Secure Encryption of Parallel Chaotic English Education Data Based on 4-order Cellular Neural Network

Mengya Wei

(Corresponding author: Mengya Wei)

School of Foreign Languages, Zhengzhou University of Science and Technology

Zhengzhou 450064, China

Email: ljnan127@163.com

(Received July 15, 2023; Revised and Accepted Oct. 1, 2023; First Online Oct. 10, 2023)

The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection

Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

In English education, the security of English data is very important. It is related to the leakage of English data in the transmission process. In order to solve the problem of uncontrollable processing behavior of parallel chaotic English data encryption and realize secure transmission of English data of network encrypted information, a parallel chaotic English education data based on a 4-order cellular neural network is designed. Firstly, the 4-order cellular neural network is synchronized by the active-passive synchronization method, generating chaotic signals. Then, the synchronous random sequence generated by the synchronous chaotic signal is used for data scrambling and diffusion. Finally, the Advanced Encryption Standard (AES) encryption algorithm is combined with the spiral matrix-based scrambling diffusion model, and the elliptic curve is used to encrypt the AES key. The key and encrypted data are transmitted through the public channel. The experimental results show that compared with the application system based on parameter optimization, the memory ratio and mixed ratio values of host components are closer to the ideal value level under the action of the 4-order cellular neural network, which not only solves the problem of uncontrollable data encryption behavior but also realizes the secure transmission and processing of network encrypted information.

Keywords: 4-order Cellular Neural Network; AES; Parallel Chaotic English Education Data; Scrambling Diffusion

1 Introduction

In the modern era of information diversification, data has become a part of People's daily life, and people use it all the time. Database management technology is widely used in data storage, reading and updating, it can provide corresponding services according to the needs of users, so as to achieve the purpose of easy data management for users [16]. However, when performing specific tasks, databases are vulnerable to a wide range of threats, such as excessive privilege abuse, legal privilege abuse, weak authentication, and backup data exposure [12, 18–20]. Therefore, it is essential to ensure the security of the database [1, 44, 47].

Domestic and foreign scholars have carried out a lot of research on how to ensure the security of database. In 2016, Malik *et al.* [27] proposed a layered reference model of database security agent to improve the ability of key applications to resist malicious attacks on database management System. It enhanced the ability of firewall reference model to defend against enemies by adding transmission unit modification function and attribute value mapping function. With the development of Data information security technology, Transparent Data Encryption (TDE) technology [26] has entered the field of vision of researchers, and since then, due to its excellent characteristics of encryption and decryption processes are completely transparent to applications and users, it has been widely used.

Today, TDE is the best choice for bulk database encryption. Based on the principle of transparent data encryption and the deployment of transparent database encryption process, Almuzaini *et al.* [2] implemented and tested the whole process of transparent database encryption in the SQL Server 2008 environment. Shmueli *et al.* [33] studied five database encryption architectures, including Always Encrypted (AE) and Transparent Data encryption (TDE), Cell Level Encryption (CLE), Dynamic Data Masking (DDM) and Vormetric Transparent Encryption (VTE). The study showed that choosing the right encryption strategy was the most important to keep-

ing your organization safe and protecting data and information. Bhattacharjya *et al.* [3] studied how the massive transparent data encryption of data security solutions on Microsoft SQL Server affected the performance of database management systems. The authors conducted stress and load tests on the performance of each system, and the results showed that using transparent data encryption on standard databases has many advantages.

Cellular Neural Network (CNN) [8, 29] is a feedback neural network proposed on the basis of artificial neural network. It is a nonlinear system formed by a finite number of cells arranged and connected according to certain rules [35]. When the connection and arrangement rules of cells meet certain conditions, CNN can produce high-dimensional hyperchaos [11,46], so it is often used to generate high-dimensional chaotic signals and applied to various encryption systems [22, 28]. At the same time, in order to more effectively resist various attacks, some digital encryption algorithms, such as Elliptic Curve Cryptography (ECC) [15, 17, 36, 38, 41], RSA encryption algorithm [6, 32, 37], etc., are also applied to encryption systems. In reference [31], the plaintext image was converted into two-dimensional code, and then ECC was used for encryption, and an anti-noise image encryption scheme was proposed based on the anti-noise property of two-dimensional code [7, 39, 40]. In reference [42], RSA algorithm was improved to control the initial values of 4-wing and Chen 4D hyperchaotic systems, and an image encryption system with larger key space and shorter encryption time was proposed [13]. Reference [43] firstly compressed the plaintext image, and then used 4D cat mapping and EC-ElGamal algorithm to globally scramble the compressed image [10, 21, 23]. RSA and ECC are the two most mainstream asymmetric cryptography technologies, which have the characteristics of simple key distribution and high key security [4, 14]. However, because of the slow encryption speed of asymmetric key system, it is difficult to be used for big data encryption. AES is a symmetric cryptographic technology that divides plaintext into independent plaintext blocks for block encryption. It has the advantages of flexible key length and fast encryption speed [34], but the key distribution of AES is more complicated. Aiming at the defects of existing image encryption schemes and the advantages of symmetric and asymmetric encryption schemes, an image encryption system based on 4-order cellular neural network and AES encryption is proposed in this paper. The key is distributed through the public channel, and the plaintext image is scrambled and diffused by synchronous random sequence and spiral matrix, which can effectively break the correlation between the plaintext image pixels The ability of encryption algorithm to resist differential attack, noise attack and clipping attack is improved.

In recent years, with the complexity of the Internet construction environment, parallel chaotic data, which combines parallel characteristics with chaotic characteristics, has become the core object of information processing. However, the encryption behavior of this type of data is always affected by various uncontrollable factors, and ultimately the security transmission ability of encrypted information is affected. Although the data encryption system based on parameter optimization can define the unit transmission capability of parallel chaotic data, it cannot encode and decode the transmitted information according to specific read and write rules, which is the main reason why the secure transmission capability of network encrypted information cannot reach the ideal standard level all the time. In order to solve the above problems, a novel parallel chaotic data encryption system is designed under the function of 4-order cellular neural network.

2 Proposed Data Encryption Scheme

The system framework of an image encryption algorithm based on 4-order cellular neural network and AES proposed in this paper is shown in Figure 1. The 4-order CNN hyperchaotic system at the sending and receiving ends realizes chaos synchronization through the active-passive synchronization method [30]. The plaintext image Hash function is used to generate AES encryption key and control the generation of random sequence. After the AES encryption key is encrypted through ECC, it is sent to the receiving end by the public channel, and the generated random sequence is used for image scrambling and diffusion at the sending end respectively.

2.1 Chaotic System

The model of the fourth-order cellular neural network at the sending end is represented as follows:

$$\begin{cases} \dot{x}_1 = -x_3 - x_4 \\ \dot{x}_2 = 2x_2 + x_3 \\ \dot{x}_3 = 14x_1 - 14x_2 \\ \dot{x}_4 = 100x_3 - 100x_4 + 100(|x_4 + 1| - |x_4 - 1|) \end{cases} \tag{1}$$

Where, x_i represents the state variable of the $i-th$ cell at the sending end.

In order to realize chaos synchronization between the sender and the receiver, active and passive synchronization methods are used in this paper, and $s(t) = x_3 + 4x_2$ is used as the driver signal of synchronization. Therefore, Formula (1) can be expressed as:

$$\begin{cases} \dot{x}_1 = -x_3 - x_4 \\ \dot{x}_2 = s(t) - 2x_2 \\ \dot{x}_3 = 14x_1 - 14x_2 \\ \dot{x}_4 = 100x_3 - 100x_4 + 100(|x_4 + 1| - |x_4 - 1|) \end{cases} \tag{2}$$

At the same time, the model of the receiving end is represented as:

$$\begin{cases} \dot{x}'_1 = -x'_3 - x'_4 \\ \dot{x}'_2 = s(t) - 2x'_2 \\ \dot{x}'_3 = 14x'_1 - 14x'_2 \\ \dot{x}'_4 = 100x'_3 - 100x'_4 + 100(|x'_4 + 1| - |x'_4 - 1|) \end{cases} \tag{3}$$

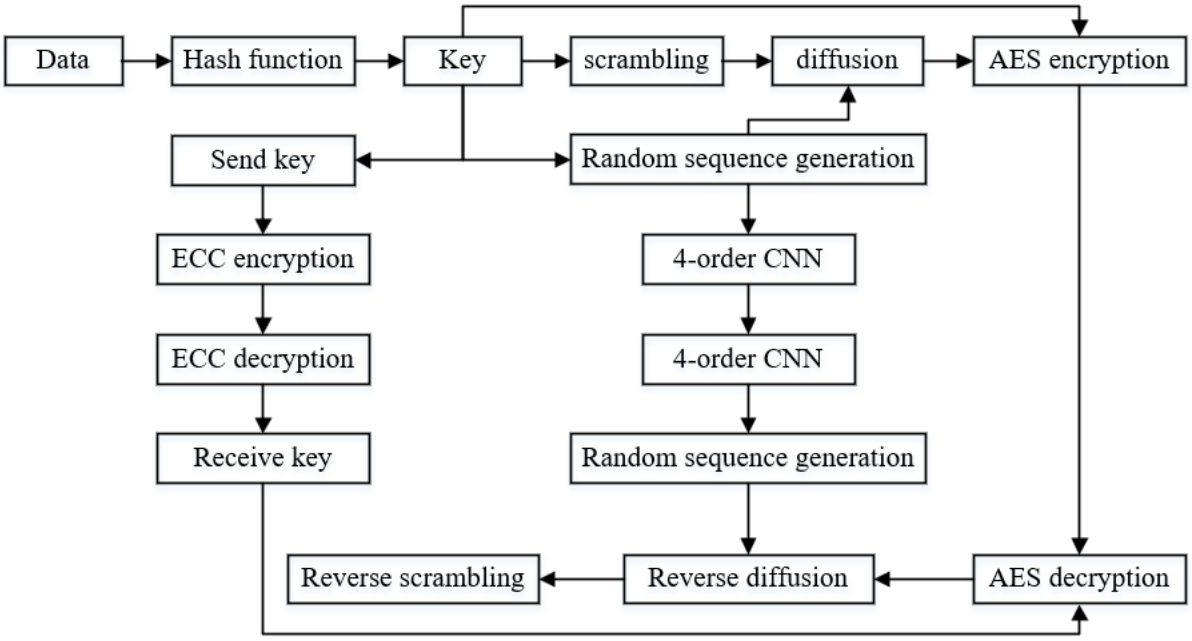

Figure 1: The proposed scheme

Its initial value is [-2,-2,1,1]. In formula (3), x'_i represents the state variable of the $i-th$ cell at the receiving end.

2.2 Key Generation

SHA-512, as a summarization algorithm, has one-way irreversibility, uniqueness and unpredictability, and can generate arbitrary data into a 128-bit hexadecimal string summarization with low algorithmic complexity [9]. This paper uses SHA-512 function to generate 128-bit hexadecimal string from plaintext image as AES key, and is used to generate random sequence, so that different plaintext image has different key and random sequence, which greatly strengthens the security of image.

2.3 Random Sequence Generation

Suppose the size of the encrypted image is $M \times N$, and the chaotic signal generated by CNN and sampled is $C_j(i)$, $i = 1, 2, \cdots, M \times N$, $j = 1, 2, \cdots, 4$. The random sequence is generated as follows:

1) Calculate the SHA-512 value of the image and get the vector H represented by the hexadecimal number;

2) Convert each digit of H to a decimal number, and sum these decimal numbers to get K;

3) Generate random sequences R_1, R_2.

$$R_1(i) = \lfloor K \times (C_1(i) + C_2(i)) \times 10^5 \rfloor \bmod (M \times N) \quad (4)$$

$$R_2(i) = \lfloor K \times (C_3(i) + C_4(i)) \times 10^5 \rfloor \bmod 256. \quad (5)$$

Where, mod(·) represents modulo operation, and $\lfloor$ and $\rfloor$ represents two different random sequences R_1 and R_2 generated by round down operation, which are respectively used for image scrambling and diffusion operations at the sending end, and the same random sequence is used for image inverse diffusion and inverse scrambling operations at the receiving end.

2.4 Scrambling and Diffusion

The scrambling and diffusion operations can greatly reduce the correlation between adjacent pixels. At the same time, in order to compensate for the small key space of AES encryption algorithm, additional nonlinear operations are provided before AES encryption [25]. Therefore, an index-based spiral matrix scrambling method is proposed, the steps are as follows:

1) Obtain the length M and width N of the plaintext image;

2) The spiral matrix S is generated according to M and N;

3) Rearrange the spiral matrix S into one-dimensional vector form s and the plaintext image into one-dimensional vector form p;

4) Arrange the random sequence R_1 from the largest to the smallest, and obtain the index sequence I after the arrangement;

5) The index sequence U is obtained by rearranging the index vectors using the spiral matrix;

6) The scrambling sequence Q is obtained by indexing the scrambling vector;

7) Rearrange the scrambled matrix G according to M and N;

8) The random sequence R_2 is rearranged into a diffusion matrix D according to the spiral matrix S;

9) The scrambling matrix G and diffusion matrix D are specified or operated to obtain the ciphertext matrix E;

2.5 Data Parallel Authentication

The data parallel authentication process must consider three physical indexes: two-factor factor factor, secure storage space of encrypted information [24] and encrypted file marking factor. Two-factor factor factor is also called PIN source protection factor, for parallel chaotic data, because the neural network environment does not limit the information transmission behavior, so the data source upper and lower limit positioning coefficient have unlimited expansion ability, which is easy to affect the encryption execution ability of the system host, but the performance ability of this influence is not unique. The secure storage space of encrypted information refers to the maximum storage capacity of the secure encryption system for parallel chaotic data. In a neural network environment, the larger the remaining space of the database host, the stronger the storage capacity of related data information. The markup coefficient of encrypted files can restrict the practical ability of the data read and write interface module, and generally satisfies the change rule that the larger the coefficient value, the stronger the module structure's ability to process data information [5, 45].

Let ξ indicate the two-factor coefficient and μ indicate the encryption file marking coefficient. $F(d)$ represents an indicator function based on the secure storage space of encrypted information. $F'(d)$ represents the inverse function of $F(d)$. d represents a given parallel chaotic data index. The data parallel authentication condition can be defined as:

$$K = \frac{Q/\xi[F(d) - F'(d)]^2}{\mu\sqrt{x_1^2 + \cdots + x_n^2}}. \tag{6}$$

Where $x_1^2 + \cdots + x_n^2$ represents n different data encryption calibration values, and n represents the maximum query result of the calibration instruction. In order to ensure the application security of encryption system, all parallel identities of chaotic data to be stored must be authenticated by neural network host.

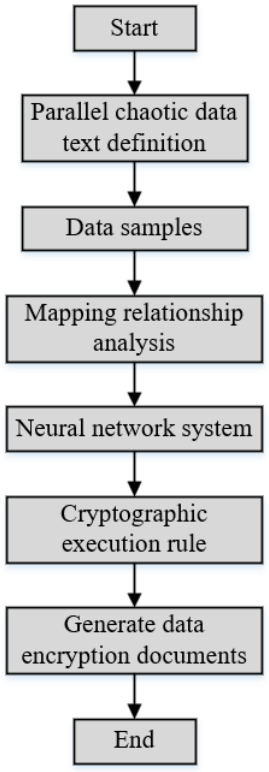

Figure 2: Encryption algorithm execution flowchart

2.6 Encryption Execution Flow

For parallel chaotic data, the encryption execution process should start with the data text definition. In the neural network environment, the storage form of these data samples is not unique, and its specific order of magnitude level should match the real-time input volume of parallel chaotic data samples. In order to satisfy the chaotic mapping relationship of data information, the neural network host should follow the principle of parallel identity authentication when processing data samples. Generally speaking, only the data samples that fully meet the authentication standards can have the ability of secondary transmission. The specific execution process is shown in Figure 2.

In the cognitive range of encryption execution law, whether the information parameter conforms to the data parallel authentication standard is the only criterion to judge whether the information parameter belongs to the parallel chaotic data. At this point, the implementation of the implementation of the hardware and software environment, the combination of the two to complete the parallel chaotic data security encryption system based on neural network design.

3 Instance Analysis

The control ability of network host for parallel chaotic data encryption processing can be considered from two

aspects: memory ratio and mixed ratio. Under normal circumstances, with the increase of parallel chaotic data transmission volume, the two indicators of memory ratio and mixed ratio will show a trend of increasing change, but when the ratio value exceeds the rated limit value (ideal maximum value), it can be judged that the network host is uncontrollable for the current parallel chaotic data encryption processing behavior. Therefore, it can be considered that when the memory ratio and mixing ratio curves are close to the ideal numerical curve, but do not exceed the rated maximum value, the network host has the strongest control ability for parallel chaotic data encryption processing.

Two Internet hosts with identical configurations were selected as experimental objects, in which the experimental host was equipped with a parallel chaotic data security encryption system based on neural network, and the control host was equipped with a data encryption system based on parameter optimization. The specific experimental execution process is as follows:

Step 1: Configure the Internet host of the experimental group and the control group at the same time, and input the neural network control program and parameter optimization control program into the established host components;

Step 2: Control the actual input of parallel chaotic data, and record the value change of correlation coefficient index after removing unreasonable information parameters;

Step 3: Record the value changes of memory ratio and mixed ratio, and compare the actual recorded results with the ideal values.

Table 1 records the change of ideal values of memory ratio index and mixed ratio index in experimental group and control group. Here, PCD: Parallel chaos data input, MER: memory ratio, MIR: mix ratio.

Table 1: Ratio indicator ideal value

PCD/Mb	MER/%	MIR/%
0	12.6	30.1
10	15.8	37.7
20	24.5	45.0
30	26.4	60.1
40	32.0	65.2
50	36.3	68.8
60	37.5	72.9
70	42.6	77.4

According to the analysis of Table 1, as the input volume of parallel chaotic data increases, both the memory ratio index and the mixed ratio index show a continuous increasing trend, but the unit increase value of the mixed ratio index is significantly greater than that of the memory ratio index.

Figure 3 reflects the actual changes of the memory ratio index in the experimental group and the control group.

The analysis of Figure 3 shows that the initial value of the memory ratio index of the experimental group is completely consistent with the initial value of the ideal curve. If this node is not considered, when the input volume of parallel chaotic data is equal to 60Mb, the difference between the memory ratio index of the experimental group and the ideal index is the smallest, only 1.2%. The initial value of the memory ratio index of the control group is slightly larger than the initial value of the ideal curve. If this node is not considered, when the input amount of parallel chaotic data is equal to 10Mb, the difference between the memory ratio index of the control group and the ideal index is at least 4.3%, which is higher than the physical value difference of the experimental group.

Figure 4 reflects the actual changes of the mixed ratio index of the experimental group and the control group.

According to figure 4, the initial value of the mixed proportion index of the experimental group is also completely consistent with the initial value of the ideal curve. If this node is not considered, when the input volume of parallel chaotic data is equal to 60Mb, the difference between the mixed proportion index of the experimental group and the ideal index is the smallest, only 2.8%. The initial value of the mixed proportion index of the control group was significantly higher than the initial value of the ideal curve. During the whole experiment, when the input of parallel chaotic data was equal to 30Mb, the difference between the mixed proportion index of the control group and the ideal index was at least 5.5%, which was higher than the difference of the physical value of the experimental group.

In summary, under the effect of neural network system, both the network host memory ratio index and the mixed ratio index can better fit the ideal value change curve. Compared with the application system based on parameter optimization, the difference between the experimental index and the ideal index is significantly reduced under the effect of the new system. It can not only solve the problem that the parallel chaotic data encryption processing behavior is uncontrollable, but also realize the secure transmission of network encrypted information, which meets the practical application requirements.

4 Conclusion

Aiming at the new parallel chaotic data security encryption system, the neural network system is taken as the entry point, and under the role of BP topology, the encryption processing module and data reading and writing interface module are combined to authenticate the parallel identity of the transmitted information by constructing a chaotic mapping relationship, so as to improve the encryption execution process of the system. From the perspective of experimental results, the trend of the memory

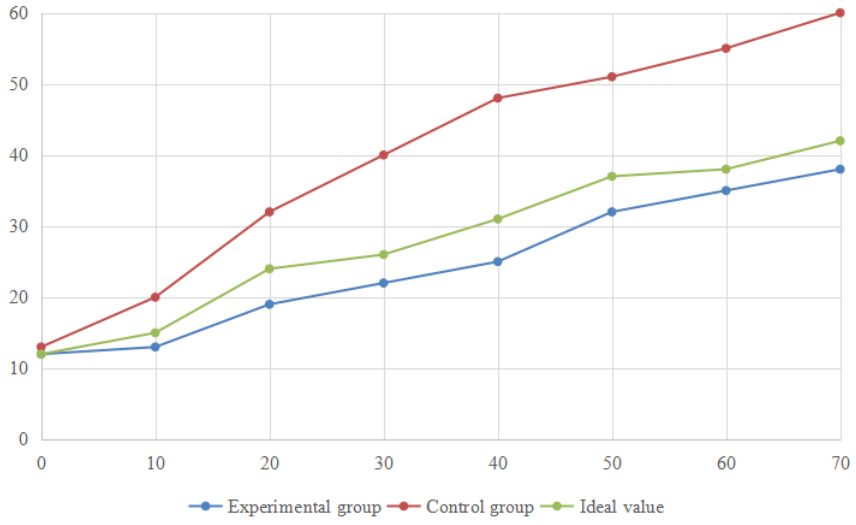

Figure 3: Memory ratio change curve

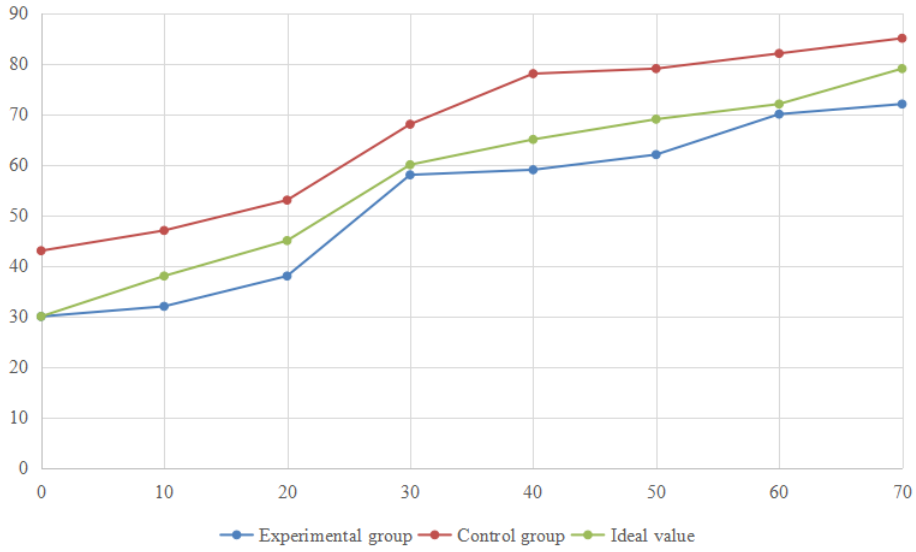

Figure 4: Mixing ratio change curve

ratio index and the mixed ratio index can fit the ideal numerical curve well, and the physical difference between them is low, which not only solves the problem of uncontrollable parallel chaotic data encryption processing, but also realizes the secure transmission of network encrypted information.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, A. Al-Fuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges," *Computer Science Review*, Vol. 43, pp. 100452, 2022.

[2] K. K. Almuzaini, A. K. Sinhal, R. Ranjan, V. Goel, R. Shrivastava, and A. Halifa, "Key Aggregation Cryptosystem and Double Encryption Method for Cloud-Based Intelligent Machine Learning Techniques-Based Health Monitoring Systems," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[3] A. Bhattacharjya, "A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication," *International Journal of Applied Mathematics and Computer Science*, vol. 32, no. 3, pp. 403-413, 2022.

[4] F. Bao, C. C. Lee, M. S. Hwang, "Cryptanalysis and improvement on batch verifying multiple RSA digital signatures", *Applied Mathematics and Computation*, vol. 172, no. 2, pp. 1195-1200, Jan. 2006.

[5] G. Cano-Quiveu, P. Ruiz-de-clavijo-Vazquez, M. J. Bellido, J. Juan-Chico, J. Viejo-Cortos, D. Guerrero-Martos and E. Ostua-Aranguena, "Embedded LUKS (E-LUKS): A Hardware Solution to IoT Security," *Electronics*, vol. 10, no. 23, pp. 3036, 2021.

[6] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[7] C. C. Chang, M. S. Hwang, T. S. Chen, "A new encryption algorithm for image cryptosystems", *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, 2001.

[8] Y. Guo, S. S. Ge, A. Arbi, "Stability of traveling waves solutions for nonlinear cellular neural networks with distributed delays," *Journal of Systems Science and Complexity*, vol. 35, no. 1, 18-31, 2022.

[9] A. Hosoyamada, Y. Sasaki, "Quantum collision attacks on reduced SHA-256 and SHA-512," in *Annual International Cryptology Conference. Cham: Springer International Publishing*, volume. 12825, pp. 616-646, 2021.

[10] L. C. Huang, M. S. Hwang, "Two-party authenticated multiple-key agreement based on elliptic curve discrete logarithm problem", *International Journal of Smart Home*, vol. 7, no. 1, pp. 9-18, 2013.

[11] M. S. Hwang, C. C. Chang, K. F. Hwang, "Digital watermarking of images using neural networks", *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–555, Jan. 2000.

[12] M. S. Hwang, Chii-Hwa Lee, "Secure access schemes in mobile database systems", *European Transactions on Telecommunications*, vol. 12, no. 4, pp. 303-310, 2001.

[13] M. S. Hwang, K. F. Hwang, I. C. Lin, "Cryptanalysis of the batch verifying multiple RSA digital signatures", *Informatica*, vol. 11, no. 1, pp. 15-18, Jan. 2000.

[14] M. S. Hwang, C. C. Lee, Y. C. Lai, "Traceability on RSA-based partially signature with low computation", *Applied Mathematics and Computation*, vol. 145, no. 2-3, pp. 465-468, Dec. 2003.

[15] M. S. Hwang, C. C. Lee, J. Z. Lee, C. C. Yang, "A secure protocol for bluetooth piconets using elliptic curve cryptography", *Telecommunication Systems*, vol. 29, no. 3, pp. 165-180, 2005.

[16] M. S. Hwang, T. H. Sun, C. C. Lee, "Achieving dynamic data guarantee and data confidentiality of public auditing in cloud storage service," *Journal of Circuits, Systems, and Computers*, vol. 26, no. 5, 2017.

[17] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73-84, 2004.

[18] M. S. Hwang and W. P. Yang, "A two-phase encryption scheme for enhancing database security", *Journal of Systems and Software*, vo1.31, no.12, pp. 257-265, 1995.

[19] M. S. Hwang, W. P. Yang, "Multilevel secure database encryption with subkeys", *Data & Knowledge Engineering*, vol. 22, no. 2, pp. 117-131, 1997.

[20] M. S. Hwang, W. P. Yang, "Integrating different semantics of classification levels in heterogeneous distributed database systems", *Journal of Applied Sciences*, vol. 2, no. 5, pp. 553-557, 2002.

[21] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[22] B. Li, Y. Feng, Z. Xiong, W. Yang, G. Liu, "Research on AI security enhanced encryption algorithm of autonomous IoT systems," *Information sciences*, vol. 575, pp. 379-398, 2021.

[23] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245-255, 2003.

[24] C. W. Liu, W. F. Hsien, C. C. Yang, M. S. Hwang, "A survey of attribute-based access control with user re-

vocation in cloud data storage", *International Journal of Network Security*, vol. 18, no. 5, pp. 900-916, 2016.

[25] Y. Liu, L. Wang, A. Qouneh, X. Fu, "Enabling PIM-based AES encryption for online video streaming," *Journal of Systems Architecture*, vol. 132, pp. 102734, 2022.

[26] E. D. Madyatmadja, A. N. Hakim, D. Sembiring, "Performance testing on Transparent Data Encryption for SQL Server's reliability and efficiency," *Journal of Big Data*, vol. 8, pp. 1-14, 2021.

[27] M. Malik, T. Patel, "Database security-attacks and control methods," *International Journal of Information*, vol. 6, no. 1/2, pp. 175-183, 2016.

[28] M. A. Midoun, X. Wang, M. Z. Talhaoui, "A sensitive dynamic mutual encryption system based on a new 1D chaotic map," *Optics and Lasers in Engineering*, vol. 139, pp. 106485, 2021.

[29] F. Musanna, D. Dangwal, S. Kumar, "Novel image encryption algorithm using fractional chaos and cellular neural network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, pp. 2205-2226, 2022.

[30] M. A. Nugroho and V. Suryani, "AADC 3: Active-Active Distributed Controller with 3-in-1 Asynchronous Heartbeat Synchronization Method in Software-Defined Networks," in *9th International Conference on Information and Communication Technology*, pp. 275-279, 2021.

[31] K. Sharma, A. Agrawal, D. Pandey, R. A. Khan, S. K. Dinkar, "RSA based encryption approach for preserving confidentiality of big data," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp. 2088-2097, 2022.

[32] M. Sharma, V. Choudhary, R. S. Bhatia, S. Malik, A. Raina, H. Khandelwal, "Leveraging the power of quantum computing for breaking RSA encryption," *Cyber-Physical Systems*, vol. 7, no. 2, pp. 73-92, 2021.

[33] E. Shmueli, R. Vaisenberg, E. Gudes, Y. Elovici, "Implementing a database encryption solution, design and implementation issues," *Computers & security*, vol. 44, pp. 33-50, 2014.

[34] L. Teng, H. Li, S. Yin, "Im-MobiShare: An improved privacy preserving scheme based on asymmetric encryption and bloom filter for users location sharing in social network," *Journal of Computers*, vol. 30, no. 3, pp. 59-71, 2019.

[35] L. Teng, Y. Qiao, M. Shafiq, G. Srivastava, A. R. Javed, T. R. Gadekallu, "FLPK-BiSeNet: Federated Learning Based on Priori Knowledge and Bilateral Segmentation Network for Image Edge Extraction," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1529-1542, 2023.

[36] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[37] S. F. Tzeng, C. Y. Yang, M. S. Hwang, "A new digital signature scheme based on factoring and discrete logarithms", *International Journal of Computer Mathematics*, vol. 81, no. 1, pp. 9-14, 2004.

[38] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review*, vol. 47, pp. 100530, 2023.

[39] C. C. Wu, M. S. Hwang, S. J. Kao, "A new approach to the secret image sharing with steganography and authentication", *The Imaging Science Journal*, vol. 57, no. 3, pp. 140–151, 2009.

[40] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme", *Journal of Systems and Software*, vol. 84, no. 12, pp. 2196–2207, 2011.

[41] C. C. Yang, T. Y. Chang, M. S. Hwang, "A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 141-145, 2003.

[42] M. Yang, I. Tjuawinata, K. Y. Lam, J. Zhao, L. Sun, "Secure hot path crowdsourcing with local differential privacy under fog computing architecture," *IEEE Transactions on Services Computing*, vol. 15, pp. 4, pp. 2188-2201, 2020.

[43] M. Yang, I. Tjuawinata, K. Y. Lam, T. Zhu, J. Zhao, "Differentially Private Distributed Frequency Estimation," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[44] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, vol. 34, pp. 11475-11490, 2022.

[45] B. You, X. Xiao, "Data encryption technology application in enterprise cost operation management based on cloud computing," *Soft Computing*, pp. 1-13, 2023.

[46] D. Zhang, M. Shafiq, L. Wang, G. Srivastava, S. Yin, "Privacy-preserving remote sensing images recognition based on limited visual cryptography," *CAAI Transactions on Intelligence Technology*, 2023.

[47] P. Zhang, C. Wang, C. Jiang and Z. Han, "Deep Reinforcement Learning Assisted Federated Learning Algorithm for Data Management of IIoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 8475-8484, Dec. 2021.

Biography

Mengya Wei biography. Mengya Wei is with the School of Foreign Languages, Zhengzhou University of Science and Technology, Zhengzhou China. Her research interests include English education, English data security analysis.