Q4_A LIGHT WEIGHT OF PARALLEL ENCRYPTION

by Wt Handoko

Submission date: 26-Jan-2024 09:59AM (UTC+0700)
Submission ID: 2206703412
File name: Tambah_Jurnal_1_Q4_A_LIGHT_WEIGHT_OF_PARALLEL_ENCRYPTION.pdf (1.27M)
Word count: 5494
Character count: 28846

Journal of Theoretical and Applied Information Technology

31st December 2023. Vol.101. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A LIGHT WEIGHT OF PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVERTEXT ENCRYPTION MODEL

WIDIYANTO TRI HANDOKO[1] , EKA ARDHIANTO[2,*] , HARI MURTI[3] , RARA SRIARTATI REDJEKI[4]

[1234] Faculty of Information Technology and Industry, Universitas Stikubank, Semarang, Indonesia

[*]Corresponding Author

E-mail: [1]wthandoko@edu.unisbank.ac.id, [2]ekaardhianto@edu.unisbank.ac.id, [3]harimurti@edu.unisbank.ac.id, [4]rara_artati@edu.unisbank.ac.id

ABSTRACT

The speed of sending documents over the internet network is influenced by the file size. Confidential documents require fast processing, reducing the risk of hacking while on the network. So, secret documents must have a light ciphertext size. The Parallel Encryption with Digit Arithmetic of Covertext (PDAC) encryption model produces covertext with an average size of 124.88% larger than plaintext. Thus, the process in the network will take longer, and give intruders a lot of time to translate it. This research aims to design a proposed new PDAC method to produce lighter ciphertext. This research was conducted using experimental methods. Proposed PDAC model that has a different covertext generator and encryption key generator design. The results obtained are a plaintext and ciphertext ratio of 100%. This means that the size of the ciphertext is the same as the size of the plaintext. Thus, the proposed new PDAC method can reduce the size of the ciphertext, thereby speeding up the transfer process over the network, saving storage space, and making it difficult for intruders to retrieve.

Keywords: *Encryption, PDAC, Ciphertext, Cryptography.*

1. INTRODUCTION

One aspect of capacity in the field of information security is file size. The size of the file sent over the network is one of the factors that influences the speed of data transmission. Confidential documents such as blueprints, warrants, financial transaction reports, meeting notes, copyrights, and company financial budgets can be classified as important assets for a person or company. Sending confidential documents must pay attention to aspects of security and speed. The expected result is a lower ratio (R) value. Thus, the size of the ciphertext will be close to plaintext, which will result in lower memory usage and storage space. Large documents will require longer processing and delivery times compared to smaller documents. The faster the document is received by the recipient, the smaller the opportunity for intruders to steal the document in transit. Apart from that, large documents require more memory allocation. Securing confidential documents requires special techniques known as cryptography and steganography.

Cryptography refers to the practice of making information unreadable to unauthorized parties while the information is over network or in storage [1]. The main process of cryptography is to hide information and manage secrets by encrypting plaintext messages into messages that are difficult to understand [2]. Cryptographic techniques also refer to methods of secure information and communication using mathematical principles and a rule-based calculation system or an algorithm [3]. Cryptography also interpreted to secures data by changing data into another form that has no meaning [4]. Techniques in cryptography are known as encryption and decryption. Encryption is a mechanism to make messages difficult to read, and Decryption is the opposite [5]. The purpose of cryptography is to make messages unintelligible, even though the human visual system can see the message, the message seems meaningless.

Steganography techniques come with different mechanisms from cryptography. Steganography aims to hide secret information in a container called

"cover", where the secret is hidden from human sight and can be returned if necessary [6]. Steganography known as the art of hiding information in cover media so that the existence of the information is unknown [7]. The advantage of steganography is that unauthorized people are not aware of the existence of a message inside the cover [8]. The steganography mechanism can provide strength in hiding data through a cover object.

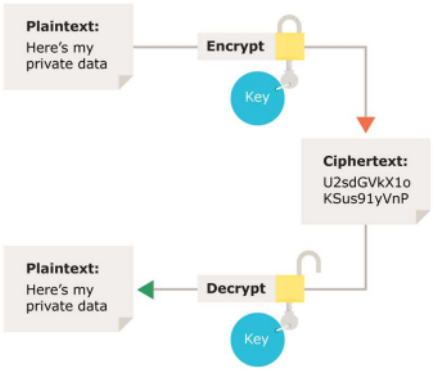

Figure 1: The Cryptography process.

The cryptographic aspect focuses on issues of privacy, authenticity, integrity, and non-repudiation. The privacy aspect is known as the confidentiality aspect which focuses on the issue of how secure the confidential information is [9], [10]. The authenticity aspect focuses on the authenticity of the information, which has not been changed by any party. The integrity aspect ensures that confidential information remains intact and is not divided into several parts [11]–[13]. The non-repudiation aspect focuses on that there is no doubt that the sender and recipient carried out a communication transaction. The field of steganography generally focuses on aspects of privacy and capacity. The privacy aspect ensures that the hidden information is safe. Meanwhile, the capacity problem focuses on the amount of information that can be stored in one media cover [14]–[16].

Cryptography and steganography have the same goal in securing confidential information in terms of privacy but use different techniques. Information will be safer if cryptography and steganography are used in one encryption model. The combination of cryptography and steganography provides double security benefits for information sent via the internet [17], [18]. Performance aspects of privacy and authenticity of confidential information can also be improved using a combination of steganography and cryptography [19]–[21].

Parallel Encryption with Digit Arithmetic of Covertext (PDAC) is a cipher model that combines steganography techniques in cryptography [22]. The PDAC encryption process is divided into several phases. The PDAC phases are known as Covertext Generator, Encryption Key Generator, Encryption, and Finalization [23]. Figure 2 shows the PDAC encryption process. Plaintext is used as the input of PDAC encryption process, and the output known as ciphertext. The first phase is Covertext Generator. Covertext Generator is the process of publishing

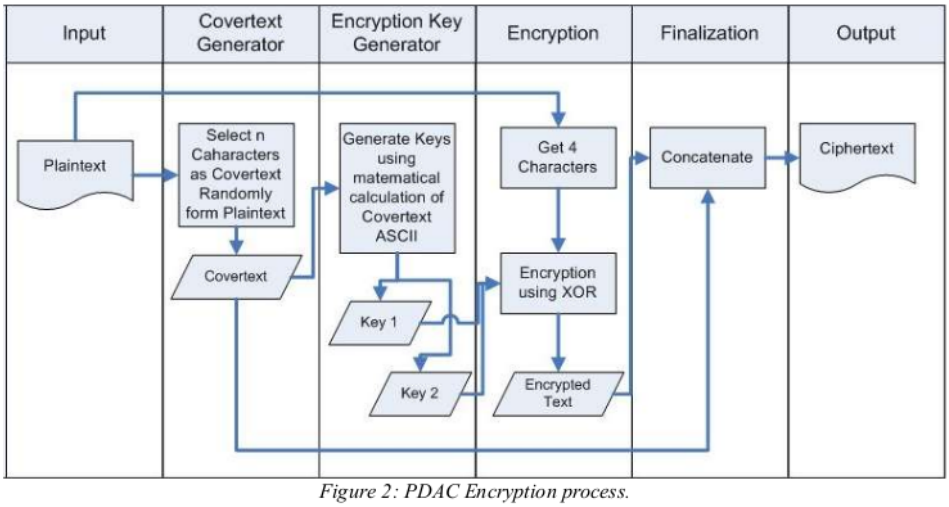

Figure 2: PDAC Encryption process.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

covertext using a random function. PDAC covertext is a character used as a generator and medium for hiding encryption keys [22]. Covertext is used as input in the encryption key generation phase. Covertext in PDAC is selected using a random function based on plaintext characters. The covertext required is 25% of the number of plaintext characters.

The Encryption Key Generation phase is conducted in Encryption Key Generator process. This phase is creating encryption keys based on the selected covertext [23]. PDAC encryption keys are processed using covertext ASCII digit addition and subtraction operations. Thus, one PDAC covertext produces 2 encryption keys. The PDAC encryption key can process a maximum of 4 plaintext characters. Thus, 1 PDAC covertext can be used to process 4 characters.

The encryption phase is performed using the XOR logic process [22]. The XOR operation is used because it is computationally light. Therefore, the XOR cipher was chosen to perform fast computing [24], [25]. The output of the encryption phase is called encryptedtext. The finalization phase works to produce the ciphertext. Ciphertext is produced by combining covertext with encryptedtext.

The problem is that the PDAC ciphertext has a size that is larger than the ciphertext file. This large ciphertext file size results in the need for a longer information transmission processing time and more memory space. A lighter ciphertext file size will minimize the transmission time of confidential information and minimize the risk of information being hacked during the transmission process.

Table 1 : R-Value of PDAC Preliminary Research.

Plaintext Size (KB)	Ciphertext Size (KB)	R (%)
1	1.25	125
2	2.5	125
3	3.75	125
4	5	125
5	6.235	124.7
6	7.475	124.58
7	8.73	124.7
8	10	125
9	11.23	124.8
10	12.475	124.75
16	19.988	124.925
32	39.98	124.94
64	79.96	124.94
128	159.909	124.93
Average of R (%)		124.88

As preliminary research, encryption experiments were performed using several different sizes of plaintext files. The performance metric used in preliminary research is the ratio value (R) using equation (1). Table 1 shows the results of the preliminary research.

$$R = \left(\frac{ciphertext\ size}{plaintext\ size}\right) \text{x } 100\% \qquad (1)$$

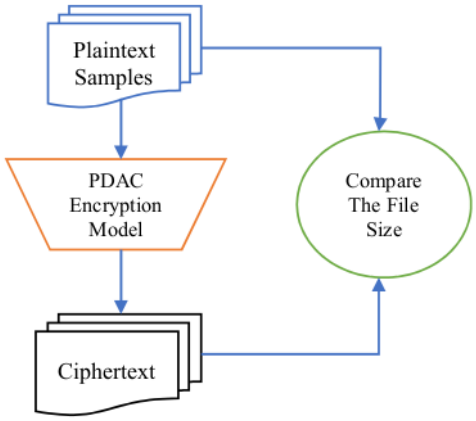

Figure 3: The Preliminary Experiment Protocol.

Preliminary research was performed by duplicating the PDAC research model. As input, samples from the astronomer dataset are used. Astronomer dataset contains short reports of astronomical data observations sent via telegram. This sample uses several different sizes, this is used to guarantee that PDAC can be used in various file size conditions. This preliminary research focuses on observing aspects of comparing the capacity of ciphertext size with plaintext size. Figure 3 shows the protocol of preliminary research.

Preliminary research results show that the size of the ciphertext is always larger than the plaintext. with an average ratio (R) of 124.88%. This means that the average size of the ciphertext is bigger than plaintext. It is almost a quarter of the size of the plaintext. Larger ciphertext size, it will require more processing time and memory.

This research focuses on the capacity aspect. This research aims to create a PDAC encryption design that produces a lighter ciphertext size. This research was performed by using experimental methods. The

expected result is that the PDAC ciphertext file size can be reduced by the ratio (R) value. The expected result is a lower ratio (R) value. Thus, the size of the ciphertext will be close to plaintext, which will result in lower memory usage and storage space.

This article is presented in several parts, the first part presents an introduction, the previous work contains several studies related to the development of PDAC, the proposed model is presented in the third session, followed by results and discussion, and a conclusion at the end of the article.

2. PREVIOUS WORKS

The PDAC encryption model has undergone several modifications. PDAC modifications are carried out to improve PDAC performance based on information security aspects. PDAC was developed into a New PDAC [26]. New PDAC focuses on increasing covertext capacity. The New PDAC has a higher covertext capacity than PDAC. The New PDAC covertext can produce 3 encryption keys. The New PDAC encryption key can encrypt 6 characters. This means that 1 covertext is used to encrypt a maximum of 6 plaintext characters. New PDAC produces a lower ciphertext size than PDAC. New PDAC development was also carried out by adding encryption process capacity with 4 encryption keys [27]. This development produces 1 covertext with 4 encryption keys. In this version of the New PDAC model, the encryption process can be used for a maximum of 6 characters, and the ciphertext size is lower than before. The New PDAC method produces ciphertext character output of 7 characters for input of 6 plaintext characters. Thus, the resulting ratio is 116.7%.

Parallel Encryption with Covertext (PECT) is a modification of PDAC in the aspects of authenticity and integrity [28]. PECT has a different covertext generator process. Each PECT covertext is produced from the conversion of 4 vowel and consonant characters in digits 0 and 1. The PECT encryption key generator produces 2 keys from each covertext. Each PECT encryption key can process a maximum of 4 plaintext characters. Thus, 1 covertext is used to encrypt 4 characters. So, the size of the PECT ciphertext has the same size ratio as PDAC. The PECT method has the same ratio as the PDAC method, namely 125%, this is because the ciphertext characters with a total of 5 characters are obtained from the concatenation of 4 plaintext characters and 1 covertext character.

PDAC was also developed in the privacy aspect using fuzzy logic. This version of PDAC is known as Fuzzy Logic PDAC [29], [30]. Fuzzy logic is applied in the PDAC covertext generator design. This fuzzy logic-based covertext generator design can generate 2 encryption keys. The impact of using fuzzy logic in PDAC is to provide randomness in information that is more difficult to predict, however with 2 keys produced by Fuzzy Logic PDAC is only able to process 4 characters. So Fuzzy Logic PDAC has a ciphertext size ratio that is almost the same as PDAC. This Fuzzy Logic PDAC method has the same capacity ratio as PDAC, namely 125%. This is because 1 covertext character and 4 plaintext characters will produce 5 ciphertext characters.

PDAC model developments that have been published always have a larger capacity ratio. This condition is a weakness of PDAC that still needs to be improved. The large size of the ciphertext requires the use of large memory and storage space, so a lot of resources are needed to encrypt secret messages. So, this condition makes it a challenge to develop a PDAC model that has a lower ratio.

3. PROPOSED MODEL

The proposed new PDAC model for reducing the size of ciphertext files is shown in Figure 4. The design of this model uses the intuition method. The encryption process in the proposed PDAC model is divided into 4 phases: Covertext Generator, Encryption Key Generator, Encryption, and Finalization.

The first phase is the Covertext Generator. Covertext generator generates covertext. The process begins by taking a character in the plaintext as *P*. Each character to be processed is converted into binary as *B*. As a sample, the character "H" with the ASCII code is 72_{10}, converted as "01001000_2" binary 8 bits. The values *P1* and *P2* contain "0100_2" and "1000_2" respectively. The *P1* value is taken from the 0th to 3rd binary sequence, the *P2* value is taken from the 4th to 7th sequence. The *P2* value is used as the covertext.

$$EncryptedText = P1 \oplus Key \quad (2)$$

The encryption key (Key) uses the covertext value "1000_2". The encryption process is carried out using the XOR operator between *P1* and the encryption key (Key) as in equation (2). The XOR logic in this

Journal of Theoretical and Applied Information Technology
31st December 2023. Vol.101. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

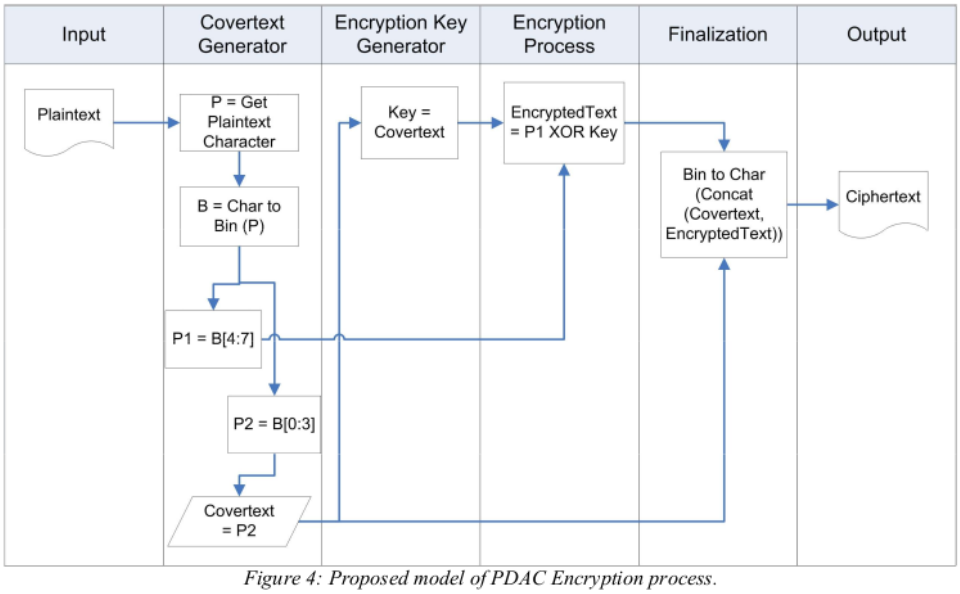

Figure 4: Proposed model of PDAC Encryption process.

process looks like a simple cipher. In this method all the character values are converted into binary values and XOR operation is performed. The XOR operation requires two operands, one is the encryption key and secret information. This XOR logic can produce different values by performing the same process using the same encryption key. XOR logic is a basic and common but complicated operation [24]. The XOR operations were also used to restore the secret information into original data [31]. In this phase, the sample character "H" becomes "0011_2" as encrypted text.

The finalization phase carries out binary conversion into characters from the concatenate process between covertext and encryptedtext. As an example of this stage of the process, the cover text is "1000_2", and the encrypted text is "0011_2" combined into "10000011_2". 8-bit binary "10000011_2" converted to ASCII code "131_{10}". The value 131_{10} is symbolized as "f". This process is repeated until the last character of the plaintext. The characters resulting from the finalization process are arranged as ciphertext.

4. RESULT AND DISCUSSIONS

In this section, the results of the experiments carried out are discussed. This experiment uses several file sizes as plaintext. This plaintext uses astronomers' data set which collected from the report of astronomer's data observations which sent through telegram. Different sizes are used to accommodate varying file sizes in real life. The proposed new PDAC model is tested with several experiments for each plaintext sample. The performance metric used is the ratios (R) using equation (1). The test results were compared with the test results on several ratio (R) value results of the previous version of the PDAC method. Table 2 shows the size of the ciphertext file obtained from the experimental results. Figure 5 shows the average

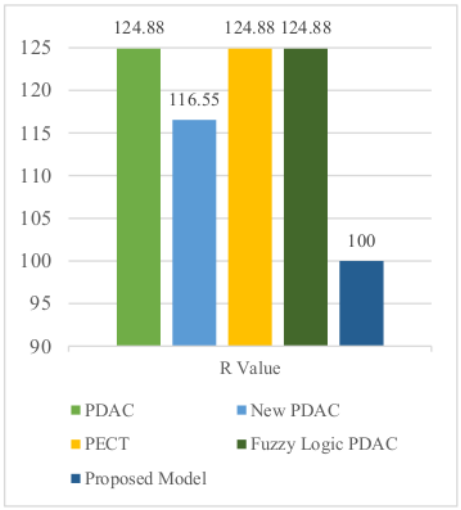

Figure 5: Average of ratio (R) Values.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of ratio (R) value between PDAC, New PDAC, PECT, Fuzzy Logic PDAC, and Proposed Model.

Table 2 shows that the proposed method has the impact of reducing the size of the ciphertext file. The proposed method's ciphertext file is the same as the size of the plaintext file. The proposed method in this experiment produces the largest ciphertext size of 128 KB with an input plaintext of 128 KB. Thus, the size of the ciphertext is the same as the size of the plaintext.

The previous version of the PDAC model gave results that the ciphertext file size was larger than the plaintext file size. PDAC ciphertext file size shows the largest value, namely 159,909 KB with a plaintext file size of 128 KB as input. This value is the same as the size of PECT, and Fuzzy Logic PDAC ciphertext models. The New PDAC model produces a ciphertext size of 149,247 KB with a plaintext input of 128 KB. Even though the New PDAC has a lower ciphertext file size than other models, the New PDAC ciphertext file is still larger than the plaintext file size.

If seen from the ratio value (R), the ciphertext size of the proposed model produces the lowest average ratio value. The average ratio (R) of the proposed model is 100%. This value means that the proposed model can reduce the size of the ciphertext file to the same size as the plaintext file. The PDAC, PECT, and Fuzzy Logic PDAC models have the same average ratio (R) value is 124.88%. This value means that the ciphertext file size is 24.88% larger than the plaintext file size. The increase in ciphertext file size in the PDAC, PECT, and Fuzzy Logic PDAC models is due to each covertext having a maximum encrypting capacity of 4 characters. Thus, the covertext requirement to run PDAC, PECT, and Fuzzy Logic PDAC is $n/4$, with the number of plaintext characters expressed as n.

The New PDAC model shows an average ratio (R) value of 116.55%, which means that the New PDAC produces a ciphertext file size of 16.55% of the plaintext file size. The new PDAC can reduce the size of the ciphertext file compared to the PDAC, PECT, and Fuzzy Logic PDAC models. This is because 1 New PDAC covertext can be used to encrypt a maximum of 6 plaintext characters. Thus, the minimum requirement for the New PDAC covertext is $n/6$, where n represents the number of plaintext characters.

Based on Table 2, the proposed method shows the average value of the ratio (R) is 100%. This value means that the size of the proposed method ciphertext file is the same as the plaintext size. The decrease in the ratio (R) value is due to the different design of the PDAC covertext generator. The proposed method uses covertext from half the length of the plaintext character bits, only 4 bits long. With the XOR logic process, the results of the encryption process will produce 4 bits of encrypted text, and the final ciphertext results will be 8 bits long. The value of 8 bits is the same as the value of 1 character.

Table 2: Ciphertext File Size of Experiment Results.

Plaintext Size (KB)	Plaintext Size (KB)				
	PDAC	New PDAC	PECT	Fuzzy Logic PDAC	**Proposed Method**
1	1.25	1.167	1.25	1.25	1
2	2.5	2.333	2.5	2.5	2
3	3.75	3.5	3.75	3.75	3
4	5	4.667	5	5	4
5	6.235	5.819	6.235	6.235	5
6	7.475	6.977	7.475	7.475	6
7	8.73	8.148	8.73	8.73	7
8	10	9.333	10	10	8
9	11.23	10.481	11.23	11.23	9
10	12.475	11.643	12.475	12.475	10
16	19.988	18.655	19.988	19.988	16
32	39.98	37.315	39.98	39.98	32
64	79.96	74.629	79.96	79.96	64
128	159.909	149.247	159.909	159.909	128
Average R (%)	124.88	116.55	124.88	124.88	**100**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3 : Significance of the ciphertext file size.

	PDAC	New PDAC	PECT	Fuzzy Logic PDAC	Proposed Model
PDAC		NS	NS	NS	S
New PDAC	NS		NS	NS	S
PECT	NS	NS		NS	S
Fuzzy Logic PDAC	NS	NS	NS		S
Proposed Model	S	S	S	S	

Through this model, the ciphertext size will be lower than the previous PDAC model.

Statistical testing was carried out to see the significance of the ciphertext file size. The Mann-Whitney calculator is used in this process. Mann-Whitney is used because it is easy to prove dependencies between two groups without having to prove normal distribution [32]. Table 3 shows the results of ciphertext size testing on PDAC, New PDAC, PECT, Fuzzy Logic PDAC, and Proposed Model. This test uses a critical value (p) of 0.05. Symbol "NS" means not significant, and symbol "S" means significant.

The results of testing the PDAC ciphertext size with New DPAC showed that the results were not significant. Testing between PDAC and New PDAC shows the *z-score* value is 0.84828, and the *p-value* is 0.39532. The results are not significant. Testing PDAC with PECT, and Fuzzy Logic PDAC shows not significant results, because these three models have the same ciphertext value.

The results of testing the proposed method with PDAC show the *z-score* is 2.09836 and the *p-value* is 0.03572. The results are significant. Testing of the proposed method with PECT and Fuzzy Logic PDAC also shows significance. Testing the Proposed method with New PDAC shows significant results. This test shows the *z-score* value is 2.49474 and the *p-value* is 0.01278.

The proposed method, apart from producing a lighter ciphertext file size, also has several other advantages, namely: that with a lighter ciphertext file size, it will speed up the process of securing confidential information and speed up the logical mathematical calculation process in it. Apart from that, the light size of the ciphertext file will result in less memory usage. The use of this memory can be in the form of internal storage memory on workstation devices, storage media, flash disks, hard disks, CDs, and common drive storage such as cloud storage and servers.

Viewed from the perspective of the vulnerability of the confidential information being sent, this proposed method provides the advantage that the transfer process time between entities will be faster. Intruders will have less time to translate the information while on the network. In this way, the security aspect of secret information remains guaranteed.

5. CONCLUSIONS

This experimental research was carried out to reduce the size of the PDAC model ciphertext file. The results obtained are that the proposed model has advantages in the capacity aspect. This proposed model produces the same ciphertext file size as the plaintext. The results of this experiment show an average ratio (R) value of 100%. The experiment shows that the ciphertext file size is 128 KB, the same as the plaintext file size. This achievement is better than the previous model which showed an average ratio (R) value of 124.88% in the PDAC, PECT, and Fuzzy Logic PDAC models, with a ciphertext size of 159.909 KB on a plaintext of 128 KB. The New PDAC model has an average ratio (R) of 116.55% with a ciphertext size of 149.247 KB on a plaintext of 128 KB. The proposed model with ratio value (R) of 100%, will impact memory usage and storage media resulting from encryption requiring more efficient resources.

Based on the results of significance testing, it was found that the proposed model had significant results compared to the previous model. While PDAC, PECT, New PDAC, and Fuzzy Logic PDAC show unsignificant result.

Based on experimental activities, the capacity ratio (R) measurement has experienced significant differences. However, this research has not measured the aspects of confidentiality and authentication. These two aspects also have an important role in the fields of information security and cryptography. So, there is a need for more in-depth research to look at these two aspects in the model that has been developed. Apart from that, the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

proposed PDAC model needs to be developed into a prototype that can be implemented in the form of a Software Development Kit system that runs in the company.

ACKNOWLEDGEMENT

This research was funded by the Ministry of Research, Technology, and Higher Education in 2023 through the National Competitive Research Scheme for Fundamental Research - Regular and Universitas Stikubank (Unisbank) Semarang.

REFERENCES:

[1] G. Surla, R. Lakshmi, and I. Thamarai, "A SYSTEMATIC SURVEY ON CRYPTO ALGORITHMS USING QUANTUM COMPUTING," *J Theor Appl Inf Technol*, vol. 30, no. 12, 2023, [Online]. Available: www.jatit.org

[2] S. Subramani, S. M, K. A, and S. K. Svn, "Review of Security Methods Based on Classical Cryptography and Quantum Cryptography," *Cybern Syst*, vol. 2023, pp. 1–19, Jan. 2023, doi: 10.1080/01969722.2023.2166261.

[3] R. M. Al-Amri, D. N. Hamood, and A. K. Farhan, "Theoretical Background of Cryptography," *Mesopotamian Journal of Cyber Security*, vol. 2023, pp. 7–15, Jan. 2023, doi: 10.58496/MJCS/2023/002.

[4] E. Ardhianto, A. Trisetyarso, W. Suparta, B. S. Abbas, and C. H. Kang, "Design Securing Online Payment Transactions Using Stegblock Through Network Layers," *IOP Conf Ser Mater Sci Eng*, vol. 879, no. 1, p. 012027, Jul. 2020, doi: 10.1088/1757-899X/879/1/012027.

[5] E. Ardhianto, H. L. H. S. Warnars, B. Soewito, F. L. Gaol, and E. Abdurachman, "Improvement of Steganography Technique: A Survey," in *Proceedings of the 1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)*, Paris, France: Atlantis Press, 2020. doi: 10.2991/assehr.k.200303.070.

[6] Y. Xu, C. Mou, Y. Hu, J. Xie, and J. Zhang, "Robust Invertible Image Steganography," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE Explore, Jun. 2022, pp. 7875–7884.

[7] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey," *Inf Sci (N Y)*, vol. 609, pp. 1451–1488, Sep. 2022, doi: 10.1016/j.ins.2022.07.120.

[8] W. T. Handoko, E. Ardhianto, K. Hadiono, and F. A. Sutanto, "Protecting Data by Socket Programming Steganography," in *IOP Conference Series: Materials Science and Engineering*, 2020. doi: 10.1088/1757-899X/879/1/012028.

[9] R. Hammad *et al.*, "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message," *J Phys Conf Ser*, vol. 2279, no. 1, p. 012006, May 2022, doi: 10.1088/1742-6596/2279/1/012006.

[10] E. Ardhianto, W. T. Handoko, H. Murti, and R. S. A. Redjeki, "Encryption with Covertext and Reordering using Permutated Table and Random Function," in *2021 2nd International Conference on Innovative and Creative Information Technology, ICITech 2021*, 2021. doi: 10.1109/ICITech50181.2021.9590171.

[11] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, Jun. 2019, pp. 1–6. doi: 10.1109/ISDFS.2019.8757514.

[12] V. B. Savant and R. D. Kasar, "A Review on Network Security and Cryptography," *Research Journal of Engineering and Technology*, vol. 12, no. 4, pp. 110–114, Dec. 2021, doi: 10.52711/2321-581X.2021.00019.

[13] M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, "Physical Layer Security: Authentication, Integrity, and Confidentiality," in *Physical Layer Security*, Cham: Springer International Publishing, 2021, pp. 129–150. doi: 10.1007/978-3-030-55366-1_6.

[14] A. Kumar, R. Rani, and S. Singh, "A survey of recent advances in image steganography," *SECURITY AND PRIVACY*, vol. 6, no. 3, May 2023, doi: 10.1002/spy2.281.

[15] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless Image Steganography: A Survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019, doi: 10.1109/ACCESS.2019.2955452.

[16] D. R. I. M. Setiadi, "Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation," *International Journal of Electronics and*

Telecommunications, vol. 65, no. 2, pp. 287–292, Jul. 2023, doi: 10.24425/ijet.2019.126312.

[17] D. Bi, S. Kadry, and P. M. Kumar, "Internet of things assisted public security management platform for urban transportation using hybridised cryptographic-integrated steganography," *IET Intelligent Transport Systems*, vol. 14, no. 11, pp. 1497–1506, Nov. 2020, doi: 10.1049/iet-its.2019.0833.

[18] F. Varghese and P. Sasikala, "A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography," *Wirel Pers Commun*, vol. 129, no. 4, pp. 2291–2318, Apr. 2023, doi: 10.1007/s11277-023-10183-z.

[19] M. S. Abbas, S. S. Mahdi, and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," in *2020 International Conference on Computer Science and Software Engineering (CSASE)*, Duhok, Iraq: IEEE, Apr. 2020, pp. 123–127. doi: 10.1109/CSASE48920.2020.9142072.

[20] A. Hadipour and R. Afifi, "Advantages and disadvantages of using cryptography in steganography," in *2020 17th International ISC Conference on Information Security and Cryptology (ISCISC)*, Tehran, Iran: IEEE, Sep. 2020, pp. 88–94. doi: 10.1109/ISCISC51277.2020.9261921.

[21] S. J. Gladwin and P. Lakshmi Gowthami, "Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images," in *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*, Amaravati, India: IEEE, Jan. 2020, pp. 1–5. doi: 10.1109/AISP48273.2020.9073306.

[22] S. Kataria, B. Singh, T. Kumar, and H. S. Shekhawat, "PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography," in *Int. Conf. on Advances in Computer Science, AETACS*, 2013, pp. 175–182.

[23] 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," in *19th IEEE Student Conference on Research and Development: Sustainable Engineering and Technology towards Industry Revolution, SCOReD 2021*, 2021. doi: 10.1109/SCOReD53546.2021.9652746.

[24] C. Singh and E. Baburaj, "XOR Reformed Paillier Encryption Method with Secure De-duplication for Image Scaling and Cropping in Reduced Cloud Storage," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 4, pp. 328–337, Aug. 2019, doi: 10.22266/ijies2019.0831.30.

[25] M. Sivalakshmi and J. K. Gothwal, "Image Encryption and Decryption Scheme using Shuffling and Reversing," in *2 nd International Conference on Emerging Trends in Engineering, Sciences & Management*, RGM College of Engineering & Technology, 2018, pp. 111–114.

[26] 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, [Online]. Available: http://www.ijritcc.org

[27] W. T. Handoko, E. Ardhianto, and E. Supriyanto, "MODIFIKASI NEW PDAC (PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVER TEXT)," in *Proceeding SENDIU 2020*, Semarang, 2020, pp. 55–59.

[28] S. Panwar, M. Kumar, and S. Sharma, "Text Steganography Based on Parallel Encryption Using Cover Text (PECT)," in *4th International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, Nain; Neeta and Vipparthi; Santosh Kumar, Eds., Springer, 2020, pp. 303–313. doi: 10.1007/978-3-030-39875-0_32.

[29] E. Ardhianto, Y. Heryadi, L. A. Wülandhari, and W. Budiharto, "Covertext Generation using Fuzzy Logic Approach in Parallel Encryption with Digit Arithmetic of Covertext to Improve Information Confidentiality," *International Journal of Innovative Computing, Information and Control*, vol. 19, no. 4, pp. 1311–1321, Aug. 2023, doi: 10.24507/ijicic.19.04.1311.

[30] E. Ardhianto, Y. Heryadi, L. A. Wulandhari, and W. Budiharto, "PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVERTEXT ENCRYPTION MODEL USING COVERTEXT GENERATOR WITH FUZZY LOGIC APPROACH," *ICIC Express Letters ICIC International*, vol. 17, no. 7, pp. 817–824, 2023, doi: 10.24507/icicel.17.07.817.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[31] Y. He, G. Xia, and C. He, "A File cloud sharing method based on XOR operation," *IOP Conf Ser Mater Sci Eng*, vol. 768, no. 7, p. 072085, Mar. 2020, doi: 10.1088/1757-899X/768/7/072085.

[32] P. V. Razumov, I. A. Smirnov, I. A. Pilipenko, A. V. Selyova, and L. V. Cherkesova, "Comparative analysis of NTRUEncrypt modified post-quantum cryptographic system and standard RSA cryptosystem," *Vestnik of Don State Technical University*, vol. 19, no. 2, pp. 185–194, Jun. 2019, doi: 10.23947/1992-5980-2019-19-2-185-194.

Q4_A LIGHT WEIGHT OF PARALLEL ENCRYPTION

ORIGINALITY REPORT

3%	3%	4%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to STIE Perbanas Surabaya Student Paper	3%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	Off		