International Journal of Innovative Computing, Information and Control
Volume **19**, Number **4**, August **2023**

ICIC International ©2023 ISSN 1349-4198
pp. **1311–1321**

COVERTEXT GENERATION USING FUZZY LOGIC APPROACH IN PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVERTEXT TO IMPROVE INFORMATION CONFIDENTIALITY

Eka Ardhianto[1], Yaya Heryadi[1], Lili Ayu Wulandhari[2] and Widodo Budiharto[2]

[1]Computer Science Department
BINUS Graduate Program – Doctor of Computer Science
Bina Nusantara University
Jl. Kebon Jeruk Raya No. 27, Kebon Jeruk, West Jakarta, Jakarta 11530, Indonesia
eka.ardhianto@binus.ac.id; yayaheryadi@binus.edu

[2]Computer Science Department
School of Computer Science
Bina Nusantara University
Jl. K. H. Syahdan No. 9, Kemanggisan, Palmerah, Jakarta 11480, Indonesia
lili.wulandhari@binus.ac.id; wbudiharto@binus.edu

Received November 2022; revised February 2023

Abstract. *The sophistication of the Internet provides fast and easy information transfer. When passing through an open channel, keeping information confidential becomes important to be well received. Therefore, a robust information confidentiality mechanism is needed. Combining cryptography and steganography provides a robust confidentiality mechanism. Parallel Encryption with Digit Arithmetic of Covertext (PDAC) is a multilevel information security model that combines cryptography and steganography. The PDAC's covertext is a part that affects the strength of confidential information. This study aims to improve the resilience of the PDAC encryption model using a fuzzy logic approach in the covertext generation section. Entropy, and time consumption are used as performance metrics. The experiment's result shows an increasing entropy up to 6.31 with an achievement value of 78.85%, and an average consumption time of 15.674 seconds.*

Keywords: PDAC, Encryption, Covertext, Fuzzy logic, Information security

1. **Introduction.** The level of confidentiality of information determines the information protection needed to prevent non-recipients from obtaining the contents of the information [1]. The security aspect of cryptographic information that focuses on the issue of security assurance is known as the confidentiality aspect [2]. The cryptographic process is a widely used method to ensure the confidentiality of information [3]. Cryptography is an information security science that concentrates on hiding information based on aspects of confidentiality, integrity, and authentication [4]. The main purpose of cryptography is to protect communication channels and networks from internal or external attacks and hide information by scrambling confidential data but leaving encrypted data visible [5,6]. The cryptographic process consists of two subprocesses: encryption, and decryption. The encryption process aims to convert data into a form so that it cannot be understood, meaning that the original data is completely changed so that it cannot be read, while the decryption process aims to get the original data from the encrypted text, which means

DOI: 10.24507/ijicic.19.04.1311

complete recovery of the original data [7]. The encryption method is also called for converting the original message (plaintext) into random and unreadable called ciphertext, and decryption is used to convert the encrypted data back into the original message form as plaintext [8].

Several studies use cryptography and steganography together to increase the confidentiality of information [9-11]. Generally, cryptography is used to encrypt information before it is embedded into the cover using steganography techniques [12]. One encryption model that combines cryptography and steganography is Parallel Encryption with Digit Arithmetic of Covertext (PDAC). PDAC works in steganography with XOR-based cryptographic techniques [13]. PDAC operation requires covertext and encryption key for securing the information. Covertext is a character or symbol that functions as a hiding object in the context of steganography [14]. The encryption key is the value that acts as the key in the encryption phase [15]. The factor that affects the confidentiality of PDAC information lies in how to choose covertext [15].

The encryption key selection process is considered a difficult process, so this process requires a special mechanism [16]. The PDAC's covertext selection also needs to be considered, because the PDAC covertext is used as input for selecting the encryption key. The random function on key selection can be applied, but it is not completely random because the random function has an initial value, so it can be predicted [17]. Choosing keys based on human intuition is also not recommended because they tend to choose keys that are easy to remember and close to their personalities, also humans will use keys repeatedly [17]. Several articles propose fuzzy logic to improve the confidentiality of information. Key selection using fuzzy logic approach strengthens the El Gamal algorithm [18]. The selection of a session key using fuzzy logic approach makes XOR encryption resistance increase in brute force attacks [19]. Fuzzy logic also helps improve the performance of the AES lightweight algorithm [20].

Based on the advantages of fuzzy logic in several previous studies which can improve the performance of cryptographic algorithms, this study aims to improve the resilience of the PDAC encryption model using a fuzzy logic approach. Thus, the PDAC's ciphertext will become more robust against hacker attacks. Entropy, and runtime consumption were used as performance metrics. The results obtained are an increase in PDAC resistance with an entropy value of 6.31 with achievement of 78.85%, and an average consumption time of 15.674 seconds. The achievement of this new value statistically shows a significant improvement.

The discussion in this article is presented in several sections, Section 1 discusses the background, Section 2 contains a literature review, Section 3 contains the proposed method, experiments and results are shown in Section 4, and conclusions are given at the end of the article.

2. **Literature Review.**

Several studies have modified PDAC in capacity, integrity, and authenticity aspects. PDAC begins from the Encryption with Covertext and Reordering (ECR) model [14]. PDAC is presented by compacting some of the ECR processes. PDAC changes the covertext generation process and the integration process on the ECR, thus reducing the size of the PDAC, and making it faster than ECR [13]. The process in PDAC is divided into several parts called: covertext generation, encryption key generation, encryption, and integration. Figure 1 shows the PDAC encryption process.

The next PDAC evolution is called the New PDAC [21]. The New PDAC focuses on the problem of increasing covertext capacity. This additional capacity results in a smaller ciphertext size, thus speeding up the delivery process and saving storage space. Parallel Encryption with Covertext (PECT) modifies PDAC by focusing on information

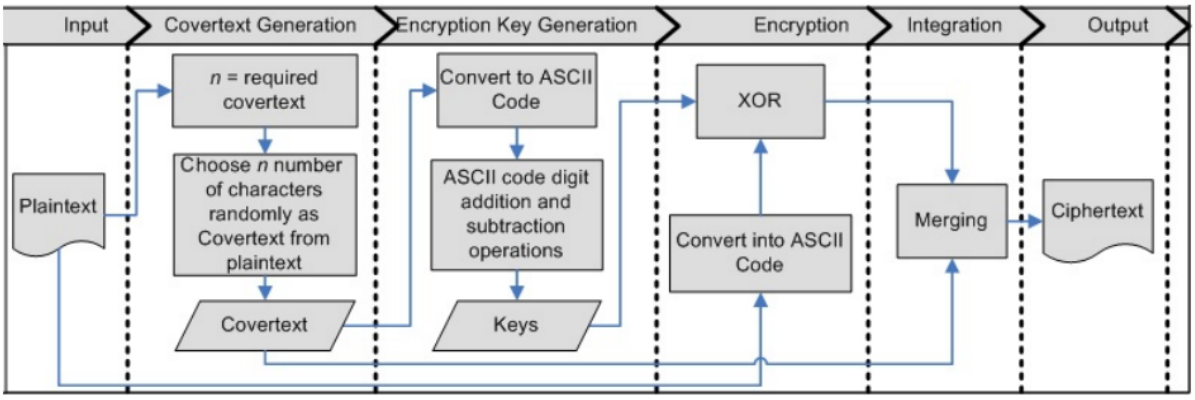

FIGURE 1. The PDAC encryption model, adopted from [13]

authentication aspects [22]. The PECT covertext is selected based on the sequence of vowel and consonant characters grouped in every 4 characters. The vowel and consonant characters are substituted with the numbers 0 and 1, and the resulting binary value is converted to decimal. This sequence of values is used for the authentication process.

The exploration of confidentiality aspects of PDAC was conducted by Ardhianto et al. [15]. This exploration aims to find aspects that affect the level of information security. This experiment compares the PDAC model with PECT. The results show that there are differences in covertext generation techniques between PDAC and PECT. PDAC uses a random function to generate covertext, while PECT generates covertext based on consonants and vowels of the plaintext. This study concluded that the one that affects the level of information security in the PDAC encryption model is the process of covertext generation. This study suggests an improvement in covertext generation techniques to increase the resilience of information security in PDAC.

3. **Proposed Method.** The proposed method to increase the security of information secured using PDAC is shown in Figure 2. This proposed method provides covertext

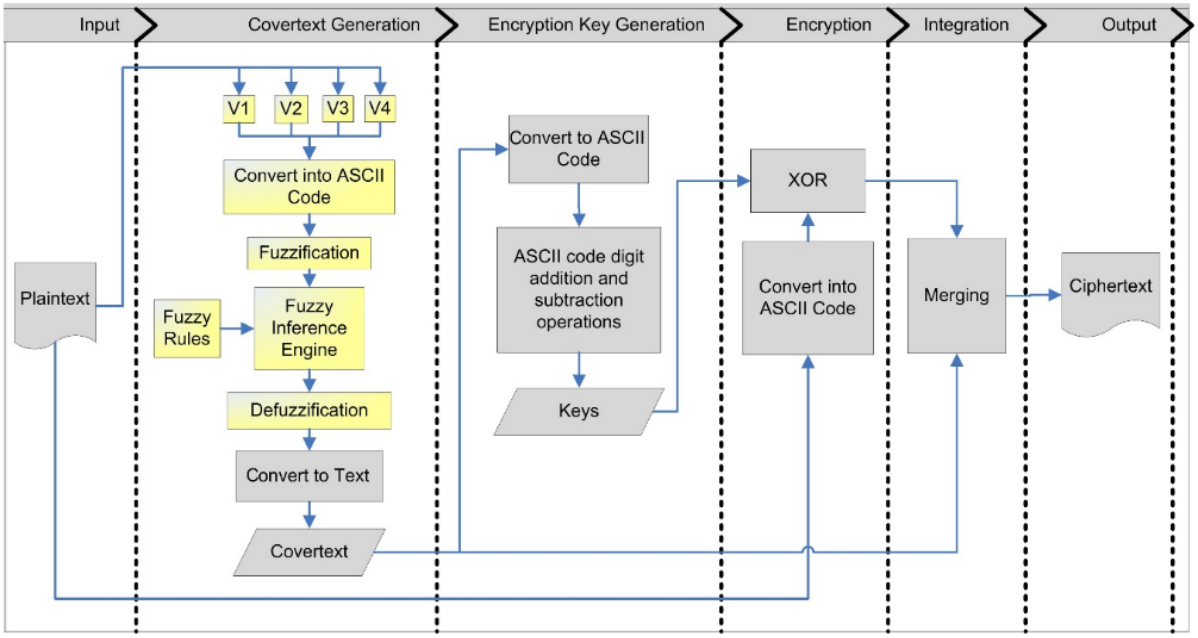

FIGURE 2. The proposed model

generation using a fuzzy logic approach. This method divides each plaintext group into 4 characters. The covertext generation section will produce covertext through a fuzzy logic approach. The fuzzy logic's output is expressed in numerical numbers and converted into characters as covertext. Each plaintext group will correspond with one covertext. The encryption key generation section generates 2 encryption keys from the addition and subtraction of ASCII covertext digits based on covertext obtained. The encryption process is performed using XOR logic between the encryption key and plaintext characters. The output of the encryption process is referred to as encrypted text. In the integration section, the encrypted text is combined with the covertext and becomes ciphertext.

Each character in the group is represented as $V1$, $V2$, $V3$, and $V4$ expressed in ASCII code form. The ASCII code value is used as input in the fuzzification phase. The input Membership Function (MF) is termed: High (μIH) and Low (μIL). The representation to describe the input set is used sigmoid. Sigmoid presents good scalability in both regular and irregular [23]. Figure 3, Equation (1), and Equation (2) represent the input membership representation.

$$\mu IH[x; V1, V2, V3, V4] = \begin{cases} 0, & x \leq 0 \\ 1, & x \geq 255 \\ 2\left(\dfrac{(x)}{255-127}\right)^2, & 0 < x \leq 127 \\ 1 - 2\left(\dfrac{255-x}{255}\right)^2, & 127 < x < 255 \end{cases} \tag{1}$$

$$\mu IL[x; V1, V2, V3, V4] = \begin{cases} 0, & x \geq 255 \\ 1, & x \leq 0 \\ 1 - 2\left(\dfrac{255-x}{255}\right)^2, & 0 < x \leq 127 \\ 2\left(\dfrac{(x)}{255-127}\right)^2, & 127 < x < 255 \end{cases} \tag{2}$$

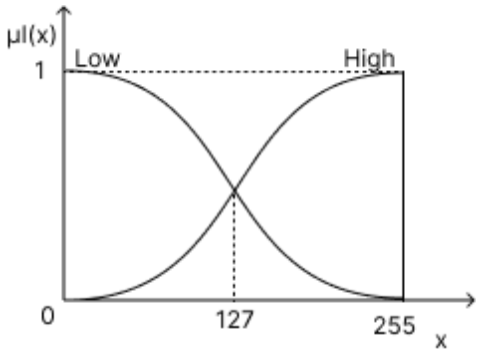

FIGURE 3. Representation of input membership function

In the fuzzy inference engine, the MF generated from each plaintext character is processed according to the design rules. Thus, the MF output is given with linguistic terms: High (μOH) and Low (μOL). The MF output expression is represented in Figure 4, Equations (3) and (4). The fuzzy rules are given in Table 1 created using the multiple conjunctive antecedent method [24]. Multiple conjunctive antecedents are expressed by function (5) [25,26]. Because there are 4 input variables, the 16 fuzzy rules are created in

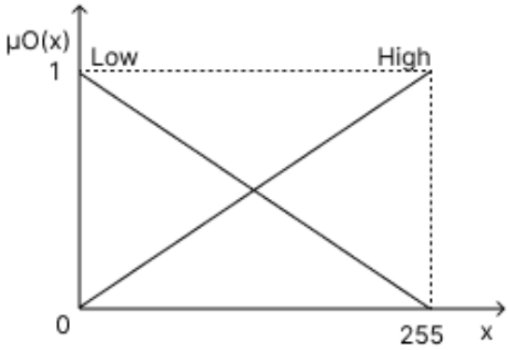

FIGURE 4. Representation of output membership function

Table 1 which accommodate all possible combinations of input and output.

$$\mu OH[x] = \begin{cases} 0, & x \leq 0 \\ 1, & x \geq 255 \\ \dfrac{x}{255}, & 0 < x < 255 \end{cases} \tag{3}$$

$$\mu OL[x] = \begin{cases} 0, & x \geq 255 \\ 1, & x \leq 0 \\ \dfrac{255 - x}{255}, & 0 < x < 255 \end{cases} \tag{4}$$

$$IF\ (condition_1)\ AND\ IF\ (condition_2) \ldots AND\ IF\ (condition_4)\ THEN\ (consequent) \tag{5}$$

TABLE 1. Table of rules

Rule	**Antecedents**	**Consequent**
1	IF $V1$ is μIH AND IF $V2$ is μIH AND IF $V3$ is μIH AND IF $V4$ is μIH	μOH
2	IF $V1$ is μIH AND IF $V2$ is μIH AND IF $V3$ is μIH AND IF $V4$ is μIL	μOH
3	IF $V1$ is μIH AND IF $V2$ is μIH AND IF $V3$ is μIL AND IF $V4$ is μIH	μOH
4	IF $V1$ is μIH AND IF $V2$ is μIH AND IF $V3$ is μIL AND IF $V4$ is μIL	μOH
5	IF $V1$ is μIH AND IF $V2$ is μIL AND IF $V3$ is μIH AND IF $V4$ is μIH	μOH
6	IF $V1$ is μIH AND IF $V2$ is μIL AND IF $V3$ is μIH AND IF $V4$ is μIL	μOH
7	IF $V1$ is μIH AND IF $V2$ is μIL AND IF $V3$ is μIL AND IF $V4$ is μIH	μOH
8	IF $V1$ is μIH AND IF $V2$ is μIL AND IF $V3$ is μIL AND IF $V4$ is μIL	μOH
9	IF $V1$ is μIL AND IF $V2$ is μIH AND IF $V3$ is μIH AND IF $V4$ is μIH	μOH
10	IF $V1$ is μIL AND IF $V2$ is μIH AND IF $V3$ is μIH AND IF $V4$ is μIL	μOH
11	IF $V1$ is μIL AND IF $V2$ is μIH AND IF $V3$ is μIL AND IF $V4$ is μIH	μOH
12	IF $V1$ is μIL AND IF $V2$ is μIH AND IF $V3$ is μIL AND IF $V4$ is μIL	μOH
13	IF $V1$ is μIL AND IF $V2$ is μIL AND IF $V3$ is μIH AND IF $V4$ is μIH	μOH
14	IF $V1$ is μIL AND IF $V2$ is μIL AND IF $V3$ is μIH AND IF $V4$ is μIL	μOH
15	IF $V1$ is μIL AND IF $V2$ is μIL AND IF $V3$ is μIL AND IF $V4$ is μIH	μOH
16	IF $V1$ is μIL AND IF $V2$ is μIL AND IF $V3$ is μIL AND IF $V4$ is μIL	μOL

The defuzzification section uses the weighted average method. This method is most often used because it has efficient computing and faster defuzzification time consumption [24]. Equation (6) shows the weighted average method expression according to the use of Table 1. The predicate value is denoted as w, z_i is the centroid of each MF, and the defuzzification value is denoted as z^*. The defuzzification value is converted into a symbol as covertext.

$$z^* = \frac{\sum_{i=1}^{16} w_i z_i}{\sum_{x=1}^{16} w_x} \tag{6}$$

4. **Experiments and Results.** In this section, the experiments and the results obtained will be presented. The plaintext sample uses short messages of astronomical observations from the Astronomer Telegram Dataset. This experiment uses 14 samples of different sizes. The number of experiments was carried out 25 times for each sample, and all of them were 700 experiments. Experiments were applied to the PDAC, PECT, and proposed models. This experiment measures entropy, and runtime consumption as performance metrics.

Measurement algorithms are an important component of good engineering. Measurement metrics play an important role in achieving good software engineering. Measurements are used to assess the situation, track progress, and evaluate [27]. In cryptography, information entropy is a measure of the randomness of the amount of information in a message. Entropy is expressed in units to express the level of randomness of information [28]. The ideal entropy value is expected to reach 8 as the sum of the optimal entropy value. The main idea behind entropy is the summation of all possible occurrences of a good probability character distribution [29]. If the entropy value is close to 8, it indicates that the encryption system designed is secure, and the information is safe from intruders [17,29,30]. The entropy value $H(m)$ of the encrypted information is calculated by Equation (7) [31-33]. The symbol n represents the overall value of the data, and $P(m_i)$ represents the probability value of the symbol (character) m_i.

$$H(m) = \sum_{i=0}^{2^n-1} P(m_i) \log_2 \frac{1}{P(m_i)} \tag{7}$$

The experimental results of the proposed model and the previous model were compared using a nonparametric Mann-Whitney U-test to see if there was a significant difference. The Mann-Whitney U-test method was used for analytical purposes to compare the differences between the two groups [34,35]. This metric is the popular one of the non-parametric tests of significance difference [34,36]. This metric becomes easier because it is used to evaluate the dependence of two groups without the need to prove the normal distribution [34]. The Mann-Whitney test is carried out using Equations (8), (9) and (10) [37].

The statistical value of the Mann-Whitney U test is denoted as *U-value*. The number of data groups is denoted as n_1 and n_2. R_2 is the number of data rankings from data group in n_2. *U-value* is obtained from the minimum value between U_1 and U_2. The *U-critical value* is obtained from the Mann-Whitney U table based on n_1 and n_2. The significance value is expressed as α. Finally, the *U-value* is compared with the *U-critical value*. If *U-value* $<$ *U-critical value*, it means that there is a significant difference between the compared algorithms results. If instead *U-value* $>$ *U-critical value*, the result is not significant.

$$U_1 = n_1 n_2 + \frac{n_1(n_{1+1})}{2} - \sum R_2 \tag{8}$$

$$U_2 = n_1 n_2 - U_1 \tag{9}$$

$$U_{value} = \min(U_1, U_2) \tag{10}$$

From the experiment, the entropy value of each experiment was obtained. Table 2 presents the average entropy values of the experiments at each sample size. The average entropies of ciphertext processed with PDAC and PECT are 5.88, and 5.90. The achievement value is calculated by comparing the average entropy value to the optimum entropy

TABLE 2. The average entropy of the experimental results

	Sample size	Model		
		PDAC	PECT	Proposed
Average entropy	1KB	5.92	5.89	6.33
	2KB	5.84	5.86	6.26
	3KB	5.70	5.78	6.14
	4KB	5.78	5.85	6.24
	5KB	5.77	5.85	6.24
	6KB	5.88	5.93	6.31
	7KB	5.82	5.90	6.27
	8KB	5.97	5.92	6.38
	9KB	5.93	5.92	6.34
	10KB	5.93	5.94	6.35
	16KB	5.99	5.93	6.39
	32KB	5.92	5.92	6.35
	64KB	5.91	5.92	6.34
	128KB	5.95	5.93	6.37
Average		5.88	5.90	**6.31**
Achievement (%)		73.50	73.71	**78.85**

value. Achievement value is expressed in percent (%). The entropy achievements of PDAC and PECT are 73.50%, and 73.71%. The difference in the average entropy value is caused by differences in the covertext generation process between PDAC and PECT. These results indicate that the PECT entropy value is higher than PDAC. If it is calculated statistically using the Mann-Whitney method, both results are not significant with a significance value (α) of 0.05. The statistical calculations show that the *U-value* is 88, and the *U-critical value* is 55. Therefore, the result is not significant, because *U-value* is 88 greater than *U-critical value* of 55.

The average entropy value of our proposed model is 6.31, with an achievement of 78.85%. If statistically calculated using the Mann-Whitney method, the results show a significant difference with a significance value (α) of 0.05. The calculations show the *U-value* is 0, and the *U-critical value* is 55. The result is significant. Thus, it means that covertext generation design using the fuzzy logic approach produces a safer ciphertext that has higher randomness than the previous method. Furthermore, this method provides better information uncertainty. Therefore, confidential information will be more difficult to guess by intruders.

Speed testing aims to measure the processing speed of the proposed model and determine whether it is included as an acceptable processing time criterion [38]. Based on the measurement of time consumption, Figure 5 shows the average consumption time of the PDAC, PECT, and proposed method models. The consumption time is calculated by adding up the encryption process time and the decryption process time. The average time required to encrypt and decrypt information in the PDAC, PECT, and proposed method models is 15.157 seconds, 15.366 seconds, and 15.674 seconds. The difference of the average time of the PDAC process and the average time of the proposed method is 0.517 seconds. Statistical testing using the calculation of the Mann-Whitney method shows that the time difference is not significant at a significance value (α) of 0.05. The Mann-Whitney method shows the *U-value* is 89.5, and the *U-critical value* is 55. Therefore, the result is not significant.

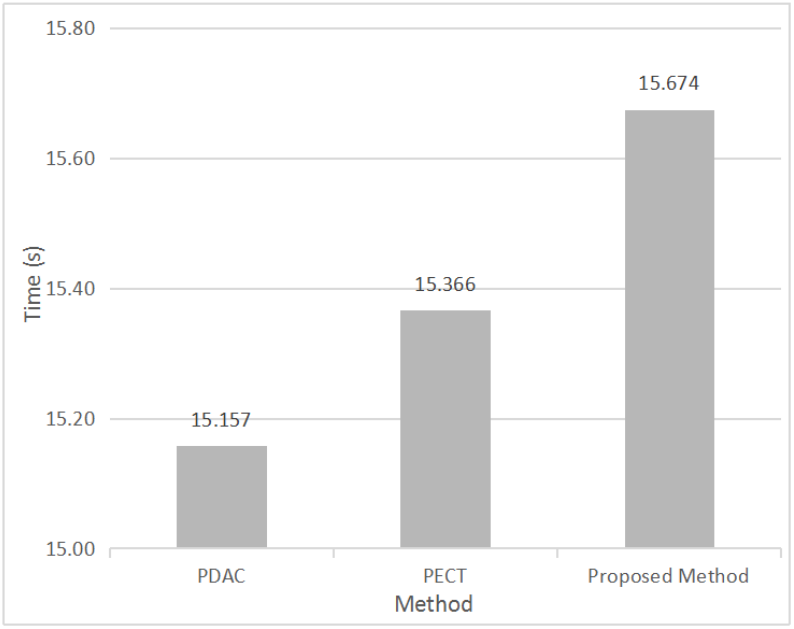

FIGURE 5. The average consumption time

Based on the results of performance measurement, our proposed method quantitatively has a better entropy value, and statistically has a significant value. Thus, our proposed method has a significant impact in improving the confidentiality of information. With higher entropy, the confidentiality of information will be guaranteed. Therefore, keeping confidential information secret using the method we propose will be safer. On the performance of time consumption, our proposed method requires a longer processing time. This longer time is due to the longer number of lines of code, and the calculation process with fractional values. However, the longer consumption time is considered insignificant.

5. **Conclusions.** This section presents the conclusions of the experiment. The fuzzy logic approach adopted in the covertext creation process can increase the robustness of the PDAC encryption model. The average entropy value in our proposed model is 6.31, with the achievement value of 78.85% which is statistically increased significantly from the previous average entropy value of the PDAC model, and the PECT model of 5.88, and 5.90, with achievements of 73.50% and 73.71%, respectively. Thus, our proposed method provides a more even symbol randomness so that the encoded information is more difficult for intruders to decipher. The processing time consumption of the proposed method is 15.674 seconds; this time is longer than the previous method although it is not significant. Thus, the adoption of fuzzy logic can make the PDAC model provide better performance than the previous version.

As a suggestion for further work, further exploration is needed to use different membership function designs with various existing representation models to increase the resilience of PDAC to be stronger.

REFERENCES

[1] K. Y. Chai and M. F. Zolkipli, Review on confidentiality, integrity and availability in information security, *Journal of ICT in Education*, vol.8, no.2, pp.34-42, DOI: 10.37134/jictie.vol8.2.4.2021, 2021.

[2] L.-N. Degambur, S. Armoogum and S. Pudaruth, A study of security impacts and cryptographic techniques in cloud-based e-learning technologies, *International Journal of Advanced Computer Science and Applications*, vol.13, no.1, DOI: 10.14569/IJACSA.2022.0130108, 2022.

[3] A. Shabbir, M. Shabbir, M. Rizwan and F. Ahmad, Ensuring the confidentiality of nuclear information at cloud using modular encryption standard, *Security and Communication Networks*, vol.2019, pp.1-16, DOI: 10.1155/2019/2509898, 2019.

[4] C. Gupta and N. V. S. Reddy, Enhancement of security of Diffie-Hellman key exchange protocol using RSA cryptography, *J. Phys. Conf. Ser.*, vol.2161, no.1, 012014, DOI: 10.1088/1742-6596/2161/1/012014, 2022.

[5] P. Das, N. H. Munshi and S. Maitra, New key-dependent s-box generation algorithm on AES, *Micro and Nanosystems*, vol.14, no.3, pp.263-271, DOI: 10.2174/1876402913666210726163822, 2022.

[6] V. Snasel, P. Kromer, J. Safarik and J. Platos, JPEG steganography with particle swarm optimization accelerated by AVX, *Concurr. Comput.*, vol.32, no.8, pp.1-11, DOI: 10.1002/cpe.5448, 2020.

[7] M. M. Abu-Faraj, K. Aldebei and Z. A. Alqadi, Simple, efficient, highly secure, and multiple purposed method on data cryptography, *Traitement du Signal*, vol.39, no.1, pp.173-178, DOI: 10.18280/ts.390117, 2022.

[8] S. Padhiar and K. H. Mori, A comparative study on symmetric and asymmetric key encryption techniques, in *A Comparative Study on Symmetric and Asymmetric Key Encryption Techniques*, IGI Global, DOI: 10.4018/978-1-7998-6988-7.ch008, 2022.

[9] M. A. Balasubramani and C. S. Rao, Sliced images and encryption techniques in steganography using multi threading for fast retrieval, *International Journal of Applied Engineering Research*, vol.11, no.9, pp.6504-6509, 2016.

[10] A. Hadipour and R. Afifi, Advantages and disadvantages of using cryptography in steganography, *2020 17th International ISC Conference on Information Security and Cryptology (ISCISC)*, pp.88-94, DOI: 10.1109/ISCISC51277.2020.9261921, 2020.

[11] B. Osman, A. Yasin and M. N. Omar, An analysis of alphabet-based techniques in text steganography, *Journal of Telecommunication, Electronic and Computer Engineering*, vol.8, no.10, pp.109-115, 2016.

[12] T. Ahmad and T. P. Fiqar, Enhancing the performance of audio data hiding method by smoothing interpolated samples, *International Journal of Innovative Computing, Information and Control*, vol.14, no.3, pp.767-779, 2018.

[13] S. Kataria, B. Singh, T. Kumar and H. S. Shekhawat, PDAC (parallel encryption with digit arithmetic of cover text) based text steganography, *Proc. of Int. Conf. on Advances in Computer Science (AETACS)*, 2013.

[14] S. Kataria, K. Singh, T. Kumar and M. S. Nehra, ECR (encryption with cover text and reordering) based text steganography, *IEEE 2nd International Conference on Image Information Processing (ICIIP-2013)*, 2013.

[15] E. Ardhianto, W. Budiharto, Y. Heryadi and L. A. Wulandhari, A comparative experiment of document security level on parallel encryption with digit arithmetic of covertext and parallel encryption using covertext, *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, pp.163-167, DOI: 10.1109/SCOReD53546.2021.9652746, 2021.

[16] M. K. Onwughalu, Enhancement of data security on transmission network using fuzzy logic, *International Journal of Scientific and Research Publications*, vol.6, no.6, 279, 2016.

[17] K. Chanda, Password security: An analysis of password strengths and vulnerabilities, *International Journal of Computer Network and Information Security*, vol.8, no.7, pp.23-30, DOI: 10.5815/ijcnis.2016.07.04, 2016.

[18] A. Pasumpon Pandian, Development of secure cloud based storage using the elgamal hyper elliptic curve cryptography with fuzzy logic based integer selection, *Journal of Soft Computing Paradigm*, vol.2, no.1, pp.24-35, DOI: 10.36548/jscp.2020.1.003, 2020.

[19] A. Bhowmik and S. Karforma, A key generation technique using concept of recurrence relation and fuzzy logic against security breach in wireless communication, *Easy Chair*, pp.1-19, 2020.

[20] S. B. Sadkhan and A. O. Salman, Fuzzy logic for performance analysis of AES and lightweight AES, *2018 International Conference on Advanced Science and Engineering (ICOASE)*, pp.318-323, DOI: 10.1109/ICOASE.2018.8548832, 2018.

[21] M. Gaur and M. Sharma, A new PDAC (parallel encryption with digit arithmetic of cover text) based text steganography approach for cloud data security, *International Journal on Recent and Innovation Trends in Computing and Communication*, vol.3, no.3, pp.1344-1352, 2015.

[22] S. Panwar, M. Kumar and S. Sharma, Text steganography based on parallel encryption using cover text (PECT), in *The 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019. ICIoTCT 2019. Advances in Intelligent Systems and Computing*, N. Nain and S. Vipparthi (eds.), Cham, Springer, DOI: 10.1007/978-3-030-39875-0_32, 2020.

[23] B. Pérez, E. Stafford, J. L. Bosque and R. Beivide, Sigmoid: An auto-tuned load balancing algorithm for heterogeneous systems, *J. Parallel. Distrib. Comput.*, vol.157, pp.30-42, DOI: 10.1016/j.jpdc.2021.06.003, 2021.
[24] T. J. Ross, *Fuzzy Logic with Engineering Applications*, John Wiley, 2010.
[25] Y. Liu and X. Zhang, Evaluating the undergraduate course based on a fuzzy AHP-FIS model, *International Journal of Modern Education and Computer Science*, vol.12, no.6, pp.55-66, DOI: 10.5815/ijmecs.2020.06.05, 2020.
[26] S. J. Habib and P. N. Marimuthu, A fuzzy framework for self-aware wireless sensor networks, *Journal of Engineering Research*, pp.1-16, DOI: 10.36909/jer.18535, 2022.
[27] E. F. Norman and P. S. Lawrence, *Software Metrics: A Rigorous and Practical Approach*, Revised, 3rd Edition, PWS Publishing Company, Boston, 1997.
[28] R. Shukla, H. O. Prakash, R. P. Bhushan, S. Venkataraman and G. Varadan, Unconditionally secure and authenticated one time pad cryptosystem, *2013 International Conference on Machine Intelligence and Research Advancement*, pp.174-178, DOI: 10.1109/ICMIRA.2013.40, 2013.
[29] A. Gutub and B. O. Al-Roithy, Varying PRNG to improve image cryptography implementation, *Journal of Engineering Research (Kuwait)*, vol.9, no.3, pp.153-183, DOI: 10.36909/jer.v9i3A.10111, 2021.
[30] S. Tariq, M. Khan, A. Alghafis and M. Amin, A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation, *Multimed. Tools Appl.*, vol.79, nos.31-32, pp.23507-23529, DOI: 10.1007/s11042-020-09134-8, 2020.
[31] E. Vidhya, S. Sivabalan and R. Rathipriya, Hybrid key generation for RSA and ECC, *2019 International Conference on Communication and Electronics Systems (ICCES)*, pp.35-40, DOI: 10.1109/ICCES45898.2019.9002197, 2019.
[32] A. Gutub and B. O. Al-Roithy, Varying PRNG to improve image cryptography implementation, *Journal of Engineering Research*, vol.9, no.3A, pp.153-183, DOI: 10.36909/jer.v9i3A.10111, 2021.
[33] A. Shukla and S. Kumar, Analysis of secure watermarking based on DWT-SVD technique for piracy, *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp.1110-1115, DOI: 10.1109/CCAA.2016.7813882, 2016.
[34] M. Riņģis and S. Bēziša, Efficiency measurement of project management software usage at state social insurance agency, *Information Technology and Management Science*, vol.19, no.1, DOI: 10.1515/itms-2016-0013, 2016.
[35] R. Bergmann, J. Ludbrook and W. P. J. M. Spooren, Different outcomes of the Wilcoxon-Mann-Whitney test from different statistics packages, *Am. Stat.*, vol.54, no.1, pp.72-77, DOI: 10.1080/00031305.2000.10474513, 2000.
[36] S. Tang, Y. Jiang, L. Zhang and Z. Zhou, Audio steganography with AES for real-time covert voice over Internet protocol communications, *Science China Information Sciences*, vol.57, no.3, pp.1-14, DOI: 10.1007/s11432-014-5063-2, 2014.
[37] H. B. Mann and D. R. Whitney, On a test of whether one of two random variables is stochastically larger than the other, *The Annals of Mathematical Statistics*, vol.18, no.1, pp.50-60, DOI: 10.1214/aoms/1177730491, 1947.
[38] E. H. Riyadi, T. K. Priyambodo and A. E. Putra, The dynamic symmetric four-key-generators system for securing data transmission in the industrial control system, *International Journal of Intelligent Engineering and Systems*, vol.14, no.1, pp.376-386, DOI: 10.22266/IJIES2021.0228.35, 2021.

Author Biography

Eka Ardhianto is a doctoral candidate at BINUS Graduate Program – Doctor of Computer Science, Bina Nusantara University, Jakarta, Indonesia. He obtained a Bachelor degree, Informatics Engineering Program, Universitas Stikubank (UNISBANK) Semarang, Indonesia in 2006. He obtained a Master degree in Computer Science from Gadjah Mada University, Yogyakarta, Indonesia in 2012. He is an assistant professor at Stikubank University (UNISBANK) Semarang. His research interest is in the field of information hiding, focusing on cryptographic techniques.

Yaya Heryadi is a faculty member and researcher in BINUS Graduate Program – Doctor of Computer Science, Bina Nusantara University, Jakarta, Indonesia. He obtained a Bachelor degree in Statistics and Computation from Bogor Agricultural University, Bogor; Master of Science in Computer Science from Indiana University at Bloomington, Bloomington, Indiana, USA; and Doctorate degree in Computer Science from University of Indonesia. His research interests include computer vision, natural language processing, interpretable artificial intelligence, and graph machine learning.

Lili Ayu Wulandhari is a faculty member in Bina Nusantara University, Jakarta, Indonesia and a former data scientist in an OTA industry in Indonesia. She obtained a Bachelor degree in Mathematics from University of Sumatera Utara, Medan, Master of Science and Doctorate degree in Computer Science from University of Technology Malaysia. Her research interests are computer vision, natural language processing and fraud detection using machine learning approach.

Widodo Budiharto received the Bachelor degree in Physics from Indonesia University, Jakarta, Indonesia, the Master degree in Information Technology from STT Benarif, Jakarta, Indonesia, and the Ph.D. degree in Electrical Engineering from the Institute of Technology Sepuluh Nopember, Surabaya, Indonesia. He took the Ph.D. Sandwich Program in Robotics with Kumamoto University, Japan, and conducted Postdoctoral Researcher work in Robotics and Artificial Intelligence with Hosei University, Japan. He worked as a visiting professor with the Erasmus Mundus French Indonesian Consortium (FICEM), France, Hosei University, Japan, and the Erasmus Mundus Scholar with the EU Universite de Bourgogne, France, in 2017, in 2016, in 2007, respectively. He is currently a professor of Artificial Intelligence with the School of Computer Science, Bina Nusantara University, Jakarta, Indonesia. His research interests include intelligence systems, data science, robot vision, and computational intelligence.