ICIC Express Letters
Volume **18**, Number **1**, January **2024**
 ISSN 1881-803X
pp. 9–15

NEW MECHANISM OF PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVER TEXT ENCRYPTION MODEL WITH REDUCED CIPHERTEXT SIZE

Eka Ardhianto*, Widiyanto Tri Handoko and Endang Lestariningsih

Faculty of Information Technology and Industry
Universitas Stikubank
Jl. Tri Lomba Juang No. 1, Semarang 50241, Central Java, Indonesia
{ wthandoko; endang_lestariningsih }@edu.unisbank.ac.id
*Corresponding author: ekaardhianto@edu.unisbank.ac.id

Received January 2023; accepted April 2023

Abstract. *Communication using the Internet requires secure and lightweight data. The Parallel Encryption with Digit Arithmetic of Cover Text (PDAC) encryption model can provide security through encryption and steganography processes. However, this model produces a ciphertext with a size 25% larger than the plaintext. This research focuses on how to reduce the size of the ciphertext generated from PDAC. The proposed model changes the PDAC cover text generation process using plaintext ASCII-coded binary values. The result obtained is that the resulting ciphertext shows the size of the ciphertext is the same as the plaintext. Thus, the plaintext and ciphertext ratio is 100%, which is lower than the previous method. Ciphertext with a small size will speed up the transfer process and reduce redundant processing. Statistical testing also showed a significant difference.*
Keywords: Ciphertext, Encryption, Cover, PDAC, Cover text, Fuzzy logic

1. **Introduction.** The invention of the computer and the Internet has greatly influenced the way information is transferred, data is shared, and the way humans communicate. Data transfer and communication quickly and widely can now be done through an open Internet [1]. Internet media that can be accessed by many entities makes the confidential data that is passed vulnerable, so it needs a special security mechanism. In the field of information security, cryptography and steganography are the solutions to secure confidential data [2-4]. Cryptography secures data using the technique of scrambling data using keys so that it becomes difficult to interpret directly [5,6]. Steganography secures data by hiding data in an object known as a "cover" so that its existence is not realized [7]. In the field of information security, the encryption is known as the process of scrambling secret messages into ciphertext, and the decryption is the process of turning ciphertext back into the plaintext [5], plaintext is data or secret messages that are secured, and ciphertext is the result of the encryption process [4].

To ensure strong data security, several studies suggest combining cryptography and steganography [8,9]. Secret data is secured using cryptographic techniques and hidden in "cover" using steganography techniques. Combining these techniques will make unauthorized parties unaware of the existence of confidential data and will be difficult to read directly [8]. This combination makes for a reliable and robust system [9].

Parallel Encryption with Digit Arithmetic of Cover Text (PDAC) is an encryption model that combines text-based steganography techniques with cryptographic techniques [10]. One important factor that makes this encryption model work is the cover text [11]. Cover text in PDAC is a character that functions as a cover in the context of steganography

DOI: 10.24507/icicel.18.01.9

[12]. The development of the PDAC is known as the New PDAC [13], and Parallel Encryption with Cover Text (PECT) [14]. New PDAC and PECT also require cover text in the process. PDAC requires $n/4$ cover text, where n is the number of plaintext characters [10]. New PDAC requires less cover text than PDAC, which is $n/6$ [13]. PECT requires the same number of cover texts as PDAC which is $n/4$ [14]. The difference in the need for the number of cover texts affects the encryption key generation process. PDAC and PECT generate encryption keys through two arithmetic processes of addition, and subtraction of cover text ASCII digits [10,14], while New PDAC generates encryption keys through three arithmetic processes of addition, subtraction, and multiplication of cover text ASCII digits [13]. Figure 1 shows the differences in the PDAC, New PDAC, and PECT processes.

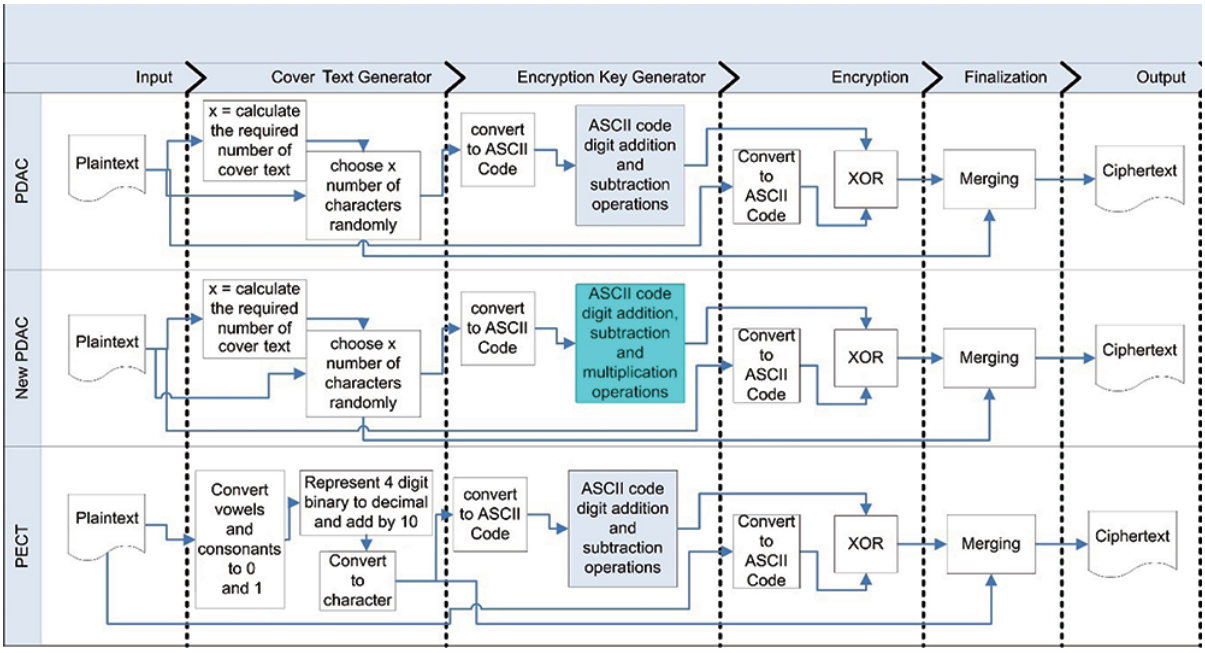

FIGURE 1. The encryption process of the PDAC, New PDAC, and PECT model adopted from [10,13,14]

As the preliminary experiment, observations were focused on the size of the ciphertext files from the PDAC, New PDAC, and PECT processes. Based on the process in Figure 1, the amount of cover text required is different for each model. The use of different amounts of cover text results in different ratios of ciphertext files. The ciphertext file ratio (R) is the percentage ratio of ciphertext file size to plaintext [15]. Equation (1) is used to calculate the ratio of ciphertext files. PDAC and PECT ciphertexts have a file size that is 25% larger than plaintext files, and the New PDAC ciphertext is 17% larger than plaintext. The increase in ciphertext file size is due to the difference in the number of keys needed. Table 1 shows the results of preliminary experiments comparing ciphertext file sizes from the PDAC, New PDAC, and PECT models.

$$R = \left(\frac{ciphertext\ size}{plaintext\ size} \right) \times 100\% \tag{1}$$

Based on Table 1, the average size of ciphertext files produced by the three methods has increased which will impact the waste of storage media. The large ciphertext size is also a problem that needs to be considered in the data security process [16]. The ciphertext with a smaller size will speed up the transfer process and reduce excessive computation [17]. Several studies have been conducted related to techniques for reducing files in the context of data security using steganography and cryptography techniques. The cryptographic approach based on the DNA algorithm can reduce the ciphertext file size by up to 33%

Table 1. Comparison of ciphertext file size with the plaintext of the preliminary experiment

Plaintext file size (bytes)	Ciphertext file size (bytes)		
	PDAC	New PDAC	PECT
1.000	1.250	1.167	1.250
2.000	2.500	2.333	2.500
3.000	3.750	3.500	3.750
4.000	5.000	4.667	5.000
5.000	6.235	5.819	6.235
6.000	7.475	6.977	7.475
7.000	8.730	8.148	8.730
8.000	10.000	9.333	10.000
9.000	11.230	10.481	11.230
10.000	12.475	11.643	12.475
16.000	19.988	18.655	19.988
32.000	39.980	37.315	39.980
64.000	79.960	74.629	79.960
128.000	159.909	149.247	159.909
Average ciphertext file ratio (%)	125	116.7	125

compared to the size of other ciphertexts that are processed using traditional encryption techniques [18]. The Policy Hiding using Logical Connective (PHLC) scheme implemented in Ciphertext Policy Attribute-Based Encryption (CP-ABE) helps reduce the size of the ciphertext and reduces the computational overhead of the encryption process in cloud data storage [17]. Searchable Encryption with a Shiftable Trapdoor (SEST) scheme is also proposed to reduce the ciphertext size [19]. LZW compression scheme in color-coded text steganography can reduce ciphertext file size and increase cover capacity through 32-bit color coding [20,21]. The use of the Huffman compression algorithm in the LSB steganography technique can reduce the size of ciphertext files to the size of plaintext files [22,23]. PDAC development into New PDAC has been able to reduce ciphertext file size with a ratio of 116.7% to plaintext [13]. Thus, a smaller ciphertext file size will speed up the data transmission process and save storage space.

The research in this article focuses on how to reduce the ciphertext file size generated by the PDAC encryption model. Ciphertext file size ratio is used as a performance metric in this experiment. The result obtained is that the ciphertext file size ratio is 100%, and it means the ciphertext has the same size as the plaintext file. This result is better than before which shows the size of the ciphertext file is 125%. This new achievement makes the data transfer process safer and faster, and requires less storage media.

The discussion in this article is divided into several sections. Section 1 describes the background. The proposed method is explained in Section 2. Section 3 provides experimental results, are given and conclusions at the end of the article.

2. **Proposed Method.**

This proposed new method experiment uses sample data taken from the Astronomer Telegram Dataset as plaintext. The samples taken have different sizes, and this is done to maintain the diversity of possible forms of data transfer. The proposed method is divided into 4 stages, which are cover text generator, encryption key selection, encryption process, and finalization. Figure 2 shows the proposed new method on PDAC. Cover text generator is a process for generating cover text, encryption key is a

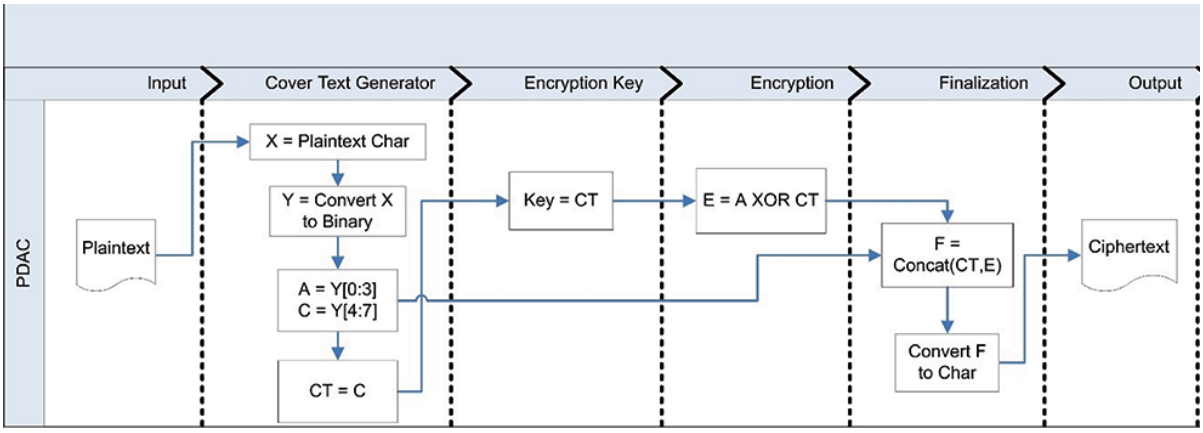

FIGURE 2. Proposed method on PDAC

process for issuing encryption keys, encryption is an encryption process using XOR logic, and finalization is a process of combining the results of the encryption with the cover text.

The cover text generator process aims to get a cover text. Each plaintext character is represented by X, and Y is the binary form of each plaintext character. For example, X = "M" with its ASCII code is 77, and its binary form in Y is 01001101. The binary digit Y is divided into two variables A and C, so that A is 0100, and C is 1101. In this phase the value of C is used as cover text (CT). The encryption key (key) uses the value on the CT. The encryption process uses XOR logic between A and CT as encrypted text (E), in the example, the result is 0100 XOR 1101 is 1001 as E. This model uses XOR logic-based encryption because it is the simplest yet most effective symmetric cryptography method, using the same key during encryption and decryption based on reversible features, which refers to the binary sequence A can return to its original value by executing twice XOR operations with sequence K, as shown by Equation (2) [12]. A is the information text, K is the key and E is the encrypted text. In the finalization phase, a concatenation process is carried out between the cover text (CT) and the encrypted text (E), to 11011001 as F, and converted to the symbol as the ciphertext.

$$\begin{aligned} A \oplus K &= E \\ E \oplus K &= A \end{aligned} \tag{2}$$

3. **Experiments and Results.** The plaintext samples were taken from conversations in the Astronomer Telegram dataset which contains short reports of astronomical observations in text format. The number of samples used is 14 conversations with different file sizes; this is done to maintain the diversity of forms of communication and data transfer that may occur. The experiment was performed 700 times for all samples. As a performance metric, the comparison of ciphertext file sizes in the PDAC, New PDAC, and PECT models, to the proposed method is calculated. Ciphertext comparison is calculated by Equation (1) [15].

The experimental results are shown in Table 2. The proposed method used to process plaintext files produces the same ciphertext size, and the ratio shows a value of 100%. This means that the plaintext file size is the same as the ciphertext size. When compared to other methods, PDAC and PECT produce a ciphertext size of 125% of plaintext, and the New PDAC method produces a ciphertext size of 116.7% of plaintext. Thus, the proposed method can reduce the ciphertext file size better. With a lighter size, the data transfer process will be faster, as well as more efficient memory usage. Figure 3 visually shows a comparison of plaintext with ciphertext for each encryption model.

This proposed method has different processes. The new method proposes the cover text using the ASCII code of the last 4 binary digits, whereas the previous cover text method

TABLE 2. Comparison of ciphertext file size with the plaintext of the preliminary experiment to the proposed method

Plaintext file size (bytes)	Ciphertext file size (bytes)			
	PDAC	New PDAC	PECT	Proposed method
1.000	1.250	1.167	1.250	1.000
2.000	2.500	2.333	2.500	2.000
3.000	3.750	3.500	3.750	3.000
4.000	5.000	4.667	5.000	4.000
5.000	6.235	5.819	6.235	5.000
6.000	7.475	6.977	7.475	6.000
7.000	8.730	8.148	8.730	7.000
8.000	10.000	9.333	10.000	8.000
9.000	11.230	10.481	11.230	9.000
10.000	12.475	11.643	12.475	10.000
16.000	19.988	18.655	19.988	16.000
32.000	39.980	37.315	39.980	32.000
64.000	79.960	74.629	79.960	64.000
128.000	159.909	149.247	159.909	128.000
Average ciphertext file ratio (%)	125	116.7	125	**100**

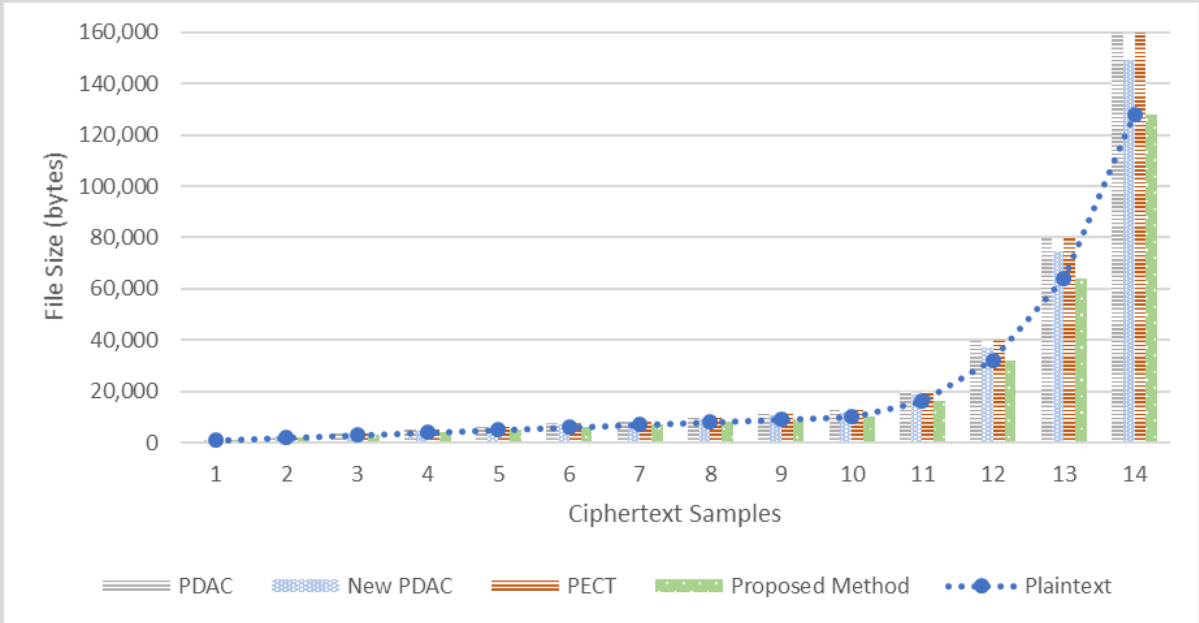

FIGURE 3. Comparison of file size cover text with plaintext

was selected using random function, and based on vowel or consonant characters. In the encryption key generator section, the encryption key uses the same value as the cover text. Thus, the encryption process only processes as many as 4 digits between the cover text and the first 4 digits of plaintext, whereas the previous model processed as many as 8 cover text digits and 8 plaintext digits. The finalization process is carried out the same as the previous model by combining encrypted text with cover text. In this model, the number of digits combined is only 4 digits, so the combined encrypted text and cover text is 8 digits. In the previous model, a combination was performed between the encrypted

text and the cover text used, so that apart from the encrypted text digits measuring 8 digits, the addition of this cover text causes an increase in the size of the ciphertext file.

To see the significance between the proposed method and the previous method, a statistical test was carried out using the Mann-Whitney method. The Mann-Whitney test is carried out using Equations (3), and (4) [24,25]. 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. The *z-score* (z) is compared with the corresponding critical value obtained from the normal distribution table for the rejection or acceptance of the hypothesis at the significance level (α).

$$U = n_1 n_2 + \frac{n_1(n_{1+1})}{2} - R_2 \tag{3}$$

$$z = \frac{U - \frac{n_1 n_2}{2}}{\sqrt{\left(\frac{n_1 n_2 (n_1 + n_2 + 1)}{12}\right)}} \tag{4}$$

The statistical test results showed the significance of the plaintext size proposed by the method to the PDAC and PECT ciphertext sizes. This statistical test uses a significant value (α) of 0.05. The results show that the *z-score* is -4.28516. So, the result is significant at $\alpha < 0.05$. Significance testing was also carried out between the proposed method ciphertext size and the New PDAC ciphertext size. The results obtained are that the *z-score* is -4.89966. So, the result is significant at $\alpha < 0.05$. Based on the results of both tests, the proposed method shows significance (meaningful) in reducing the size of the ciphertext.

4. **Conclusions.** The small ciphertext file size becomes important in accelerating data transfer. In this article, the proposed method contributes to reducing the size of ciphertext files with a ratio of 100% to plaintext files. This means that the size of the ciphertext is the same as the size of the plaintext. The resulting size in the proposed method is better than the previous method, namely PDAC ciphertext and PECT which produces a ratio of 125%, and New PDAC ciphertext which has a ratio of 116.7% to plaintext. As further research, it is necessary to have more in-depth thought on the proposed model regarding the resulting security aspects so that in addition to the resulting ciphertext having a small size, it also remains secure.

REFERENCES

[1] Z. L. Wang, Entropy theory of distributed energy for Internet of Things, *Nano Energy*, vol.58, pp.669-672, DOI: 10.1016/j.nanoen.2019.02.012, 2019.

[2] M. S. Abbas, S. S. Mahdi and S. A. Hussien, Security improvement of cloud data using hybrid cryptography and steganography, *2020 International Conference on Computer Science and Software Engineering (CSASE)*, pp.123-127, DOI: 10.1109/CSASE48920.2020.9142072, 2020.

[3] 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.

[4] M. Alkhudaydi and A. Gutub, Securing data via cryptography and Arabic text steganography, *SN Comput. Sci.*, vol.2, no.1, p.46, DOI: 10.1007/s42979-020-00438-y, 2021.

[5] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, Hiding data using efficient combination of RSA cryptography, and compression steganography techniques, *IEEE Access*, vol.9, pp.31805-31815, DOI: 10.1109/ACCESS.2021.3060317, 2021.

[6] M. T. Ahvanooey, Q. Li, H. J. Shim and Y. Huang, A comparative analysis of information hiding techniques for copyright protection of text documents, *Security and Communication Networks*, vol.2018, pp.1-22, DOI: 10.1155/2018/5325040, 2018.

[7] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, Image steganography: A review of the recent advances, *IEEE Access*, vol.9, pp.23409-23423, DOI: 10.1109/ACCESS.2021.3053998, 2021.

[8] O. M. Osman, M. E. A. Kanona, M. K. Hassan, A. A. E. Elkhair and K. S. Mohamed, Hybrid multistage framework for data manipulation by combining cryptography and steganography, *Bulletin*

of Electrical Engineering and Informatics, vol.11, no.1, pp.327-335, DOI: 10.11591/eei.v11i1.3451, 2022.

[9] A. Bose, A. Kumar, M. K. Hota and S. Sherki, Steganography method using effective combination of RSA cryptography and data compression, *2022 1st International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, pp.1-5, DOI: 10.1109/ICEE ICT53079.2022.9768402, 2022.

[10] S. Kataria, B. Singh, T. Kumar and H. S. Shekhawat, PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) based text steganography, *Int. Conf. on Advances in Computer Science (AETACS)*, pp.175-182, 2013.

[11] 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, *The 19th IEEE Student Conference on Research and Development: Sustainable Engineering and Technology towards Industry Revolution (SCOReD2021)*, DOI: 10.1109/SC OReD53546.2021.9652746, 2021.

[12] 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.

[13] 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.

[14] 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)*, vol.1122, pp.303-313, DOI: 10.1007/978-3-030-39875-0_32, 2020.

[15] S. Timilsina and S. Gautam, Analysis of hybrid cryptosystem developed using blowfish and ECC with different key size, *Technical Journal*, vol.1, no.1, pp.10-15, DOI: 10.3126/tj.v1i1.27582, 2019.

[16] N. H. UbaidurRahman, C. Balamurugan and R. Mariappan, A novel DNA computing based encryption and decryption algorithm, *Procedia Comput. Sci.*, vol.46, pp.463-475, DOI: 10.1016/j.procs. 2015.02.045, 2015.

[17] S. D. M. Satar, M. Hussin, Z. M. Hanapi and M. A. Mohamed, Towards virtuous cloud data storage using access policy hiding in ciphertext policy attribute-based encryption, *Future Internet*, vol.13, no.11, 279, DOI: 10.3390/fi13110279, 2021.

[18] L. M. Gupta, H. Garg and A. Samad, An improved DNA based security model using reduced cipher text technique, *International Journal of Computer Network and Information Security*, vol.11, no.7, pp.13-20, DOI: 10.5815/ijcnis.2019.07.03, 2019.

[19] J. Kim, W. Susilo, Y.-W. Chow, J. Baek and I. Kim, Pattern matching over encrypted data with a short ciphertext, in *Information Security Applications. WISA 2021. Lecture Notes in Computer Science*, H. Kim (ed.), Cham, Springer, 2021.

[20] J. K. Sadié, L. M. Metcheka and R. Ndoundam, Two high capacity text steganography schemes based on color coding, *arXiv.org*, arXiv: 2004.00948, 2020.

[21] A. Kaur, S. Kaur and G. Sehti, Improved text steganography scheme based on LZW compression and color coding, *International Journal of Computational Engineering Research (IJCER)*, vol.8, no.6, pp.26-34, 2018.

[22] M. Y. Elmahi and T. M. Wahbi, Multi-level steganography aided with compression, *2019 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, pp.1-6, DOI: 10.1109/ICCCEEE46830.2019.9071188, 2019.

[23] N. A. A. Mustafa, Text hiding in text using invisible character, *International Journal of Electrical and Computer Engineering (IJECE)*, vol.10, no.4, pp.3550-3557, 2020.

[24] 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.

[25] E. U. Oti, M. O. Olusola and P. A. Esemokumo, Statistical analysis of the median test and the Mann-Whitney U test, *International Journal of Advanced Academic Research*, vol.7, no.9, pp.44-51, 2021.