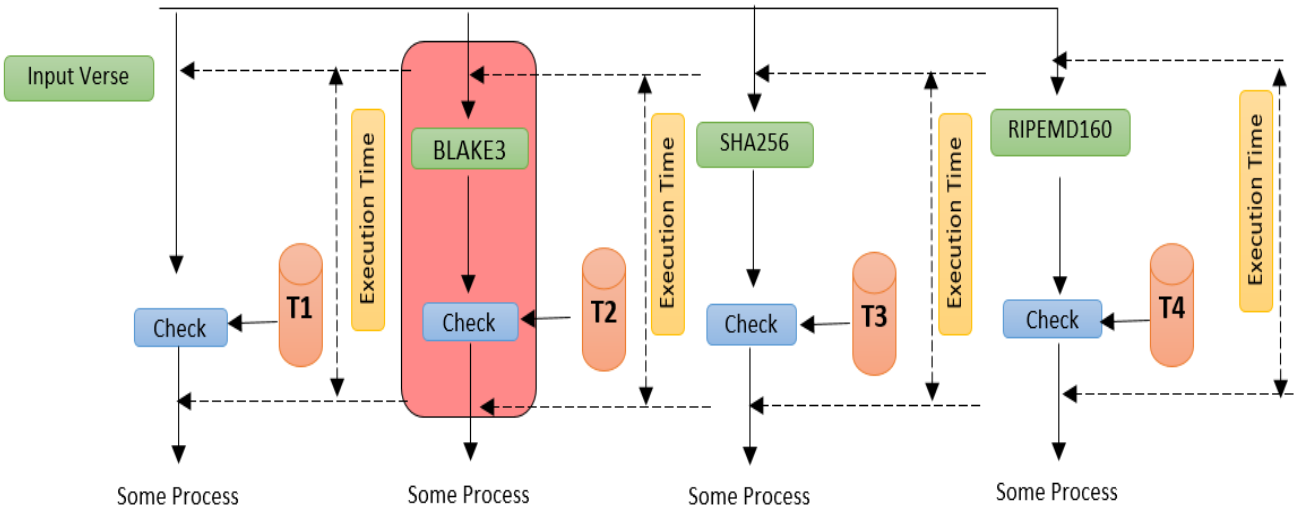

Figure 2: Performance analysis experiment setup

Through researching and experimenting, it was noted that the execution time is divided into two types: the first type is the time of applying the hash functions to the Qur'anic text, and the second type is the time of searching and matching the database for the required verse or hash symbols. In the research [1], the searching time was shed light on, and it was metaphorically called the execution time. In this research, the topic will be presented in greater detail, which is an explanation of both types of execution time, which is the time of searching and matching the required verse or hash value and the time of applying hash function on each verse and produce hash value .

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.

C. Performance Analysis Results

Note that the first column in Table1 refers to the number of record in the digital Holy Quran database which is a text file obtained from Tanzil. The order of the records is according to the order of the verses in the hard copy of Holy Quran.In this paper, the results of both the time elapsed in the search process, which was called in this research the term search time, and the time elapsed in the process of applying the hash function to the verses of the Qur'an, which was called the term applying time, in relation to the search time, the time of searching for a specific verse was monitored Using the text of the verse or by using one of the used hash functions, and for the application time, the applying time of each of the three 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 the Blake3 hash function is faster than using SHA256 and RIPEMD160 hash functions of the process of hashing digital Holy Quran. The listed results in Table1 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.

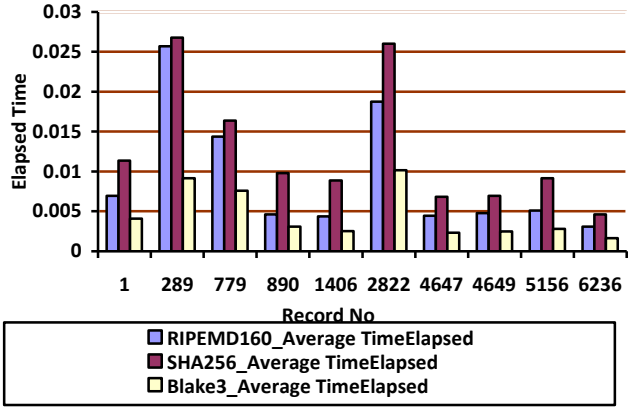

Figure 3. Hashing Holy Quran Verses

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 Figure.3 were obtained, where the figure shows that the BLAKE3 function is actually faster than the rest of the used hash functions, as the execution time elapsed in the BLAKE3 function is the shortest time. By noting the numbers in the last three columns in the Table1, we note that the numbers in the column for results average The execution time of the SHA256 function contains numbers that are from two to three times the results of the Blake3 function, and the same thing applies to the results of the RIPEMD160 function, where it is also the time elapsed in the hash process using the RIPEMD160 is two to three times greater than the time elapsed using the Blake3 function and the graph It also clarifies this, and thus we arrive at the conclusion that the Blake3 function is the fastest in the hashing process by two to three times as much as the least. The previous results talking about time elapsed for applying hash function algorithms on verses, and this final results for this process. Now the elapsed time for searching process in each three hash function and searching process in table of original verses by using matching technique will be focusing in the following lines. The following Table2 shows the results of the time elapsed in the search process using the verse text shown in the column of the original verse and the rest of the columns show the time of the search using the message digest of the three hash functions used.

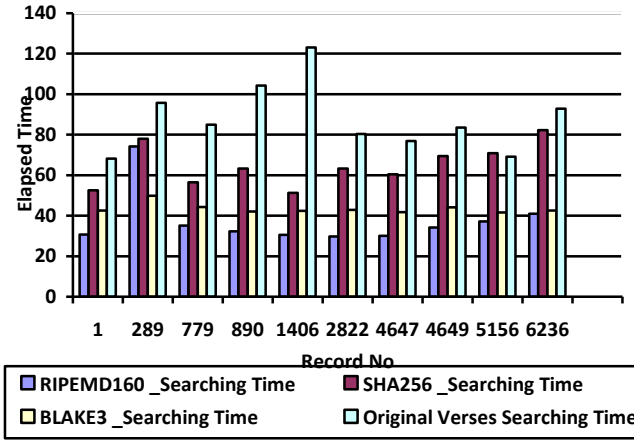

Figure 4. Searching Holy Quran Verses

Both the Table 2 and the Figure 4 show that searching by using the original text of a verse takes longer time than searching using the message digest value of the hash function, and accordingly we come to the conclusion that searching using a message for the hash is faster than searching using the original text of the verse and with more scrutiny of the results and a comparison between the three hash functions used ,we note that the BLAKE3 hash function is faster than the SHA256 hash function, where the search time using it is less. As for the RIPEMD160 hash function, it is noticeable that in most of the results it is the

least in the search 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 and the Blake3 hash functions, both of 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 three hash functions SHA256, RIPEMD160 and BLAKE3 are discussed in the following Table3.

D. Conclusion

SHA256, RIPEMD160 and Blake3 hash functions are evaluated in the field of integrity verification of digital holy Quran. One table is generated for blake3 hash function next to two tables are generated for SHA256, RIPEMD160 hash functions while the verification process is taking place. The time that was taken in the generation process is termed in this research as the applying time, the time that was taken in the verification process is termed in this research as the searching time. The results of the conducted experiments show that the Blake3 hash function is –approximately- 3x faster than SHA256 and 2x faster than RIPEMD160 especially in applying time. And the resulting number of the time that the attacker need to come up with a fake verse using SHA256/BLAKE3 will be greater than the number obtained by using RIPEMD160, 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 and all of this are shown clearly in tables and figures above.

E. Future work

Through this thesis; many ideas not achieved yet. We can suggest some ideas or future study:

- Verification of the Holy Qur'an for all its words according to the drawing that was revealed to it and all text based holy Quran applications or online websites that provide verification or searching property don't take care on this differences in qurani_drawing or called The jurisprudence of Quranic drawing. Any application treat with holy Quran text don't concern this differences in future works I hope to create a verification and searching technique on holy Quran that take care on this some word drawing differences and using the most accurate methods Compare between anther hash functions on digital copy holy Quran integrity verification.

Table1 : Performance analysis results of applying time. The measured time is in milliseconds (ms) and the size is in bytes

Record No	Sura num	Verse num	Verse length	RIPEMD160_Average TimeElapsed	SHA256_Average TimeElapsed	Blake3_Average TimeElapsed
1	1	1	41	0.00696	0.01135	0.0041
289	2	282	1174	0.02572	0.02679	0.00914
779	5	110	588	0.01436	0.01638	0.0076
890	6	101	148	0.0046	0.00979	0.00311
1406	10	42	98	0.00439	0.00886	0.00253
2822	24	31	746	0.01874	0.02604	0.01016
4647	50	17	75	0.00447	0.00684	0.00234
4649	50	19	74	0.00476	0.00696	0.00247
5156	60	6	156	0.00512	0.00917	0.00281
6236	114	6	26	0.00308	0.00462	0.00164

Table 2 : Performance analysis results of searching time. The measured time is in milliseconds (ms) and the size is in bytes.

Record No	sura_num	Vers_num	Verse length	RIPEMD160 _Searching Time	SHA256 _Searching Time	BLAKE3 _Searching Time	Original Verses Searching Time
1	1	1	41	30.7569	52.507	42.5757	68.2412
289	2	282	1174	74.1769	78.0417	49.8669	95.7787
779	5	110	588	35.1333	56.424	44.3638	84.9313
890	6	101	148	32.3398	63.2399	42.0436	104.317
1406	10	42	98	30.5405	51.1976	42.3612	123.1292
2822	24	31	746	29.6825	63.2668	42.8276	80.3263
4647	50	17	75	30.0467	60.4857	41.7551	76.9587
4649	50	19	74	34.1086	69.4664	44.073	83.5532
5156	60	6	156	37.2471	70.9009	41.5786	69.1038
6236	114	6	26	41.0281	82.1896	42.6252	92.9041

Table3 : 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	[21]
SHA256	512 -bit	256-bit	32 -bit	64	ADD, XOR, OR, AND SHIFT, ROTATE	[22]
BLAKE3	64-byte	256-bit	32-bit words	7	ADD ,XOR, Bitwise Right Rotation	[18]

REFERENCES

[1] M. Almazrooie, A. Samsudin, A. a. Gutub, M. S. Salleh, M. A. Omar, and S. A. 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.

[2] S. HAKAK, A. KAMSIN, O. TAYAN, M. YAMANI, I. IDRIS, A. GANI, and S. ZERDOUMI, "Preserving Content Integrity of Digital Holy Quran: Survey and Open Challenges," IEEE Access, 2017.

[3] I. Alsmadi and M. Zarour, "Online integrity and authentication checking for Quran electronic versions," Elsevier, 2015.
[4] Reddy, G. Narayana, A. Keerthan, K. Vineetha, and H. Prasad, "Multiple Hashing Using SHA-256 and MD5," in Advances in Computing and Network Communications, ed: Springer, 2021, pp. 643-655.
[5] C. D. Michael, S. Ariel, and MedinaRuji, "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, 2020, pp. 24-28.
[6] V. K. Sarker, G. T. Nguyen, T. Hannu, and W. Tomi, "Lightweight security algorithms for resource-constrained IoT-based sensor nodes," in ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-7.
[7] J.-P. Aumasson, CRYPTO DICTIONARY 500 Tasty Tidbits for the Curious Cryptographer, 2021.
[8] D. P. Santos, G. D. Silvestre, and A. Carvalho, "Predictable universally unique identification of sequential events on complex objects," Data & Knowledge Engineering - Elsevier, 2021.
[9] S. Kumar, D. Kumar, and H. S. Lamkuche, "TPA Auditing to Enhance the Privacy and Security in Cloud Systems," Journal of Cyber Security and Mobility, vol. 10 3, pp. 537–568, 25 May 2021.
[10] S. Hakak, A. Kamsin, O. Tayan, M. Y. I. Idris, and G. A. Gilkar, "Approaches for preserving content integrity of sensitive online Arabic content: A survey and research challenges," Elsevier journal, 2017.
[11] N. M. Alaidroos and H. S. Baqtian, "A comparative study between RIPEMD160 and SHA256 hash functions on digital Holy Quran integrity verification," ijsrnsc journal, 2022.
[12] A. Machado and A. Domingues, "Ecological friendly proof-of-work cryptocurrency," Suacoin, 2020.
[13] L. Laouamer and O. Tayan, "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.
[14] A. M. Hilal, F. AlWesabi, A. Abdelmaboud, M. A. Hamza, M. Mahzari, and 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.
[15] Rachmawati, Tarigan, and 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.
[16] S. Long, "A Comparative Analysis of the Application of Hashing Encryption Algorithms for MD5, SHA-1, and SHA-512," ICEMCE, 2019.
[17] H. Shobharam, V. Bhaskar, L. Sapparam, S. Singh, and R. Deepak, "Enhancing the Security and Performance of Cloud for E-Governance Infrastructure: Secure E-MODI," International Journal of Cloud Applications and Computing, 2021.
[18] J. Connor, J. Aumasson, S. Neves, and Z. W. Hearn, "BLAKE3 one function, fast everywhere," https://blake3.io, 2021.
[19] J. M. Biju, N. Gopal, and A. Prakash, "CYBER ATTACKS AND ITS DIFFERENT TYPES," international Research Journal of Engineering and Technology (IRJET), 2019.
[20] H. Yu, G. Wang, G. Zhang, and X. Wang, "The Second-Preimage Attack on MD4," presented at the National Natural Science Foundation of China, China, 2005.
[21] B. Preneel, H. Dobbertin, and A. Bosselaers, "The Cryptographic Hash Function RIPEMD-160," CryptoBytes 1997.
[22] 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.

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.

