ICIC Express Letters
Volume **17**, Number **7**, July **2023**

 ISSN 1881-803X
pp. **817–824**

PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVERTEXT ENCRYPTION MODEL USING COVERTEXT GENERATOR WITH FUZZY LOGIC APPROACH

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
yayaheryadi@binus.edu
*Corresponding author: eka.ardhianto@binus.ac.id

[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 July 2022; accepted October 2022

Abstract. *Confidentiality is an important aspect of an information security system. The reliability of cryptographic methods is assessed from the ability to secure information. The more reliable the method, the more secure the information. This article discusses the Parallel Encryption with Digit Arithmetic of Covertext (PDAC) method which adopts fuzzy logic in its covertext generator. The purpose of this method modification is to increase the resilience of the encryption model so that confidential information becomes difficult for cryptanalysts to crack. The results obtained are that this proposed modification has the same covertext capacity, slightly different processing time consumption, and an increase in entropy of more than 80% compared to the previous PDAC method so that the information encoded by the current PDAC becomes stronger against the intruder.*
Keywords: Covertext, PDAC, Fuzzy logic, Encryption, Information security

1. **Introduction.** Confidentiality is an achievement in the information security system. Confidentiality can be achieved by increasing the level of information security. Two well-known information security techniques are cryptography and steganography. Cryptography refers to the art of secret writing which concentrates on maintaining confidentiality through hiding information by scrambling messages but leaving it visible [1,2]. Steganography focuses on how to hide the existence of confidential information into the cover object [2]. The difference between them lies in the techniques used. Steganography works differently from cryptography by hiding confidential information inside the cover of file formats such as images, videos, audio, and text [3] while cryptography makes information difficult to read by scrambling it.

Increasing the level of security can be performed by combining cryptography and steganography. Steganography can be used in conjunction with cryptography by hiding encrypted messages into covertext. This adoption technique has been used in several studies. They show good results when encrypting hidden messages before the hiding process [4]. Combine steganography and encryption properties to make it harder for steganalysis to get back plain text from secret messages [5]. Combining these systems makes for a more reliable and robust system.

DOI: 10.24507/icicel.17.07.817

Parallel Encryption with Digit Arithmetic of Covertext (PDAC) is an encryption model that adopts a combination of text-based steganography with cryptographic techniques [6]. In securing information, the existence of the key becomes something important. PDAC has two important factors that are covertexts and encryption keys [7]. A PDAC covertext is a character used as a cover in a steganography context [8]. Covertext in PDAC is selected using random functions based on plaintext characters. Covertext is required in the key generation process. The number of covertext requirements in the plaintext is $n/4$, with n as the number of plaintext characters [6]. While encryption keys are used for encryption operations. The PDAC encryption process is divided into four sub-processes: covertext generator, encryption key generator, encryption, and finalization. Figure 1 shows the PDAC model encryption process.

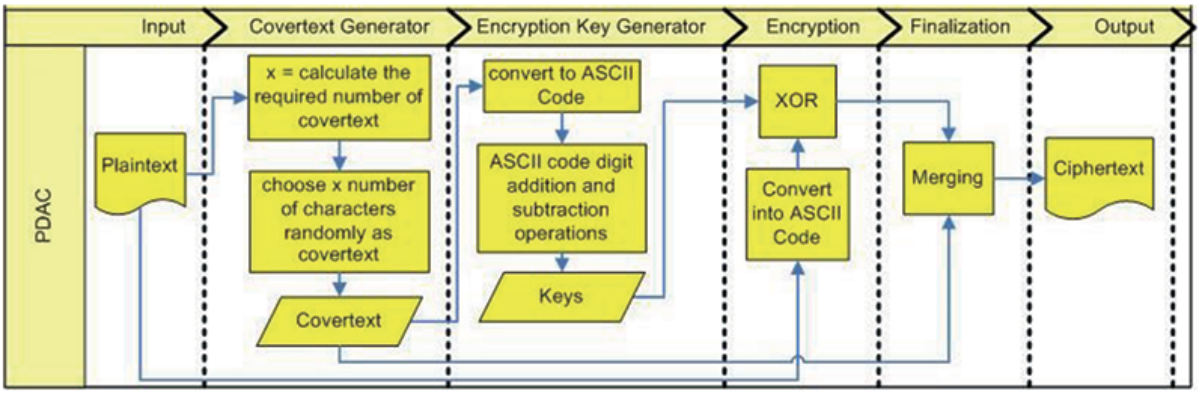

FIGURE 1. The encoding process of the PDAC model [6]

Keys in information security are considered the heart of the algorithm, so generating keys is considered difficult, ambiguous, and confusing [9]. Thus, generating covertext on the PDAC model is also considered difficult. The selection of PDAC covertext is currently done by utilizing random functions. Although it looks random, the random value generated from a Pseudorandom Number Generator (PRNG) does not completely produce a random number because it uses an initial value to proceed [10]. The process of randomly selecting covertext is seen as a weakness of PDAC; this is because the covertext is taken from the symbol contained in the plaintext.

An important aspect of cryptography is confidentiality. The evolution of PDAC to date has focused on aspects of capacity and authenticity. This paper focuses on the confidentiality aspect by improving the resilience of information by adopting fuzzy logic in the PDAC covertext generator. Entropy, capacity, and processing time are used as evaluation metrics. With the same capacity and a slight difference in time consumption with PDAC, the use of fuzzy logic adoption in the PDAC covertext generator provides additional algorithm resistance with an increase in entropy of up to 80% of the optimum value compared to the previous version.

This article is divided into several sections as follows. Section 1 discusses the background of the problem. Section 2 describes the development of PDAC in the literature review. Section 3 describes the proposed method. Section 4 discusses the experimental results and conclusions are given in Section 5.

2. **Literature Review.** Several studies related to PDAC have modified PDAC and explored the confidentiality aspect. The evolution of PDAC to date has focused on the aspects of capacity and authenticity, and exploration is carried out to find important aspects of PDAC confidentiality. PDAC begins with the Encryption with Covertext and Reordering model (ECR) [8]. ECR is a text based steganographic approach that works on a simple encryption technique using the XOR operation of two characters and rearranging

them to be more secure and difficult to read. ECR is improved by a simpler process as PDAC [6]. PDAC changes the key generation and merging process in ECR. Gaur and Sharma increased the PDAC's covertext capacity [11]. This model is known as New PDAC. This study focuses on reducing the size of the large output file (ciphertext) which hinders the transmission of information. This study resulted bigger covertext capacity of $n/6$. This means that one covertext will process 6 plaintext characters. The achievement obtained is an increase in the capacity of the covertext which is affected in a reduction in the size of the output file. Panwar et al. [12] developed PDAC into Parallel Encryption with Covertext (PECT). This study focuses on the authentication aspect of information secured. The method used is to create covertext based on consonants and vowels from the input file character sequence (plaintext), and converted to 1 and 0, representing binary numbers then converted to decimal. Covertext obtained will eventually be used in the authentication process. The achievement obtained in this research is the guarantee of the accuracy of the information. Although PDAC has been developed, the confidentiality aspect offered has not been deep explored about the information confidentiality strength.

The exploration of the PDAC and PECT models was conducted by Ardhianto et al. [7]. This experiment aims to obtain the important part that affects information security. The two models were compared by measuring the level of confidentiality. This experiment found that there is difference technique in the covertext generator. PDAC adopts a random function in generating covertext, while PECT produces covertext based on the vowel and consonant alphabets. The results obtained are that the covertext generator process becomes an important part in increasing information confidentiality. This study suggests new design in the covertext generator to strengthen the PDAC from intruders.

3. **Proposed Method.** This proposed method adopts fuzzy logic on the covertext of the PDAC generator. Samples were taken from the Astronomer Telegram Dataset as plaintext. Plaintext characters are divided into 4 characters group in ASCII code format. These 4 characters correspond to $n/4$, covertext capacity. Each group of 4 characters is used as an input on the covertext generator and produces an output as covertext character. Covertext is obtained as input for encryption key generator. The encryption process performs the XOR process between the plaintext and the keys to produce encrypted text. The merging process is producing the final ciphertext by combining the encrypted text and covertext. The whole process is shown in Figure 2.

The symbols $c1$, $c2$, $c3$, and $c4$ in the covertext generator represent every 4 plaintext characters. The fuzzy logic method used is Tsukamoto. The Tsukamoto method is flexible

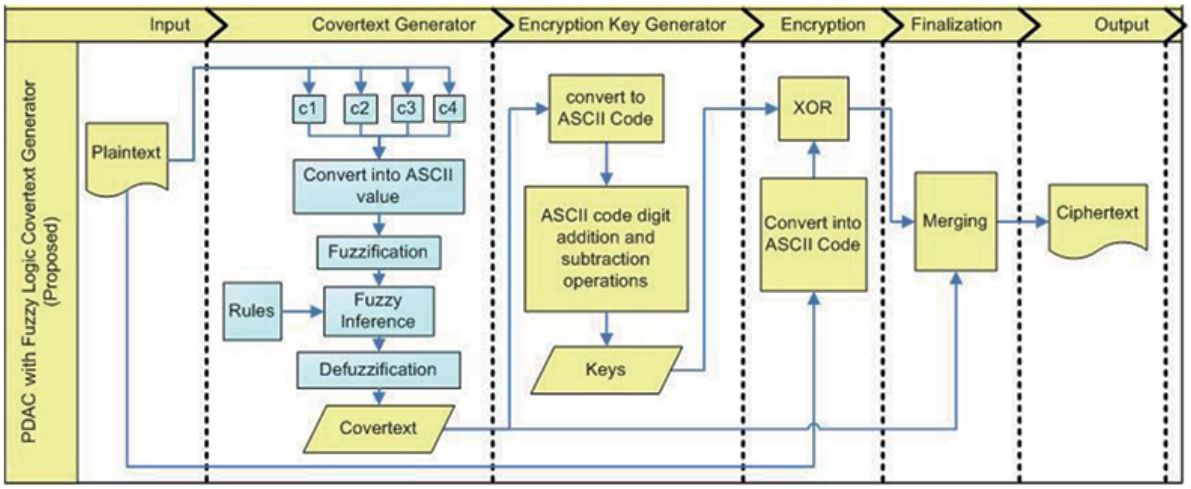

FIGURE 2. Proposed adoption of fuzzy logic on PDAC covertext generator

to apply and has good time complexity [13]. At this stage, the ASCII values of each character assigned to the input Membership Function (MF) are represented by the terms: High (μIT) and Low (μIR). There are 5 models of MF representation such as linear line, triangle, trapezoid, Gaussian, and sigmoid [14,15]. In this paper the proposed method uses a linear MF representation; it is chosen because each term value is given in the form of a clear interval with values at the end, values 0 and 1 for μIR and μIT. The input MF is shown in Equations (1) and (2).

$$\mu IT\,[x; c1, c2, c3, c4] = \begin{cases} 0, & x \leq 0 \\ 1, & x \geq 255 \\ \dfrac{x}{255}, & 0 < x < 255 \end{cases} \tag{1}$$

$$\mu IR\,[x; c1, c2, c3, c4] = \begin{cases} 0, & x \geq 255 \\ 1, & x \leq 0 \\ \dfrac{255 - x}{255}, & 0 < x < 255 \end{cases} \tag{2}$$

In the inference engine, the resulting MF assigned to each character is combined according to a specific rule. Thus, the new MF is explained by giving the linguistic terms: High (μOT) and Low (μOR). Equations (3) and (4) indicate the output MF concerning the term linguistic. Fuzzy rules are given in Table 1, and there are sixteen fuzzy rules listed to describe all possible combinations of input and output. AND logic is used to create rules table.

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

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

TABLE 1. Fuzzy rules table

Rule	**Antecedents**	**Consequent**
1	IF $c1$ is μIT AND IF $c2$ is μIT AND IF $c3$ is μIT AND IF $c4$ is μIT	μOT
2	IF $c1$ is μIT AND IF $c2$ is μIT AND IF $c3$ is μIT AND IF $c4$ is μIR	μOT
3	IF $c1$ is μIT AND IF $c2$ is μIT AND IF $c3$ is μIR AND IF $c4$ is μIT	μOT
4	IF $c1$ is μIT AND IF $c2$ is μIT AND IF $c3$ is μIR AND IF $c4$ is μIR	μOT
5	IF $c1$ is μIT AND IF $c2$ is μIR AND IF $c3$ is μIT AND IF $c4$ is μIT	μOT
6	IF $c1$ is μIT AND IF $c2$ is μIR AND IF $c3$ is μIT AND IF $c4$ is μIR	μOT
7	IF $c1$ is μIT AND IF $c2$ is μIR AND IF $c3$ is μIR AND IF $c4$ is μIT	μOT
8	IF $c1$ is μIT AND IF $c2$ is μIR AND IF $c3$ is μIR AND IF $c4$ is μIR	μOT
9	IF $c1$ is μIR AND IF $c2$ is μIT AND IF $c3$ is μIT AND IF $c4$ is μIT	μOT
10	IF $c1$ is μIR AND IF $c2$ is μIT AND IF $c3$ is μIT AND IF $c4$ is μIR	μOT
11	IF $c1$ is μIR AND IF $c2$ is μIT AND IF $c3$ is μIR AND IF $c4$ is μIT	μOT
12	IF $c1$ is μIR AND IF $c2$ is μIT AND IF $c3$ is μIR AND IF $c4$ is μIR	μOT
13	IF $c1$ is μIR AND IF $c2$ is μIR AND IF $c3$ is μIT AND IF $c4$ is μIT	μOT
14	IF $c1$ is μIR AND IF $c2$ is μIR AND IF $c3$ is μIT AND IF $c4$ is μIR	μOT
15	IF $c1$ is μIR AND IF $c2$ is μIR AND IF $c3$ is μIR AND IF $c4$ is μIT	μOT
16	IF $c1$ is μIR AND IF $c2$ is μIR AND IF $c3$ is μIR AND IF $c4$ is μIR	μOR

4. **Experiments and Results.** The plaintext sample was taken from the Astronomer Telegram Dataset which contains a short report of astronomical observations in text format. The sample used is 14 with different sizes. Experiments were carried out 700 trials on all samples. Experiments were performed on the proposed model, PECT, and PDAC. The entropy, time, and covertext capacity of each trial are calculated and compared as performance metrics.

Entropy is a measure of randomness in information. It measures uncertainty in information [10]. Information entropy is defined as a measure of the randomness of the amount of information in a message [16,17]. Entropy reflects the performance of cryptographic algorithms [18]. The higher the entropy, the more uncertainty and the smaller the chance of guessing [10]. Under random conditions, the encrypted text must have an entropy value close to 8 (optimal entropy value). If the entropy value is close to 8, it indicates that an encryption system designed is secured and the information is to be secure from intruders [10,16,17,19]. The entropy value $H(m)$ of encrypted information is calculated by Equation (5) [20].

$$H(m) = \sum_{i=0}^{2^n-1} P(m_i) \log_2 \frac{1}{P(m_i)} \tag{5}$$

n indicates the overall value of the data, and $P(m_i)$ indicates the probability value of the symbol (character) m_i. With Equation (5) the entropy value is calculated in each experiment, and then the average value is calculated. Table 2 shows the results obtained. The results show that the entropy value in the PDAC method with fuzzy covertext logic is higher than the entropy value in the PDAC and PECT methods. The average entropy value in PDAC with fuzzy logic covertext is 6.409. Meanwhile, the average value of the previous version, PDAC and PECT entropy is 5.880 and 5.897. The achievement value is calculated by comparing the average value of each method with the optimum entropy value, and the results are expressed in percent (%). The proposed method has a higher achievement of 80.11% than the previous method: 73.50% and 73.71%. This means that PDAC with fuzzy logic covertext produces a safer ciphertext that has higher randomness than the previous method. Furthermore, the performance of this method is better by

Table 2. Average entropy value of experimental results

	File size	PDAC	PECT	PDAC with fuzzy logic covertext (proposed)
Average entropy	1KB	5.91638	5.89006	6.42395
	2KB	5.83901	5.86067	6.36634
	3KB	5.70130	5.78797	6.24796
	4KB	5.78091	5.85201	6.34059
	5KB	5.76723	5.85151	6.33711
	6KB	5.87811	5.92523	6.40000
	7KB	5.81984	5.89736	6.35734
	8KB	5.97156	5.92365	6.47485
	9KB	5.92799	5.92030	6.45593
	10KB	5.93264	5.94016	6.45395
	16KB	5.99440	5.93269	6.49274
	32KB	5.91797	5.92130	6.44952
	64KB	5.91482	5.92348	6.44769
	128KB	5.95272	5.93429	6.47214
Average		5.87963	5.89719	6.40858
Achievement (%)		73.50	73.71	80.11

generating more uncertainty. So, there is less possibility for the cryptanalyst to guess the contents of the original information.

The capacity testing aims to see the ability of the covertext capacity between the previous method and the proposed method. The PDAC covertext capacity is $n/4$, which means that the ability of 1 covertext character can be used to process a maximum of 4 plaintext characters. It means that the size of the covertext is 25% of the size of the plaintext. Figure 3 shows a comparison of the covertext and plaintext for each experimental sample. The speed testing aims to measure the processing speed of the proposed model and determine whether it still meets the real-time processing criteria [16]. The time measured is the encryption and decryption process time. The result is that the larger the processed file the longer it will take, but this amount of time consumption still qualifies as real time. The average processing time of the proposed method is 15.206 seconds while the previous version of PDAC is 15.157 seconds.

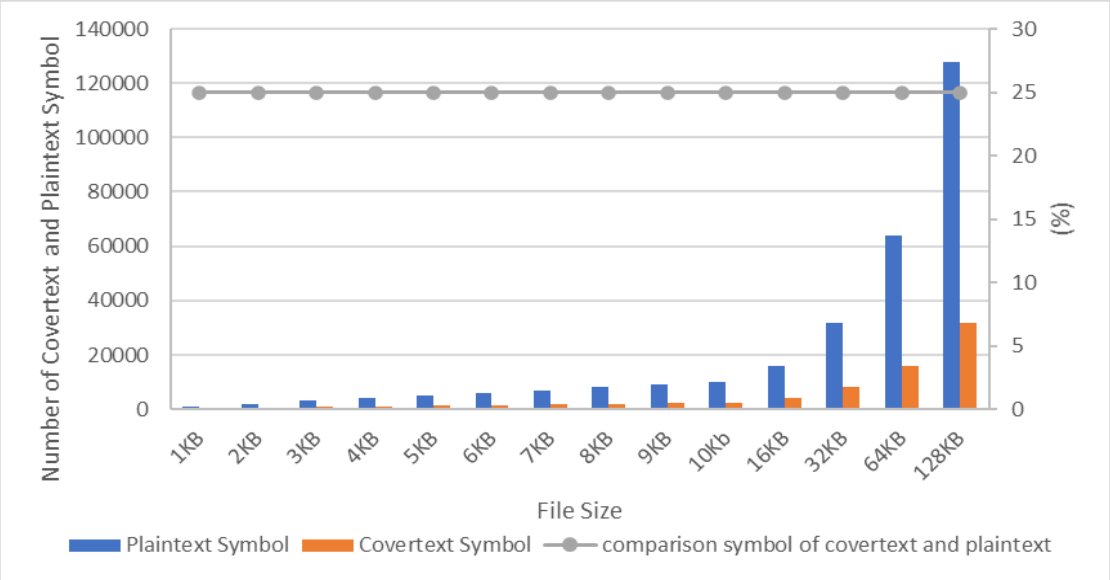

FIGURE 3. Covertext capacity comparison

To see the significance of the difference between the PDAC method and the proposed method, a paired t-test was performed on the results of the PDAC method with the results of the proposed PDAC method. Table 3 shows the significance value (2-tailed) is 0.000. The significance value is lower than the significant level (0.01). So the results of PDAC and PDAC with Fuzzy Logic Covertext (proposed) have significant differences (meaningful).

TABLE 3. T-test paired

N	Correlation	Sig.	Paired differences					t	df	Sig. (2-tailed)
						99% confidence interval of the difference				
			Mean	Std. deviation	Std. error mean	Lower	Upper			
14	0.987	0.000	−0.52894391	0.020160562	0.005388137	−0.54517447	−0.51271336	−98.168	13	0.000

5. **Conclusions.** The security of the information encoded by the encryption model against intruders is important in the aspect of confidentiality. In this article, the new PDAC model has achieved an increase in the entropy value of up to 6.40858 (80.11%) better than the previous version, so that the randomness of symbols is more evenly distributed

so that the encoded information will be more difficult for intruders to decipher. This proposed model has the same covertext capacity value as the previous version model. Thus, the resulting file size is also the same as the previous PDAC model. In terms of processing speed, this model takes a little longer, but the difference is insignificant and still acceptable. As further research, it is necessary to modify the PDAC key generation part to increase the robustness of this model.

REFERENCES

[1] 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.

[2] 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.

[3] D. Shehzad and T. Dag, LSB image steganography based on blocks matrix determinant method, *KSII Transactions on Internet and Information Systems*, vol.13, no.7, DOI: 10.3837/tiis.2019.07.024, 2019.

[4] 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.

[5] 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.

[6] 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)*, pp.175-182, 2013.

[7] 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, DOI: 10.1109/SCOReD53546.2021.9652746, 2021.

[8] 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)*, pp.612-616, 2013.

[9] M. K. Onwughalu and C. M. Ogwata, Enhancement of data security on transmission network using fuzzy logic, *International Journal of Scientific and Research Publications*, vol.6, no.6, pp.279-281, 2016.

[10] 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.

[11] 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.

[12] S. Panwar, M. Kumar and S. Sharma, Text steganography based on Parallel Encryption using Cover Text (PECT), *The 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, pp.303-313, DOI: 10.1007/978-3-030-39875-0_32, 2020.

[13] A. Borany and S. B. Sadkhan, Decision-making approach in cognitive radio using Tsukamoto and Mamdani FIS, *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, pp.144-148, DOI: 10.1109/BICITS51482.2021.9509910, 2021.

[14] Math Work, *Fuzzy Logic Toolbox MATLAB R2017a*, R2017a ed. Math Work, www.mathworks.com, 2017.

[15] M. Hudec, *Fuzziness in Information Systems: How to Deal with Crisp and Fuzzy Data in Selection, Classification, and Summarization*, Springer International Publishing, DOI: 10.1007/978-3-319-42518-4, 2016.

[16] 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.

[17] E. H. Riyadi, A. E. Putra and T. K. Priyambodo, Improvement of nuclear facilities DNP3 protocol data transmission security using super encryption BRC4 in SCADA systems, *PeerJ. Comput. Sci.*, vol.7, pp.1-28, DOI: 10.7717/peerj-cs.727, 2021.

[18] P. Patil, P. Narayankar, D. G. Narayan and S. M. Meena, A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish, *Procedia Comput. Sci.*, vol.78, pp.617-624, DOI: 10.1016/j.procs.2016.02.108, 2016.

[19] 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.

[20] 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.