International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2022 | Issue 53 | Volume 14 | Number 4 | Pages 101-106

WALLET RECOVERY KEYS GENERATOR USING ZERNIKE MOMENT AND MERSENNE PRIME NUMBER

A.R. Salman A.A.S. Al Karkhi N.F. Hassan

Department of Computer Science, University of Technology, Baghdad, Iraq
cs.20.59@grad.uotechnology.edu.iq, asia.a.alkarkhi@uotechnology.edu.iq, 10020@uotechnology.edu.iq

Abstract- Encryption is a key feature of blockchain, a new technology that can ensure data integrity and security. The process of generating a strong key is considered to be the foundation of any algorithm that performs this function. In this paper, we use Zernike moment and Mersenne prime numbers to generate strong prime numbers by extracting the features from biometrics (speech) that are used in the RSA algorithm. The selection of a public key and the production of a private key are the fundamental obstacles in RSA. To produce the keys, the speech wallet keys proposal would use the RSA technique to deliver these unique and strong prime numbers. To encrypt data, these keys serve as a public address and a private key for the wallet. The value of this work is that it creates secure keys that may be used via unsecured channels, hence providing high levels of protection for personal data.

Keywords: Blockchain, Biometrics (Speech), Key Generation, Zernike Moment (ZM), Mersenne Prime (MP), RSA Algorithm.

1. INTRODUCTION

Trust is built into a blockchain network from the start. Blockchain lowers the cost of "trust" by getting rid of the traditional third parties that were needed to provide trust. This is made possible by the way the blocks are linked using cryptography, by spreading the ledger, and by using an algorithm to reach a consensus [1,2]. Many projects want to replace centralized solutions with decentralized solutions based on blockchain. When centralized authorities are taken out of the "trust" business, people have more control over their assets and the cost of trust goes down. But this makes the people in the network more responsible for managing their own keys [3,4].

Asymmetric keys are a key part of figuring out who is in a network and who controls the assets in a blockchain network. An asymmetric key pair is made up of a public key that anyone can use and a private key that needs to be kept secret. In the blockchain, each participant is given an asymmetric key pair. The public key of the asymmetric key pair is used to identify a participant, while the private key is used to control asset ownership and transfers [5] [6].

Private and public key pairs are typically generated by wallets. Client private keys are encrypted and stored on linked server machines when using a web wallet service. Web wallets let users access and manage their assets from any web browser or mobile device. Desktop wallets such as Electrum allow users to encrypt their private keys. More security is provided by symmetrically encrypted digital wallets. In order to retrieve the key, the user must remember the password that was used to encrypt it [7]. Biometric technology is becoming more and more popular and important every day. A biometric system uses physical and behavioral traits to try to find personal information. For biometric technology to be useful and reliable, it must meet the following requirements: it must be unique, available, permanent, and collectible, perform well, be acceptable, and be hard to get around [8-10].

Voice is biometric that shows both physical and behavioral characteristics. How a person's voice sounds depend on the shape and size of the parts of the body that make the sound, such as the vocal tracts, mouth, nasal cavities, and lips. Everyone's physical parts of speech are the same, but the way a person talks changes over time because of things like age, health problems (like a cold), mood, etc. Voice is also not very unique, so it might not be a good way to identify a lot of people. A text-based voice recognition system works by listening for the speaker to say a set phrase. A voice recognition system that doesn't depend on what people say can figure out who is talking no matter what they say. A system that doesn't depend on text is harder to make, but it protects against fraud better than a system that does [11-13]. The following is how the paper is organized: section 2 includes the related works. Zernike moment and Mersenne number are presented in sections 3 and section 4. The RSA is presented in section 5. The methodology is presented in section 6. Section 7 describes the experimental results. Section 8 ultimately offers a conclusion.

2. RELATED WORK

Another issue that must be addressed is the selection of biometric data to produce key pairs in decentralized digital blockchain identity. Researchers have examined a

number of biometric characteristics in the production of that look at how to combine biometric traits with RSA keys. Fabian Monrose [14], proposed a technique for consistently generating a cryptographic key from a user's password-spoken voice. Even if an attacker acquires all system information related to producing or validating the cryptographic key, the key is resistant to cryptanalysis. In addition, the technique is robust enough for the user to dependably regenerate the key by reciting her password. Using 250 recorded utterances from 50 users, describe an empirical evaluation of the technique.

Nguyen [15], proposed a new technique for biometric encryption key (BEK) production depending on both inner production processes and error correction coding to safeguard "private key and biometric information". The integration of the algorithm into the BK-BioPKI system is also described, followed by the results of the experiments. The proposed algorithm and BK-BioPKI system were successfully performed in a network setting at laboratory. Using the Fingerprint Encryption Key, the Private Key may be safeguarded safely and effectively, as demonstrated by the initial experimental results. Thus, they can able to demonstrate the viability of employing biometrics to safeguard Private Keys in PKI systems. Using the Fingerprint Encryption Key, the Private Key may be safeguarded safely and effectively, as demonstrated by the initial experimental results. Thus, they can able to demonstrate the viability of employing biometrics to safeguard Private Keys in PKI systems. Benli [16], introduced a concept called BioWallet for protecting electronic currency within wallets using biometric approaches by employing user fingerprints. This model increases the usability and security of payment transactions involving digital currencies held in wallets.

Rezaeighaleh [17], suggested a new digital technique for securely backing up a hardware wallet that relies on the side-channel human visual verification of the hardware wallet's display screen. Using an unsecured interface such as a smartphone, they employ this approach to securely communicate the root of private keys across hardware wallets. The user will then have two hardware wallets with identical private keys, one of which she can use as her primary wallet and the other as her backup wallet. pund [18], suggested an innovative bitcoin wallet management method depended on Decentralized Multi-Constrained Derangement (DMCD) for storing keys in a decentralized network securely and reliably. DMCD provides a high level of data dispersion as well as a good balance between utilization and contribution of storage space which in turn assuring more stable and secure for crucial storage and recovery.

3. ZERINKE MOMENT (ZM)

The Zernike moment (ZM) can be described as a set of complete, complex, square-integrable orthogonal basis functions defined over the unit disk. ZM was utilized for the first time in picture analysis. ZM is Zernike polynomial-based orthogonal moments. In this case, orthogonality indicates that there is no redundancy or biometric cryptography keys. There aren't many studies overlap of information between the events. Moments are quantified uniquely based on their ordering. ZM's distinctive characteristic is the rotational invariance of its magnitude. ZM is defined as [19-21]:

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

where, 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. The R_{nm} () is a radial polynomial of the form [20]:

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

where,

n: Positive integer or zero

m: Positive and negative integers subject to constraint n-$|m|$ even, $|m| \leq n$

ρ: length of the vector from the origin to (x,y) pixel

θ: angle between vector p and x-axis in a counterclockwise direction

R_{nm}: is a radial polynomial

4. MERSENNE PRIME (MP) NUMBER

The Mersenne prime number (MP) is named after Marin Mersenne, a French monk who conducted early 17th century research on these numbers. These numbers have the form $M_p = 2p$-1, where, p is a prime integer [23] [24]. The first few "Mersenne prime numbers are 1, 3, 7, 15, 31, 63, 127, 255".

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:
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. RSA ALGORITHM

Public key ciphering is the foundation of the RSA algorithm, which uses block ciphering to achieve high security. When using the RSA algorithm, two sets of keys are needed: a public key that's available to everyone, and a private key that's only known for decrypting the cipher text [25][26]. There are two primes in RSA's public key: n=p*q, where n is the product of these two primes. n is not a prime number, but a composite one. The public key e and the composite integer n are required to encrypt a message. Coprime the public key e with n's Euler totient function, $e(n)$. To decode the message, we'll need n (the same key used for encryption) is needed and d (a generated private key). The inverse of the public key e modulo is this private key (n) as shown in Figure 1 [27] [28].

6. THE METHODOLOGY

A block diagram of the proposed encryption system is depicted in Figure 2. The system employs a new method

for generating a key from a speech by extracting the features represented by Zernike moments. The RSA technique will construct an encryption key using these features, which are identified as data points (p, q).

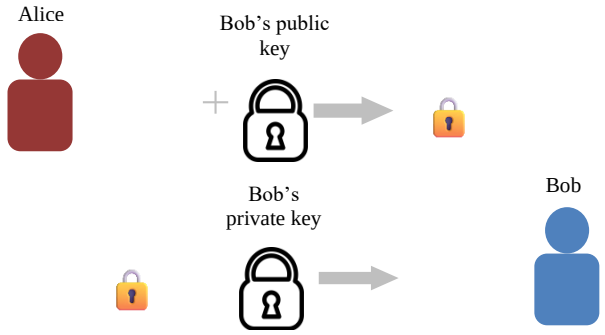

Figure 1. RSA algorithm [27]

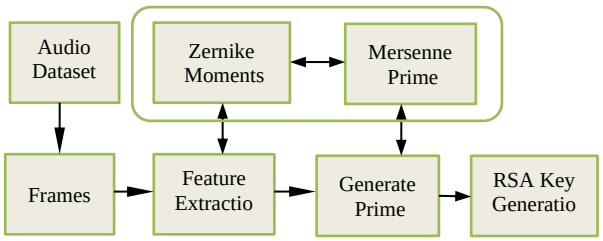

Figure 2. Block diagram of the methodology

A one-dimensional speech signal converted to a two-dimensional format, including 13,100 brief audio clips, was initially fed into the system under consideration. At least 25 values (features) are extracted using the Zernike moment as a starting point for feature extraction. At least ten digits are required for each feature. The Zernike moment has a positive component that will help generate a powerful key. Table 1 shows how these features will be handled as float points.

Table 1. Points extracted from each speech

Speech No.	Float Points Features
Speech 1	0.31830988618378997, 0.2503346036023001, 0.11016895217314297, 0.4223803531891137, 0.2563672714042696, 0.32523389575625883, 0.1462784362427294, 0.259546741135625, 0.46308875620248663, …
Speech 2	0.31830988618379036, 0.5370583286300056, 0.3643668142020986, 0.2952810235820359, 0.4420813761331757, 0.5687312992535854, 0.1575775542976482, 0.46384436905788257, 0.2531395763445344, …

A complete integer number of features (primes) is then extracted, as well as a partial integer number of features (primes) is passed to the Mersenne number to extract unique and strong prime by removing redundant prime. These strong prime numbers are passed to RSA key generation as p and q to get the public key and private key in the RSA algorithm in the step of generating keys of blockchain wallets (private and public keys). Table 2 shows these strong prime numbers that are used in RSA key generation.

Table 2. Example of strong prime numbers that represent p and q

No. of Speech	Strong Prime Numbers (p, q)
Speech 1	(8039511228524857, 28342930113959303), (34710907932725953, 51168864864703981), (5657778010293917, 3473957834994167), …
Speech 2	(3514047606096089, 2970364297263071), (41364796855369937, 14815252998887849), (39616064413257539, 39792777817090901), …

From the table above we can see that it is possible to choose a unique and strong pair of prime numbers for each speech and enter to RSA algorithm to generate private and public keys as shown in algorithm 1. This approach will make it difficult for the attacker to predict the key as it depends on the biometric, giving a high level of security for the user information transfer through insecure channels.

Algorithm 1. RSA Key Generation (Wallet Keys)

Input: Strong prime numbers.
Output: Private and public keys of blockchain wallet.
Start
Step$_1$: Choose to strong prime (p, q).
Step$_2$: Compute $n = p*q$.
Step$_3$: Compute Euler $\Phi = (p\text{-}1)\ (q\text{-}1)$.
Step$_4$: Choose e. $1<e<\Phi$ and must be coprime.
Step$_5$: Generate the private key (n) of the wallet.
Step$_6$: Generate the public key (e) of the wallet.
End

To conclude, the system can identify which keys will be used in the RSA algorithm by taking into account the most important features. In the case of primes, these key pairs must be extremely secure. A strong key is generated while retaining high-security levels to safeguard information sent through insecure channels as a result of this proposal.

7. THE EXPERIMENTAL RESULTS

The 25 Zernike features are computed immediately after each speech sample is read from the dataset by the proposed system. Table 3 lists the various criteria for each speech.

Table 3. Speech Parameters

Parameter	Speech 1	Speech 2
Size	50 KB	49 KB
Speech File Format	WAV	WAV
Number of channels	1	1
Sample width	2	2
Frame rate	22050	22050
Number of frames	24989	24477

The proposed approach uses Zernike moments with a wide range of radius to extract Zernike features from the speech after it has been read. Table 4 shows how to extract the previous and next prime for each prime feature in a speech, which contains twenty-five prime features with a radius starting at 2500 and higher.

Table 4. Example of four features for each speech

No. of Speech	Zernike Prime (Completely Number)	Previous Prime	Next Prime
Speech 1	31830988618378997	31830988618378987	31830988618379029
	2503346036023001	2503346036022983	2503346036023009
	11016895217314297	11016895217314277	11016895217314321
	4223803531891137	4223803531891039	4223803531891187
Speech 2	31830988618379036	31830988618379033	31830988618379063
	5370583286300056	5370583286300033	5370583286300059
	3643668142020986	3643668142020979	3643668142020997
	2952810235820359	2952810235820323	2952810235820377

Table 5. Wallet keys generator

Public Key	30819f300d06092a864886f70d010101050003818d003081890281810086665407b75e2271ed4f366894b526df60e7256ca3182a74c4c76335a77a09ba6eec50b9611052492622db9261eeb15b31132c4316067abeaf4cfa498dad007dcb8ced5ba28105ecd6ed415da8d24188bba2b247578650fdef140987160fc4c495c7f7936ad8ee4c14de944778bc468b92ed2467f9c52ddd249c9089f30322690203010001
Private Key	3082025c0201000281810086665407b75e2271ed4f366894b526df60e7256ca3182a74c4c76335a77a09ba6eec50b9611052492622db9261eeb15b31132c4316067abeaf4cfa498dad007dcb8ced5ba28105ecd6ed415da8d24188bba2b247578650fdef140987160fc4c495c7f7936ad8ee4c14de944778bc468b92ed2467f9c52ddd249c9089f30322690203010001028180000f24e1fc69ef13813434f973d8a87e3ed6be74fb19783ef5cab93a369b83d180ce6aebc057c2ed0d625cb47d241d2f4d8fe967281007f4361f03ff828b9248e70f5ad852efa4629eccb77f752a570e116e7301bd8b6601d991ea6b809efd15e57b1c1f1e4e71fce9732656e37c3e51058f65d37e20c365b8e0c09e4d09fba81024100b6e46c8ab8a5d58d59234f8d3481de8e116cd25834e74d5dfcc4c65b4c24cea2979730b8e1eff8dd35ec31f8f30b0f5bdccfe95651e331c39332a84829de5ee9024100bc1f9ae48f19945540c9ea597c76ebeaf461a3eb426421621c18358bb48ce46eeae2310e86c6098937196ac57b34ed5fd057e0ea2c64f00cadc3e34cccbf7781024046c358cfcfa3b25dcf485f4646339d75a07e5760738faf1a976b574809cd0ffa4ee6db9e1d25294805ce0e83c11ddd6270ac2d1f0dedf6da3200dea5953589c90241008e98364440e3d6b7b86054ae77d57c859fafd31c243ad9c310209995c7c973ed4f451c82324e32343bfb9c1f0c80d5dce683760c8a920812d433c33b17879a0102403af6331f28aabf313841243b8371f99fe26eb90aba92dfda0e1530f300f29026a6a5032d738a70cb657bb1d18973154930d0f4aacf6fcd1369693c9b3923df8e

A strong and unique prime is then extracted by deleting the redundant primes in the proposed system, which takes a partial number of each feature extracted using the Zernike moment. This is a simple example of how to use the simply library to build a strong and unique prime: for the first feature value, we take the integer number 31830988618378997 and take the next and previous prime for it, and then take the first three integer numbers 318 to do the same. Table 5 shows the private and public keys of the wallet that were generated from the speech wallet keys proposal.

To create and encrypt blockchain wallets using the RSA algorithm, an example of asymmetric encryption in cryptography is as follows:

- It is possible to check the balance on the Blockchain using the public address.
- To access and spend the crypto, the private key must be used in conjunction with this public key.

As soon as the proposed system discovered its prime number, it utilized that number to generate the public and private keys in the RSA technique, which is employed for the encryption of data. Table 6 depicted a comparison of similar works in terms of the encryption methods and algorithms used.

Table 6. The comparison of two or more works

No. of Reference	Method	Encryption Algorithm
[14]	Taking biometric information from users (Username, Password) as a key, a total of 250 utterances from 50 people were analyzed.	Segmental VQ Algorithm
[15]	the computation of inner productions and error correction coding to build Biometric Encryption Key (BEK) based on a new technique for protecting "both Private Key and biometric information".	Enrollment algorithm
[16]	Extracting Zernike moments from a voice signal and using them as features of the speech signal	Support Vector Machine (SVM)
[17]	Watermarks can be included into low-order moments to provide a more secure system. The linear relationship between audio amplitude and moments can be deduced by analyzing and subtracting.	New digital algorithm
[18]	To include high level of stored keys which are available, use a Shamir-Kademlia-Neighbor (SKN) redundancy method.	Using DCMD which provides management of the key efficient, secure and stable
The Proposed	Biometric (speech) features can be used to construct a private key and public key for the Wallet by extracting the Zernike moment and Mersenne prime number.	RSA Algorithm

8. CONCLUSION

The RSA algorithm is used by most blockchains to create and encrypt blockchain wallets. By extracting twenty-five feature values from a speech file using Zernike moment, a speech wallet keys proposal was used to safeguard the material in this paper. Mersenne prime is then used to generate a large number of prime numbers from these feature values, which are then utilized in the RSA technique to encrypt the data and keep it safe. Keys based on biometrics (speech), extracted using Zernike moment and obtained using the Mersenne number will be strong and unique for the specific person who can use them to safeguard information, and these keys represent a public address and a private key when constructing a cryptocurrency wallet. Sending or receiving digital currency will be done via the public address. On the other side, this private key is utilized in conjunction with this public key to access and spend the bitcoin. Key generation in our approach and RSA technique means that the key cannot be guessed by an attacker because it is generated in our way.

REFERENCES

[1] T. Kitsantas, A. Vazakidis, E. Chytis, "A Review of Blockchain Technology and Its Applications in the Business Environment", International Conference on Enterprise, Systems, Accounting, Logistics and Management, pp. 1-16, Chania, Crete, Greece, October 2019.

[2] Y. Sabri, "Blockchain Control to Manage the Medical Supply Chain in the Context of Internet of Things (IoT)",

International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 51, Vol. 14, No. 2, pp. 183-189, June 2022.
[3] A.R. Sathya, B.G. Banik, "A Comprehensive Study of Blockchain Services: Future of Cryptography", Int. J. Adv. Comput. Sci. Appl., Vol. 11, No. 10, pp. 279-288, 2020.
[4] M.S. Mahdi, N.F. Hassan, G.H. Abdul Majeed, "An Improved Chacha Algorithm for Securing Data on IoT Devices", SN Appl. Sci., Vol. 3, No. 4, pp. 1-9, 2021.
[5] A.K. Farhan, M.S. Mahdi, "Proposal Dynamic Keys Generator for DES Algorithms. Islamic College University Journal, Vol. 29, pp. 25-48, 2014.
[6] H. Najm, H.K. Hoomod, R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System", Int. J. Interact. Mob. Technol., Vol. 15, No. 02, p. 184, 2021.
[7] J. Seo, D. Ko, S. Kim, V. Sugumaran, S. Park, "Reminisce: Blockchain Private Key Generation and Recovery Using Distinctive Pictures-Based Personal Memory", Mathematics, Vol. 10, Article No. 2047, pp. 1-21, 2022.
[8] E. Benli, I. Engin, C. Giousouf, M.A. Ulak, S. Bahtiyar, "BioWallet: A Biometric Digital Wallet", The Twelfth International Conference on Systems (Icons 2017), No. April 2017, pp. 38-41, 2017.
[9] G. Gutoski, 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.
[10] M.S. Mahdi, R.A. Azeez, N.F. Hassan, "A Proposed Lightweight Image Encryption Using ChaCha with Hyperchaotic Maps", Periodicals of Engineering and Natural Sciences, Vol. 8, No. 4, pp. 2138-2145, 2020.
[11] M. Singh, D. Pati, "Linear Prediction Residual Based Short-Term Cepstral Features for Replay Attacks Detection", Proc. Annu. Conf. Int. Speech Commun. Assoc. Interspeech, Vol. 2018-September, No. 9, pp. 751-755, 2018.
[12] A.R. Thota, P. Upadhyay, S. Kulkarni, P. Selvam, B. Viswanathan, "Software Wallet Based Secure Participation in Hyperledger Fabric Networks", 2020 Int. Conf. Commun. Syst. NETworkS, COMSNETS 2020, pp. 1-6, 2020.
[13] P. Singh, A.N. Mishra, U. Sharma, "Visual Speech Recognition through Zernike Moments", Vol. 2, No. 14, pp. 42-45, 2015
[14] F. Monrose, M.K. Reiter, Q. Li, S. Wetzel, "Cryptographic key Generation from Voice", Proc. IEEE Comput. Soc. Symp. Res. Secur. Priv., No. February, pp. 202-213, 2001.
[15] N.T.H. Lan, T.Q. Duc, N.T. Hoan, "A Biometrics Encryption Key Algorithm to Protect Private Key in BioPKI based Security System", The 7th International Conference on Information, Communications and Signal Processing (ICICS), pp. 1-5, 2009.
[16] M. Pacharne, V.S. Nayak, "Speech Classification Using Zernike Moments", Computer Science & Information Technology (CS and IT), Vol. 02, pp. 294-303, 2011.
[17] S. Xiang, J. Huang, R. Yang, C. Wang, 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.
[18] S.M. Pund, C.G. Desai, "Implementation of RSA Algorithm Using Mersenne Prime", Int. J. Netw. Parallel Compuring, Vol. 1, No. 3, pp. 33-41, 2013.
[19] B. Oluleye, "Zernike Moments and Genetic Algorithm: Tutorial and Application", Br. J. Math. Comput. Sci., Vol. 4, No. 15, pp. 2217-2236, 2014.
[20] E. Yakhti Fard, A. Amiri, "Finding Specific Targets Based on Fuzzy Logic Using Zernike Moments and Support Vector Machine", International Journal on Technical and Physical Problems of Engineering (IJTPE). Issue 23, Vol. 7, No. 2, pp. 60-64, June 2015.
[21] S. Pal, V.G. Diaz, D.N. Le, "Chapter 6 Encryption of Data in Cloud-Based Industrial IoT Devices in IoT: Security and Privacy Paradigm", Internet of Everything (IoE) Series, 1st Edition, CRC Press, pp. 111-131, 2020.
[22] T. Arif, Z. Shaaban, L. Krekor, S. Baba, "Object Classification Via Geometrical, Zernike and Legendre Moments", J. Theor. Appl. Inf. Technol., Vol. 7, No. 1, pp. 31-37, 2009.
[23] M. Bresar, "Chapter Two: Examples of Groups and Rings in Undergraduate Algebra: A Unified Approach", 1st Edition, Springer, pp. 50-55, 2019.
[24] T.H. Obaida, A.S. Jamil, N.F. Hassan, "Real-time Face Detection in Digital Video-based on Viola-Jones Supported by Convolutional Neural Networks", International Journal of Electrical and Computer Engineering (IJECE), Vol. 12, No. 3, pp. 3083-3091, 2022.
[25] N.F. Hassan, A. Aladhami, M.S. Mahdi, "Digital Speech Files Encryption based on Henon and Gingerbread Chaotic Maps", Iraqi Journal of Science, Vol. 63, No. 2, pp. 830-842, 2022.
[26] H. Najm, H.K. Hoomod, R. Hassan, "A Proposed Hybrid Cryptography Algorithm based on GOST and Salsa (20)", Period. Eng. Nat. Sci., Vol. 8, No. 3, pp. 1829-1835, 2020.
[27] M. Mahdi, N. Hassan, "A Suggested Super Salsa Stream Cipher", Iraqi Journal for Computers and Informatics, Vol. 44, No. 2, pp. 5-10, 2018.
[28] R.A. Azeez, M.K. Abdul Hussein, M.S. Mahdi, H.T.H.S. Al Rikabi, "Design a System for an Approved Video Copyright over Cloud based on Biometric Iris and Random Walk Generator using Watermark Technique", Period. Eng. Nat. Sci., Vol. 10, No. 1, pp. 178-187, 2021.

BIOGRAPHIES

Asmaa Rashid Salman was born in Diyala, Iraq on January 18, 1986. She received the B.Sc. degree in Computer Science from Diyala University, Diyala, Iraq in 2007. She is currently a M.Sc. student in Computer Science at University of Technology, Baghdad, Iraq. She has been working at the same university since 2008 to present.

Asia Ali Salman Al Karkhi was born in Baghdad, Iraq on June 20, 1977. She received the Ph.D. degree from University of Essex, UK in 2018. She is a senior lecturer with a permanent job working as a lecturer in computer science at University of Technology, Baghdad, Iraq. She is working on the SCADA projects for developing the data and control in the national control center for power distribution in Baghdad, Iraq.

Nidaa Flaih Hassan was born in Baghdad, Iraq on September 12, 1965. She received the Ph.D. degree in computer science from Computer Science Department, University of Technology, Baghdad, Iraq in 2005. She is currently a Full Professor at Computer Science Department, University of Technology. Her current research interests are in data security, computer security, network security, and image processing.