ISSN: 0067-2904

Wallet Key Generation for a Generic Blockchain based on Speech

Asmaa Rashid*, Asia Ali Salman Al-karkhi, Nidaa Flaih Hassan
Department of Computer Science, University of Technology, Baghdad, Iraq

Received: 21/4/2022 Accepted: 13/7/2022 Published: 30/3/2023

Abstract

As a new technology, blockchain provides the necessary capabilities to assure data integrity and data security through encryption. Mostly, all existing algorithms that provide security rely on the process of discovering a suitable key. Hence, key generation is considered the core of powerful encryption. This paper uses Zernike moment and Mersenne prime numbers to generate strong prime numbers by extracting the features from biometrics (speech). This proposed system sends these unique and strong prime numbers to the RSA algorithm to generate the keys. These keys represent a public address and a private key in a cryptocurrency wallet that is used to encrypt transactions. The benefit of this work is that it provides a high degree of protection to secure personal user transactions by creating secure keys that can be used for insecure channels.

Keywords: Blockchain, Biometrics, Key generation, Zernike moment, Mersenne prime

توليد مفاتيح لمحفظة البلوكجين بالاعتماد على الصوت

اسماء رشيد ، اسيا علي ، نداء فليح
قسم علوم الحاسوب ، الجامعة التكنولوجية ، بغداد ، العراق

الخلاصة

تعتبر تقنية (Blockchain) واحدة من اهم التقنيات في الحقبة الحالية، حيث توفر blockchain القدرات اللازمة لضمان سلامة البيانات وأمن البيانات من خلال استعمال التشفير. ان اغلب الخوارزميات التي تقوم بالحفاظ على البيانات تعتمد على عملية اكتشاف مفتاح مناسب ، لان إنشاء المفتاح الافضل يعتبر جوهر التشفير القوي. في هذه الورقة نستعمل لحظة Zernike وأعداد Mersenne الأولية لتوليد أعداد أولية قوية عن طريق استخراج الميزات من القياسات الحيوية (الكلام). يرسل هذا النظام المقترح هذه الأرقام الأولية الفريدة والقوية إلى خوارزمية RSA لإنشاء المفاتيح. تمثل هذه المفاتيح عنوانًا عامًا ومفتاحًا خاصًا في محفظة للعملات المشفرة تُستعمل لتشفير البيانات في (Blockchain) عامة الاستخدام. كما تكمن فائدة هذا العمل في أنه يوفر درجة عالية من الحماية لتأمين البيانات الشخصية من خلال إنشاء مفاتيح آمنة يمكن استعمالها للقنوات غير الآمنة.

1. Introduction

The fundamental premise of blockchain technology is that it makes use of a distributed database to facilitate a variety of transactions that are totally visible to participants. The

*Email: cs.20.59@grad.uotechnology.edu.iq

blockchain system verifies all transactions, and after a transaction is completed, it preserves all transaction records in perpetuity [1]. According to the blockchain's standards, it enables complete verification of all transactions and maintains an unalterable record of all transactions [2] [3].

In terms of blockchain technology, Bitcoin is one of the most renowned instances, having introduced the world to a multi-billion-dollar market with all transactions being anonymous and devoid of any centralized authority. It is one of the most well-known cryptocurrencies, attracting millions of people to participate, but it is also fraught with controversy [4]. Cryptography, a part of mathematics, is used to create an open, distributed ledger of all transactions involving value, money, items, property, work, or even notes. Cryptography ensures that data cannot be tampered with. It was developed as a way to account for Bitcoin and is currently used in a range of commercial applications. The basic role of the blockchain is to ensure data integrity. Computerizing code and adding any document to the blockchain is a simple process [5].

A blockchain is a form of database that the public can access by holding an encrypted ledger; this implies that a “block” is the current segment of the blockchain that records the most recent transactions. Once authenticated, it becomes an indelible component of the developing blockchain. The system's administrators utilize a computer to store bundles of documents created by others, known as "blocks," in chronological order. The "block" is the most significant component of the blockchain, as it verifies and stores all recent transactions. After the block is completed, it is saved in the blockchain's permanent database. When a block is finished, it takes precedence over the previous one. In this manner, several blocks are linked to one another. Each block carries some information, some from the previous block and some from the new block [6], [7]:

- **Data:** The information contained in each block is determined by the type of blockchain [8].
- **Hash:** The block contains a hash, which can be compared to a biometric. It is always unique and serves to identify the block. Changes made within the block will cause the hash to change. The hash function is extremely useful in the detection and upgrading of blocks. This essentially produces blockchains and secures the blockchain [8].
- **The hash of the previous block:** The initial block is referred to as “the block header”. If the checksum of the preceding blocks is modified, the subsequent blocks become invalid [8].

The Blockchain employs cryptography in a variety of ways, particularly for security and privacy features. Cryptography is used in a variety of applications, including digital signatures, wallet generation, and secure transparent transactions [9-11]. As shown in Figure 1, hashing, digital signatures, and Merkle Trees are some of the most important cryptographic techniques utilized in blockchain [12].

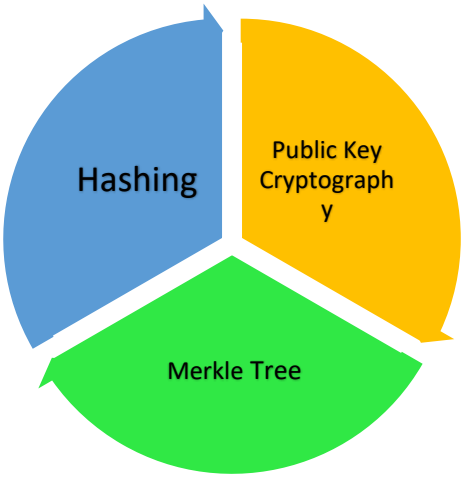

Figure 1: Cryptography's Role in Blockchain [12].

A digital wallet, represented in Figure 2, is made up of private and public keys. The private key produces the public key, and the public key produces the public key identifier. The private key can only be used with the digital object linked to the public key address. A private key can be used to enable the secure management of digital assets. Digital things can be obtained using the public key and the public key ID. The maintenance of private keys is the same as managing digital assets. The purpose of the blockchain wallet is to store and manage cryptographic keys [13] [14]. This application has three key functions: managing user transaction addresses; initiating transfer operations; and accessing transaction history. Each user has a wallet with a unique set of secret keys that they can access. Thus, attackers will target users' digital assets by stealing them from their wallets [15].

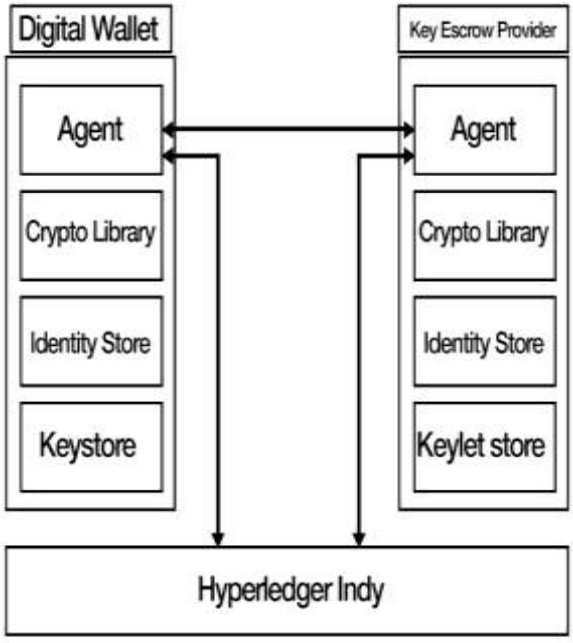

Figure 2: Digital wallet [15].

A cryptocurrency wallet is a sort of cryptography program that stores and manages a user's private keys, addresses, and seeds in the blockchain and cryptocurrency ecosystems. This program is capable of running on a web server, a laptop, a smartphone, or even on

customized hardware [16] [17]. It would securely produce and store keys, as well as facilitate their backup and recovery. There are numerous wallet kinds, including brain wallets, paper wallets, hot wallets, cold wallets, desktop wallets, and many others [18].

Biometric technology is rapidly gaining popularity, becoming an indispensable part of daily life [19]. A biometric system attempts to identify personal data using biological and behavioral characteristics [20 -22]. To be helpful and dependable, biometric technology must meet the following requirements: uniqueness, availability, permanence, collectability, performance, acceptability, and resistance to circumvention [23 -25].

Speech is a biometric blend of physical and behavioral elements. The form and size of the vocal tracts, mouth, nasal cavities, and lips involved in sound synthesis influence the physical qualities of a person's voice. During feature extraction, formants or sound qualities that are unique to each person's vocal tract are frequently measured [26] [27].

The following is how the paper is organized: Section 2 includes related works. The Zernike moment and Mersenne number are presented in sections 3 and 4. The proposed system methodology is presented in section 5. Section 6 describes the results. Section 6 ultimately offers a conclusion.

2. Related Works

Some papers on the implementation of wallet generators have recently been released. Benli [28] suggested a model called BioWallet for securing electronic currency within wallets using biometric methods by utilizing user fingerprints. The proposed model improves both the usability and security of payment transactions involving digital currencies stored in wallets. Gutoski [29] presented an HD wallet that could store several private keys. Some security issues arise because of the hierarchical nature of the private keys, which are linked to each other. Rezaeighaleh [30] proposed a new digital technique for securely backing up a hardware wallet that depends on the hardware wallet's display screen's side-channel human visual verification. They use this mechanism to securely transmit the root of private keys between hardware wallets, even when using an insecure interface such as a smartphone. When this process is complete, the user will have two hardware wallets with identical private keys, one of which she can use as her primary wallet and the other as a backup wallet. Li [31] devised a new methodology for user authentication and used it to create an electronic wallet that enables the user to acquire verification without revealing his or her secret key and increases the use of the secret key application, allowing the currency system to perform the authorization function. He [32] proposed a revolutionary bitcoin wallet administration technique based on Decentralized Multi-Constrained Derangement (DMCD) for securely and reliably storing keys in a decentralized network. The data distribution technique DMCD provides a high degree of data dispersion and a better balance of storage space usage and contribution, thereby ensuring the security and stability of critical storage and recovery. Thota [33] developed and demonstrated a secure mobile software wallet for use on the Hyperledger Fabric blockchain network. According to them, a Hyperledger Fabric transaction flow is an excellent example of the employment of the software wallet in the network. Their presentation demonstrated how software wallets may enhance security and empower end-users by seamlessly integrating with company processes.

3. Zerinke Moment

Zernike defined a series of complex coefficients that define an ortho set over the unit circle's interior, i.e., $x^2 + y^2 = 1$. Assume that V_{nm} is the collection of these formulas (x, y). These expressions have the following structure [34]:

$$V_{nm}(x, y) = V_{nm}(p, \theta) = R_{nm}(p)e^{jm\theta} \quad (1)$$

When n is a positive integer or zero, m is a nonnegative and even integer subject to constraints (n|m|), is the length of the vector from the origin to the (x, y) pixel, and is the counterclockwise angle between the vector and the x-axis. $R_{nm}()$ is a radial polynomial of the form [35]:

$$(p) = \sum_{s=0}^{(n-|m|)/2}(-1)^s \left(\frac{\frac{n-s}{s(n+|m|)}\, j^{n-2s}}{2} s\left(n - \frac{|m|}{2}\right)s\right) \quad (2)$$

Zernike functions are a collection of orthogonal basis functions that are unit circle mapped. Zernike moments are formed by projecting a pattern onto those functions. They share three significant traits [36] [37]:

- The orthogonality of this feature assures that each moment's contribution is distinct and independent.
- The rotation invariance property states that the magnitude of Zernike moments is invariant concerning the pattern's planar rotation around its center of mass.
- Low-frequency components of a pattern are mostly encoded as low-order moments, resulting in data compression. As a result, microscopic descriptors are impervious to noise and deformation.

4. Mersenne Prime Number

The Mersenne number is named after Marin Mersenne, a French monk who conducted early 17th-century research on these numbers. These numbers have the form $Mp = 2^p - 1$, where p is a prime integer [38].

The first few Mersenne prime numbers are 1, 3, 7, 15, 31, 63, 127, 255, etc.

The great Mersenne Prime race has been going on for almost 600 years and shows no signs of slowing down. This list includes some of the more suitably sized prime numbers that create Mersenne primes [39]:
2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203,2281,3217,4253,4423,9689,9941,11213,19937,21701,23209,44497,86243,..... and so on.

5. The Proposed System Methodology

The proposed system goal is to generate a strong and unique prime number that will be used to generate public and private keys for the wallet. In the proposed system, there are three stages: reading audio; feature extraction; and generating prime, as shown in Figure 3.

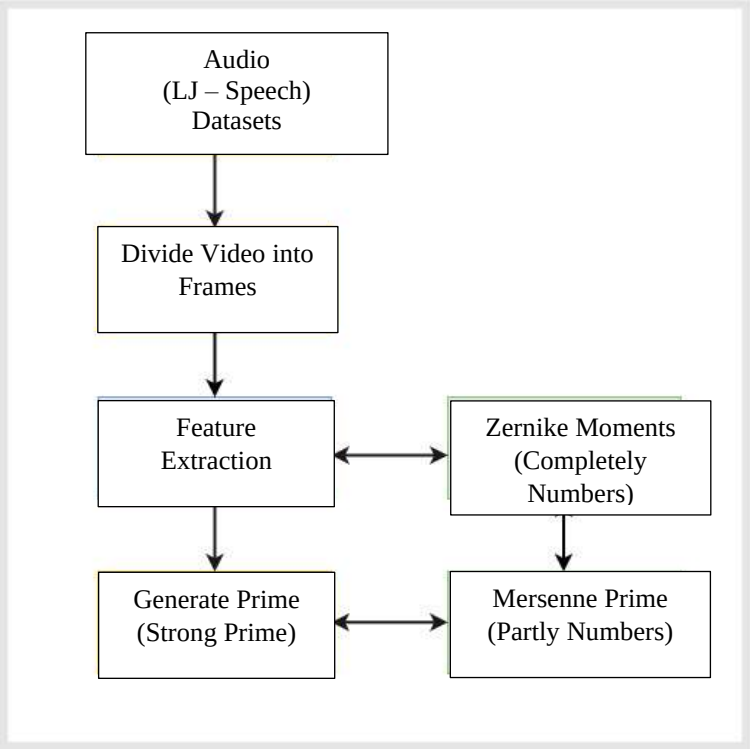

Figure 3: Block diagram of the proposed system.

Initially, the proposed system read the LJ speech dataset that consisted of 13,100 short audio clips, one-dimensional speech signals converted to two-dimensional. Secondly, the feature extraction is started by using the Zernike moment, where at least 25 values (features) are extracted using the Zernike moment. Each feature contains at least 10 digits. There is a good aspect to the Zernike moment that will aid in the generation of a strong key. These features will be treated as float points, as shown in Table 1.

Table 1: Features extracted from each speech.

No. of Speech	Float Points Features
Speech 1	0.31830988618378314, 0.5914831235934308, 0.7279063960930335, 0.8079711591751931, 0.7640721507018284, 0.9605032300660602, 0.6069726063107997, 0.7155732857598893, 0.462331867365562, …….
Speech 2	0.3183098861837909, 0.8509106145003062, 0.38230833132629793, 0.28630842592842837, 0.1473311602400111, 0.16256306535335932, 0.4054412984647574, 0.31354745909421583, 0.2794961439362199, …..
Speech 3	0.3183098861837897, 0.3506705981460109, 0.3372916147357609, 0.30879297625230595, 0.6375328182746908, 0.2550195925612763, 0.2573759355931037, 0.7178481077128454, 0.20650345490203728, ….

Then take a complete integer number of features (prime) and extract the previous and next prime for each one by using the Zernike function, as well as, the proposed system takes a partly integer number of features and passes them to the Mersenne number to extract unique and strong primes by removing redundant primes, as shown in algorithm 1 and algorithm 2.

Algorithm 1: Feature extracting by using Zernike moment.

Input: Biometric speech file;
Output: Extract features (previous and next prime);
Initialization;
Step_1: Divide Input into Frames;
Step_2: For each Frame do the following:
Frame = 1;
While (frame < number of frames)
Step_2.1: Feature extract by using Zernike moment by taking a completely integer number;
Step_2.2: Feature extract by using Mersenne number by taking partly integer number;
Frame = frame + 1;
End while
End

Algorithm 2: Strong prime number extracting

Input: Prime number (n);
Output: Strong prime (n);
Initialization;
Previous prime = n -1;
Next prime = n + 1;
Step_1: For each prime do the following:
While (next prime = false && previous prime = false)
Next prime = next prime + 1;
Previous prime = previous prime - 1;
End while
Step_2: Mean = (previous prime + next prime) / 2;
If (n > mean)
Return strong;
Else
Return weak;
End if
End

Finally, the system recognizes the precise keys that will be utilized in the RSA technique based on these prime features. When both x and y are primes, these keys must be strong. As a consequence, this proposal generates strong keys while maintaining a high level of security to protect information transmitted through insecure channels.

6. Results and Discussion

The proposed system employs a new approach for generating a key from a speech by extracting the features represented by Zernike moments. The proposed system computes the 25 features from Zernike moments after reading each speech from the dataset. Each speech has several parameters, as shown in Table 2.

Table 2: Speech Parameters.

Parameters	Speech 1	Speech 2	Speech 3
Size	415 KB	81.8 KB	221 KB
Type	WAV	WAV	WAV
Number of channels	1	1	1
Sample width	2	2	2
Frame rate	22050	22050	22050
Number of frames	212893	41885	113309

After reading the speech, the proposed system extracts Zernike features from it by using Zernike moments with many radii. Each speech has a twenty-five-prime feature with a radius starting at 2500 and above. Then remove a decimal point from each feature and take a complete number to extract the previous (x) and next prime (y) for each prime feature, as shown in Table 3.

Table 3: Example of four features for each speech

No. of Speech	Zernike Prime (Completely Number)	X Value (Previous Prime)	Y Value (Next Prime
Speech 1	31830988618378314	31830988618378307	31830988618378333
	5914831235934308	5914831235934301	5914831235934373
	7279063960930335	7279063960930301	7279063960930379
	8079711591751931	8079711591751873	8079711591752011
Speech 2	3183098861837909	3183098861837899	3183098861837953
	8509106145003062	8509106145003053	8509106145003151
	38230833132629793	38230833132629779	38230833132629821
	28630842592842837	28630842592842827	28630842592842839
Speech 3	3183098861837897	3183098861837879	3183098861837899
	3506705981460109	3506705981460089	3506705981460119
	3372916147357609	3372916147357439	3372916147357613
	30879297625230595	30879297625230553	30879297625230673

After that, the proposed system takes part of the number of each feature extracted by the Zernike moment and enters it into Mersenne prime to extract a strong and unique prime by removing the redundant primes. For example, the first feature value equals 0.31830988618378314. We take the integer number 31830988618378314 and use the Simpy library to find the next and previous prime for it. Then take the first three integer numbers, 318, and find the next and previous prime. Then enter them into Mersenne prime to see if they are primes and generate a strong and unique prime.

After discovering the prime number, the proposed system used x as a p and y as a q to obtain the public key and private key in the RSA algorithm during the key generation stage to encrypt the data. Table 4 illustrates the comparison between related works in terms of the method used and their encryption algorithms.

Table 4: The comparison between related works

No. of Reference	Method	Encryption Algorithm
[28]	Take biometric information from the user (Username, Password) as a keys	RSA
[29]	With a master public key size of O, it can withstand the leakage of up to m private keys (m).	One-more discrete logarithm problem (1MDLP)
[30]	Even when using an untrusted terminal, such as a smartphone, securely transfer the root of private keys from one hardware wallet to another.	Elliptic-curve cryptography
[31]	Hierarchical key generation scheme	A new digital signature algorithm
[32]	To ensure the high availability of stored keys, use a Shamir-Kademlia-Neighbor (SKN) redundancy method.	DCMD to manage the key efficiently, securely, and stably
The Proposal	Using Zernike moment and Mersenne prime number to generate a strong prime number by extracting the features from biometric (speech) to generating a private key and public key of Wallet.	RSA

7. Conclusion

Blockchain technology is one of the most powerful methods that is currently used in most of the available distributed systems all over the world. However, improving blockchain entities is a critical goal in many of the available and evolving works. In this work, the creation and encryption of a generic blockchain wallet's transactions are designed and implemented. The proposed system generates the keys that are used in the RSA algorithm to secure the transactions. This proposal is presented by extracting the twenty-five feature values from a speech file by using Zernike moment. Then these feature values remove decimal points from them and enter them into Mersenne prime to obtain many prime numbers. These numbers detect unique and strong prime numbers, which will be used in the RSA algorithm to protect the information. Because the created keys are based on biometrics (speech), extracting the features using Zernike moment and utilizing Mersenne number to obtain the keys, these keys will be strong and unique for the specific person that can use them to protect the wallet's transactions. These keys represent a public address and a private key. The public address will be used to receive cryptocurrency and check your Blockchain balance. The private key, on the other hand, will be used in conjunction with this public key to gain access to and spend the cryptocurrency. Our proposed method of generating the key and the RSA algorithm prevents the attacker from guessing the key because it is required to break the ciphertext.

References

[1] T. Kitsantas, A. Vazakidis, and E. Chytis, "A Review of Blockchain Technology and Its Applications in the Business Environment," Conf. Pap., no. October, pp. 1–16, 2019, [Online]. Available: https://www.researchgate.net/publication/334615432.

[2] B. Düdder and O. Ross, "Timber Tracking (Position Paper)," Ssrn, 2017, [Online]. Available: https://www.researchgate.net/publication/324666461_Timber_Tracking_Reducing_Complexity_of_Due_Diligence_by_Using_Blockchain_Technology.

[3] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," 2019, doi: 10.6028/NIST.IR.8202.

[4] Obaida, Tameem Hameed, Abeer Salim Jamil, and Nidaa Flaih Hassan, "Real-time face detection

in digital video-based on Viola-Jones supported by convolutional neural networks," *International Journal of Electrical & Computer Engineering* (2088-8708) 12, no. 3 (2022).

[5] Mahdi, M. S. "Proposed Secure Internet of Everything (IoE) in Health Care," University of Technology, PhD Thesis, Baghdad, Iraq, (2018).

[6] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," Proc. 18th IEEE Int. Conf. High Perform. Comput. Commun. 14th IEEE Int. Conf. Smart City 2nd IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2016, no. December, pp. 1392–1393, 2017, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[7] M. Zhang and Y. Ji, "Blockchain for healthcare records: A data perspective," *PeerJ*, vol. 6, no. May, pp. 2–6, 2018.

[8] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J. Med. Syst.*, vol. 40, no. 10, 2016, doi: 10.1007/s10916-016-0574-6.

[9] Mahdi, Mohammed Salih, Nidaa Falih Hassan, and Ghassan H. Abdul-Majeed, "An improved chacha algorithm for securing data on IoT devices," *SN Applied Sciences*, vol. 3, no. 4 (2021): 1-9.

[10] Mahdi, Mohammed Salih, Raghad Abdulaali Azeez, and Nidaa Falih Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 4 (2020): 2138-2145.

[11] Abdulrazzaq, Husam I., and Nidaa F. Hassan, "Modified Siamese Convolutional Neural Network for Fusion Multimodal Biometrics at Feature Level," In 2019 *2nd Scientific Conference of Computer Sciences* (SCCS), pp. 12-17. IEEE, 2019.

[12] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the Application of Cryptography on the Blockchain," *J. Phys. Conf. Ser.*, vol. 1168, no. 3, 2019, doi: 10.1088/1742-6596/1168/3/032077.

[13] Farhan, A. K., & Mahdi, M. S., "Proposal dynamic keys generator for DES algorithms," *Islamic College University Journal*, vol. 29, pp. 25-48, 2014.

[14] Hassan, Nidaa F., Akbas E. Ali, and Teaba Wala Aldeen, " Generate Random Image-Key using Hash Technique," *Eng. & Tech. Journal*, vol. 28, no. 2, 2010.

[15] Azeez, R. A., Abdul-Hussein, M. K., Mahdi, M. S., & ALRikabi, H. T. S., "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering and Natural Sciences*, vol.10, no. 1, pp. 178-187, 2021.

[16] Mahdi, M., & Hassan, N., "A suggested super salsa stream cipher," *Iraqi Journal for Computers and Informatics*, vol. 44, no. 2, pp. 5-10, 2018.

[17] Alawi, Ataa R., & Nidaa F. Hassan., "A Proposal Video Encryption Using Light Stream Algorithm," *Engineering and Technology Journal*, vol. 39, Part B (2021), No. 01, Pages 184-196.

[18] H. Rezaeighaleh, "Improving Security of Crypto Wallets in Blockchain Technologies," pp. 2020–403, 2020, [Online]. Available: https://stars.library.ucf.edu/etd2020/403.

[19] Hassan, Nidaa F., and Hala Bahjat Abdul Wahab, "Proposed a new approach for voiced/unvoiced decision of speech file using lagrange technique," *Telecommunications and Radio Engineering*, vol. 72, no. 6, 2013.

[20] Hassan, Nidaa Flaih, Ayad Aladhami, and Mohammed Salih Mahdi, "Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps," *Iraqi Journal of Science*, pp. 830-842, 2022.

[21] Ibrahem, Mahmood Khalel, and Hussein Ali Kassim, "VoIP Speech Encryption System Using Stream Cipher with Chaotic Key Generator," *Iraqi Journal of Science*, pp. 240-248, 2021.

[22] Abd Aljabar, Raya W., and Nidaa F. Hassan, "Encryption VoIP based on Generated Biometric Key for RC4 Algorithm," *Engineering and Technology Journal*, vol. 39, Part B (2021), no. 01, Pages 209-221, 2021.

[23] N. Radha and A. Kavitha, "Rank level fusion using fingerprint and iris biometrics," *Indian J. Comput. Sci. Eng.*, vol. 2, no. 6, pp. 917–923, 2012, [Online]. Available: http://www.ijcse.com/docs/INDJCSE11-02-06-146.pdf.

[24] Al-Karkhi, Asia AS, and Maria Fasli, "Virtual Organizations for Resource Allocation under Random Failure in a Network of Agents," *2019 2nd Scientific Conference of Computer Sciences*

(SCCS). IEEE, 2019.

[25] Najm, Hayder, Haider K. Hoomod, and Rehab Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa (20)," *Periodicals of Engineering and Natural Sciences*, 8, no. 3, pp. 1829-1835, 2020.

[26] K. Delac and M. Grgic, "A survey of biometric recognition methods," *Proc. Elmar - Int. Symp. Electron. Mar.*, no. June, pp. 184–193, 2004, doi: 10.1109/ELMAR.2004.1356372.

[27] Ali, Akbas Ezaldeen, and Nidaa Flaih Hassan, "Proposing a Scheme for Human Interactive Proof Test sing Plasma Effect," *Baghdad Science Journal*, vol. 16, no. 2, 2019.

[28] E. Benli, I. Engin, C. Giousouf, M. A. Ulak, and S. Bahtiyar, "BioWallet: A Biometric Digital Wallet," *Twelfth Int. Conf. Syst*. (Icons 2017), no. April 2017, pp. 38–41, 2017, [Online]. Available: https://www.researchgate.net/publication/329373831_BioWallet_A_Biometric_Digital_Wallet.

[29] G. Gutoski and D. Stebila, "Hierarchical deterministic bitcoin wallets that tolerate key leakage," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8975, pp. 497–504, 2015, doi: 10.1007/978-3-662-47854-7_31.

[30] H. Rezaeighaleh and C. C. Zou, "New secure approach to backup cryptocurrency wallets," 2019 IEEE Glob. Commun. Conf. GLOBECOM 2019 - Proc., 2019, doi: 10.1109/ GLOBECOM38437.2019.9014007.

[31] Q. Wei, S. Li, W. Li, H. Li, and M., "Wang, Payment with Online Wallet for Blockchain," vol. 2, no. March 2019. Springer International Publishing, 2019.

[32] X. He, J. Lin, K. Li, and X. Chen, "A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement," *IEEE Access*, vol. 7, pp. 185250–185263, 2019, doi: 10.1109/ACCESS.2019.2961183.

[33] A. R. Thota, P. Upadhyay, S. Kulkarni, P. Selvam, and B. Viswanathan, "Software Wallet Based Secure Participation in Hyperledger Fabric Networks," 2020 Int. Conf. Commun. Syst. NETworkS, COMSNETS 2020, pp. 1–6, 2020, doi: 10.1109/COMSNETS48256.2020.9027445.

[34] P. Singh, A. N. Mishra, and U. Sharma, "Visual Speech Recognition through Zernike Moments," vol. 2, no. 14, pp. 42–45, 2015.

[35] M. Pacharne and V. S. Nayak, "S PEECH CLASSIFICATION USING ZERNIKE MOMENTS," pp. 294–303, 2011, doi: 10.5121/csit.2011.1227.

[36] W. C. Yau, D. K. Kumar, S. P. Arjunan, and S. Kumar, "Visual speech recognition using wavelet transform and moment based features," ICINCO 2006 - *3rd Int. Conf. Informatics Control. Autom. Robot. Proc*., vol. RA, pp. 340–345, 2006, doi: 10.5220/0001210203660371.

[37] S. Xiang, J. Huang, R. Yang, C. Wang, and H. Liu, "Robust audio watermarking based on low-order Zernike moments," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 4283 LNCS, pp. 226–240, 2006, doi: 10.1007/11922841_19.

[38] D. Aggarwal, A. Joux, A. Prakash, and M. Santha, "A new public-key cryptosystem via mersenne numbers," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10993 LNCS, pp. 459–482, 2018, doi: 10.1007/978-3-319-96878-0_16.

[39] S. M. Pund and C. G. Desai, "Implementation of RSA algorithm Using Mersenne Prime," *Int. J. Netw. Parallel Compuring*, vol. 1, no. 3, pp. 33–41, 2013, [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.682.4401&rep=rep1&type=pdf