




Text Encryption by Indexing ASCII of Characters Based on the Locations of Pixels of the Image



Seerwan W. Jirjees^{*}, Farah F. Alkhalid[†], Ahmed M. Hasan[‡]

Control and Systems Engineering Department, University of Technology- Iraq, Baghdad 10066, Iraq

Corresponding Author Email: seerwan.w.jirjees@uotechnology.edu.iq

<https://doi.org/10.18280/ts.400240>

ABSTRACT

Received: 29 November 2022

Accepted: 10 March 2023

Keywords:

text encryption, brute force, cryptanalysis, encoding pixels, key sensitivity

Network security has recently become a major issue since the growth of electronic data exchange so cryptography is important in protecting secure online data resources from integrity, confidentiality, and safety perspective against potential attacks such as eavesdropping and brute force. In this paper, we proposed a method for encrypting the transmitted information based on an image, which worked as a key that is saved by the client and the server. The encryption process of the text will be to encode characters by changing the ASCII code of characters with the locations (row and column) of the ASCII code equivalent in the image data, the locations will be chosen randomly. The proposed algorithm provides a relatively greater degree of security in avoiding avalanches, eavesdropping attacks, and password space because the character encoding method will be dynamic depending on the size and type of image used. Several securities analyses were presented, and the proposed algorithm proved to be highly secure. Compared to some current text cypher schemes, the proposed algorithm is very safe against modern cryptanalysis.

1. INTRODUCTION

With the advancement of technology, the need for information security has become necessary to maintain privacy and data integrity as individuals and organizations exchange digital data daily like passwords, credit cards, personal information, accounts, cloud storage and others. The term of privacy denotes to make persons able to control and manage their information and prevent unauthorized, integrity refers to the reliability and accuracy of reaching the transmitted data without any modification from sender to receiver [1]. Various methods and techniques have been developed to protect transmitted data from unauthorized access. Secure information is achieved through the use of cryptography and steganography [2]. The former sends data in an unintelligible format, whereas the latter sends data in a hidden format which converts confidential data from its original form to unrecognizable encrypted data. Cryptography is a math method for encrypting and decrypting data. Encryption provides for storing or transmitting sensitive information over unsecured networks so that only the intended recipient can read it. substitution and transposition are the methods to perform one or both primary operations for encrypting data and producing secure encrypted data. substitution involves changing the confidential information's original values into various new values [3, 4], and transposition involves changing the order of the original values of the confidential data to new values. Because these two procedures are well-known, the strength of any new encryption system depends on the innovation of the style method and keys utilized [5, 6].

The security of cryptographic algorithms depends on the security of the keys used, which describe how to perform substitutions and substitutions on the original confidential data.

A key is a piece of variable data provided as input to an encryption algorithm to perform this type of operation, there are two types of encryptions: symmetric key and asymmetric encryption. A symmetric key called a private key uses the same key to encrypt and decrypt data, while an asymmetric key called public key cryptography uses two types of keys: private and public keys [7, 8].

The main idea of the proposed system is how to keep the information transmitted over the transmissions confidential so that the attacker would struggle to figure out the plaintext. In this paper, we present an algorithm based on encoding text characters with values represented by pixel locations of an image that acts as a pre-agreed key between sender and receiver. Not directly using text in the encryption process gives the algorithm high security against statistical attacks, key sensitivity and cipher only attacks. In addition to the randomness in the way of encoding the characters of the text from the pixels image locations, it provides high resistance to statistical attack. The experimental results showed that the proposed method achieves different random values in each encryption process and a larger size to resist the key sensitivity analysis attack.

The rest of the paper is organized as follows. Section 2 contains a brief literature review of relevant previous work. Section 3 presents the proposed algorithm in detail. The experimental results and security analysis are shown in section 4. Finally, conclusions are provided in Section 5.

2. RELATED WORK

Security and privacy are among the main concerns of users during communication, so the text message encryption process has gained great attention from researchers. We briefly review

some of the schemes used to encrypt texts.

Thinn and Thwin [9] proposed a symmetric algorithm for text ciphering, based on a modified Advanced Encryption Standard (AES), they added an additional key and Sub-Bytes step, the operation is done by creating a second key, then XORing with plain text, finally applying Modification in the SubBytes function. Zeena and Melad [10] used DNA code, depending on taking 8 adjacent letters, then encrypted these letters using DNA Table by Substituting separately a matching letter on the table, authors finally hid the encrypted text inside the image using four pseudo random generated from chaotic operation to choose a position in the image authors [11] proposed a novel way for text encryption from three steps, the first is applying cyclic shift on encoded plain text to generate a diffusion set, the second step is applying the Pell sequence, a weight function, and a binary sequence to encode each element of the diffused plain text into real numbers, finally Confused encoded text by generating two bijections. Murillo-Escobar et al. [12] proposed an encryption for authentication using fingerprint, by depending on pseudorandom sequences created by a chaotic scheme. Some chaotic features are powerfully linked with cryptography features, then created unidimensional logistic map which is the simple non linear chaotic system that achieve clearly the chaos route.

Authors [13] presented a new method for text encryption by converting the plain text to ASCII, then partition the ASCII values to sets, then each set is converted to big integer values taking specified base, then pad to 32 to refer to blank space in ASCII, then create a random factor for dot production. The authors [14] proposed an encryption method for intranet application, this is done by implementing a secure method via Elliptic curve cryptography for cryptographic algorithm and integrate checksum prediction system, data is divided into chunks for processing and the key is generated for further process. Muhammad et al. [15] proposed a new algorithm for encryption by ASCII values and Gray Code (AGC) to keep data safe via communication. Using Gray code had given the technique of strong encryption, in addition, the size of the encrypted text was less than the plain text. The authors [16] encoded the source code of the PHP page by using a mixture of the Merkle-Hellman Knapsack algorithm, Discrete Logarithm and character modification to obtain complex encryption. Authors [9] studied the cryptography using the ASCII codes and then used the modified Vigenere table in order to get extremely cryptographic the same time using simple steps. Sakshi et al. [17] used two cypher algorithms (Vigenere and Caesar), then modified Vigenere table, the ASCII code took to decrease the complication and increase the security. Dharshini et al. [18] proposed a new cryptography method based on mapping characters table depending on mix two strategies Cryptography and Polygram, this method led to a decrease the time of encryption and decryption process. The author [19] proposed to convert text to ASCII code then encoded it as an image using the private table, then combined images and saved as a new image as a Sumerian image then encrypted them. Huwaida et al. [20] proposed an algorithm for steganography using ASCII imbedded in the coloured image depending on equivalent value location. The proposed system for most researchers listed previously depends on the key and its length, as is the case with encryption algorithms while the proposed algorithm depends on the size and specifications of the images that act as a key The method of encoding the password can be changed and updated according to the protocol between the sender and the recipient.

3. PROPOSED ALGORITHM

A practical method has been developed to encode text by representing the ASCII code for text characters at locations representing the row and column of the image. This method is designed to solve problems in the field of text coding and to develop procedures and business strategies to provide scientific and logical justification for the results. It will be agreed on a number of images that will be stored at the sender and recipient, representing a key for the encryption and decryption process, as they will be numbered uniformly at both ends. At each encryption process, one of these images will be used randomly, and the code for the image will be sent with the ciphertext where the same image will be used in the decryption process. The step-by-step working method of the proposed method is illustrated in Figure 1, there are three main steps of encoding and decrypting a text. In the first step, the text is converted to an ASCII array. After that, an image will be randomly selected and converted into three tables. Then the ASCII value of each character will be searched in the three tables and one will be chosen randomly.

3.1 Encryption strategy

The encryption strategy consists of 3 levels as demonstrates in Figure 1. In the first level, each character in plain text is converted to ASCII code independently, in the second level, three different matrices are created Red, Green, Blue, finally, looking for each ASCII code we got from Level1 inside the 3 matrices we got from level2, then fix each code we found inside the three matrices in a new table, encoding ASCII by random indexing (row, column). The original image will first be read, then divided into colours (Red, Green, Blue), In the next step, the text encoding process will begin, where it will be divided into characters and then converted to the ASCII code then search for it's in all encrypted images (R,G,B), finally is to choose one random location to represent the character and then encode the location as shown in Algorithm 1.

Algorithm 1: Proposed Text Encryption

Input: Plain image I with the size $r \times c \times 3$ where r, c rows and columns of the image and Plain text $S=(t_0, t_1, \dots, t_z)$ where t =alphanumeric and z =length of S

Output: Cipher text P

- 1: Decompose the input image S into three R, G, and B sub bands images ER, EG, EB.
 - 2: For $i = 1$ to z
 - 3: Choose random value (g)
 - 4: If $g=1$ then
 - 5: $Q = ER$
 - 6: Else if $g=2$ then
 - 7: $Q = EG$
 - 8: Else
 - 9: $Q = EB$
 - 10: End if
 - 11: convert characters $S[i]$ to ASCII code (AS)
 - 12: Find all locations($Q[r,c]$) of AS and save it in temporary array TA
 - 13: Select random value from TA
 - 14: $E = \text{Encoding TA } [g, \text{row}, \text{column}] = // \text{ call algorithm2}$
 - 15: $P[i] = E$
 - 16: End For i
-

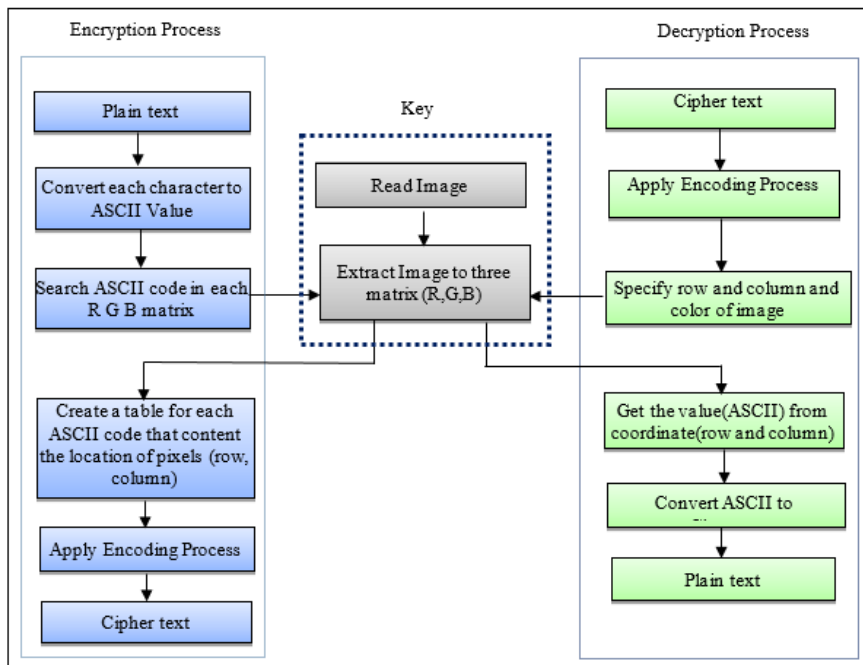


Figure 1. The proposed algorithm for encryption and decryption

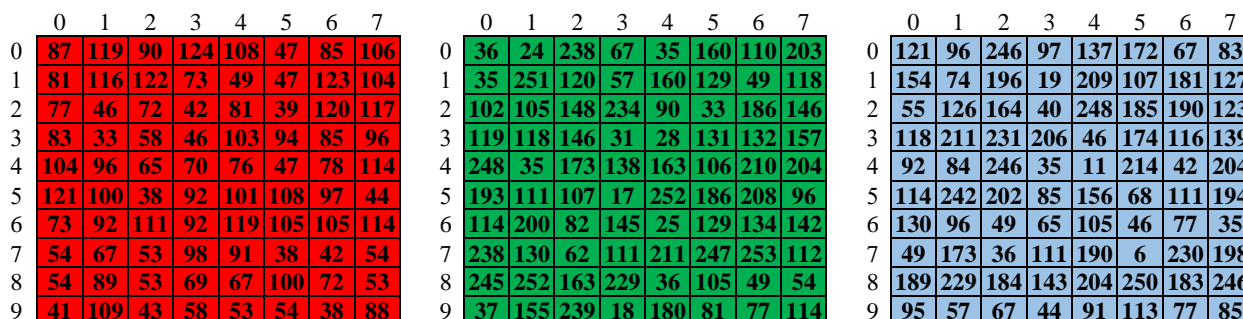


Figure 2. Three matrices of the coloured image

Each character after converting it to the ASCII code will be encoded into a value represented by a location (row and column), and since the values of the selected rows and columns are different in relation to the number of digits that represent the value. Image size will be variable, so we will represent a value of eight places, (four places for the row and column) and will be represented, each character represents in 9 as shown in Algorithm 2. Encoding character = S_1 bytes & R_4 bytes & C_4 bytes

$$S = \begin{cases} 0 & \text{if image selection is Red} \\ 1 & \text{if image selection is Green} \\ 2 & \text{if image selection is Blue} \end{cases} \quad (1)$$

Algorithm 2: Proposed Coding Operation

Input: image dimension r,c and the random value g chosen in the algorithm (1)

Output: Encoding location E of Pixel

Define two variables r_r,c_c//where r_r represent row and c_c represent colour

- 1: Start to compare the size of r // the size of r must be 4 digits
- 2: h=CTV(r) //where CTV means covert decimal value to character
- 3: If r < 10 then

```

4:  r_r='000'&h //Symbol (&) mean's append two
    characters
5:  Elseif r < 100 then
6:    r_r='00'&h
7:  Elseif r < 1000 then
8:    r_r='0'&h
9:  else
10: r_r=h
11: End if
10: Repeat steps 2 to step 10 to evaluate c_c with replace
    r_r to c
11: E=g & r_r & c_c //append color image, row and
    column

```

For example, let the plain text is “CoM19\$”, let the image size is 10×8, Figure 2 shows the 3 matrices showing the channels of the image (Red, Green, Blue).

Level1: Get the ASCII code for each character in the password “CoM19\$”.

Level2: Create three matrices for coloured image, as denoted in Figure 2.

Level3: looking for the value of each ASCII code we got from level1 inside the matrices we got from level2, firstly, the

password "CoM19\$" is consists of (C, o, M, 1, 9, \$), for each ASCII code (67, 111, 77, 49, 57, 35) looking for each ASCII value in matrices, "67" is found in Red matrix in position (7,1) and (8,4), in Green matrix in position (0,3), in Blue matrix in (0,6) (9,2), repeat the looking for all other codes, Table 1, shows the new table we got from level3.

Table 1. ASCII's location in the coloured image

Character	ASCII	Red	Green	Blue
C	67	[7,1], [8,4]	[0,3]	[0,6], [9,2]
o	111	[6,2]	[5,1], [7,3]	[5,6], [7,3]
M	77	[2,0]		[6,6], [9,6]
1	49	[1,4]	[1,6], [8,6]	[7,0], [9,1]
9	57		[1,3], [3,7]	[9, 1]
\$	35		[0,4], [4,1], [1,0]	[4,3], [6,7]

Table 2 shows selecting one random location for each ASCII that got from the previous table for each letter then encode the character to location Pixel values, where (Red=1, Green=2, Blue=3), so the cipher text will be: (200000003100060002200090006300070000100090001200040001)

Table 2. Encode character to location Pixel values

Plain Character	Image Channel	Location	Encode character to location Pixel values	
			Array converter	Byte converter
C	Green=2	[0, 3]	2, 0, 3	200000003
o	Red=1	[6, 2]	1, 6, 2	100060002
M	Green=2	[9, 6]	2, 9, 6	200090006
1	Blue=3	[7, 0]	3, 7, 0	300070000
9	Blue=3	[9, 1]	3, 9, 1	100090001
\$	Green=2	[4,1]	2, 4, 1	200040001

3.2 Decryption strategy

The decryption process will be done as shown in Figure 3, First of all, the image will be read, then divided into colours and then the decryption process of the ciphertext will begin. The text will be divided into segments of 9 bytes, the first byte representing the colour of the image. The remainder part represents the row and column number and the intersection between them represents the ASCII code of the character.

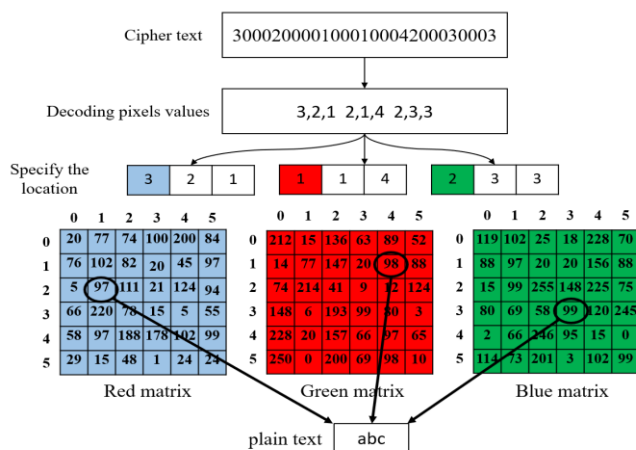


Figure 3. The proposed decryption algorithm

3.3 Specification of key image

The key adopted in the proposed algorithm is a set of images agreed upon in advance between the sender and the recipient, where the size and type of images will be determined by the user of the algorithm. In the proposed algorithm, the image size can reach (9999×9999) taking into account the image specifications like the parameters of histogram, entropy and correlation.

4. ANALYSIS AND SECURITY

The proposed algorithm was implemented on a laptop running Windows 11 with an Intel core i5-3110M CPU, 2.40 GHz and 16 GB memory. We used the Python programming language to implement the algorithm. The encryption time of 1126 symbols (abstract of this paper) are just 0:140 seconds; the decryption time is 0:109 seconds. Therefore, the algorithm proposed is fast to encrypt text and it can be implemented in real time application in this section we briefly discuss some security tests and their results for the proposed algorithm as well as a comparison of the security of the proposed algorithm and some of the existing text cipher schemes.

4.1 Brute force attack

To decrypt the ciphertext, cryptanalysts use a brute force attack method, resistance to this attack is by using key spacing, which is the upper limit of the algorithm's security. Key spacing is defined as the number of distinct secret keys it can generate. The cipher is secure if the key spacing is at least 2100 [21]. The proposed algorithm uses an image that acts as a key to encode the message based on its dimensions, so the key size is 2^{r*c*3} , The dimensions of the row (r) and column (c) will be variable according to the size of the image used for encryption, and this gives the algorithm the power to counteract a brute force attack. If we assume that the image dimensions are 100×100, the value of the key spacing will be 230000.

4.2 Known plaintext attack

This type of attack is an attempt by a cryptanalyst to find out the secret key or to develop an algorithm that enables it to decrypt any message after knowing or having access to the ciphertext and its corresponding plaintext [22]. In the proposed scheme, the text is encrypted with locations from an image randomly and the image is also randomly selected during session creation, the attacker will try to find a relationship between the encoding of each character of the text with the numbers from the ciphertext but it will not find any relationship because the numbers that were used for the encryption are chosen randomly in every encryption process.

4.3 Secret key sensitivity analysis

In the concept of encryption, when the same key is used on a text or a simple change in the text or the key, the output of the encryption process must be completely different [23]. In Table 3 the same image is used to encrypt the same text, the text that has been encrypted using the same key does not show any similarity, even if there is a similarity this is due to randomness in the selection of sites, and therefore the proposed system is sensitive to the secret key.

Table 3. Secret key sensitivity analysis


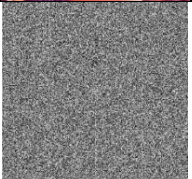
Image key	Plain text		Cipher text
	1234567890ABCD EF1234567890AB CDEF	1st session	002490040100410045200230088101270046200080035000090100102020120100 810079102420050200360178100940039101980143002330212101010191202420 203000690145002200201200890195100690
		2nd session	101050213102030029200110160001970244002220230000740188101550072100 200250100560012200380166001120007000220065100060068001510182201460 087101530012200050052201580150101870
	1234567890ABCD EF1234567890AB CDEF	1st session	201380021100630031201730064202510061000500226201660223000520158202 370239201310223202160067100350216002280243001330058100250254000350 254001050044000980111001210028201240
		2nd session	001210105100040253200030000202070238001170215200670084201730061102 380078100500170002230115101250218202190143000520014100470250101160 132101630236000600190200170145101020

Table 4. Comparison of the proposed algorithm with the other encryption algorithms

Algorithms	This work	Ref. [15]	Ref. [17]	Ref. [18]	Ref. [24]	Ref. [25]	Ref. [26]
Type of Key	image	text	text	text	text	text	text
Length of Key	dynamic	static	static	static	static	static	static
Entropy	yes	NA	NA	NA	yes	yes	NA
Chosen/known plain	yes	NA	NA	NA	yes	yes	yes
Secret keyspace	dynamic	Limited	Limited	Limited	limited	Limited	Limited
Randomness keys	Yes	NA	NA	NA	NA	NA	NA

4.4 Ciphertext only attack

The attacker cannot detect the plaintext if he owns the encryption algorithm and the ciphertext because applying brute force attack will not be very helpful because the key size is very big and this will take a long time even several years depending on the image size [27].

4.5 Comparison

The encryption process consists of 3 levels as shown in Figure 1, first convert each character in plain text to ASCII independently, then create 3 different tables by using cryptography system by a symmetric algorithm to encrypted images (red, green, blue), finally encoding ASCII by random indexing (row, column) for one of the encryption values in table.

The results obtained in Table 4 give the proposed method better results or a similar approach in term of Length of Key and other metrics such as Secret keyspace and for Chosen/known plain when compared with previous similar works for encryption text.

5. CONCLUSIONS

In this work, we proposed an algorithm for encoding plain text, that depends on the locations of the pixel values of the image, where the ASCII value of each character in the text is encoded with the value of the location that corresponds to the ASCII in the image represented by the line and column number of the location. Through the security analysis of the algorithm, numerical calculations of the relationship between the original data (the secret text) and the generated data (the encrypted image) prove that the generated data is completely different from the original data, and attackers cannot find useful information in the ciphertext. Besides, the secret key size is large to resist a violent attack, it can resist entropy attack, it creates a uniform histogram with low autocorrelation, it is

strong against classical attacks and this proves that it can be implemented in real applications of embedded systems. Moreover, the security strength of the proposed system was compared with the text encryption algorithms in Table 4. The comparison shows that the proposed scheme is more secure against modern cryptanalysis. The proposed approach can be used in many sensitive applications as it offers excellent encryption properties such as passwords, fingerprint template protection, voice fingerprint, File transferring and more, the future development of this work may investigate its use in authentication systems and the possibility of using a fingerprint instead of images to encrypt texts.

REFERENCES

- [1] ALRikabi, H.T.S., Hazim, H.T. (2021). Enhanced data security of communication system using combined encryption and steganography. *International Journal of Interactive Mobile Technologies (IJIM)*, 15(16): 144-157. <https://doi.org/10.3991/ijim.v15i16.24557>
- [2] ALattar, I.M., Rahma, A.M.S. (2021). A comparative study of research based on magic square in encryption with proposing a new technology. *Iraqi Journal of Computers, Communication, Control & Systems Engineering*, 21(2): 102-114. <https://doi.org/10.33103/uot.ijccce.21.2.8>
- [3] Herbadji, D., Derouiche, N., Belmeguenai, A., Herbadji, A., Boumerdassi, S. (2019). A tweakable image encryption algorithm using an improved logistic chaotic map. *Traitement du Signal*, 36(5): 407-417. <https://doi.org/10.18280/ts.360505>
- [4] Zahid, A.H., Al-Solami, E., Ahmad, M. (2020). A novel modular approach based substitution-box design for image encryption. *IEEE Access*, 8: 150326-150340. <https://doi.org/10.1109/ACCESS.2020.3016401>
- [5] Pekereng, M.A.I., Wowor, A.D. (2021). Square transposition: an approach to the transposition process in the block cipher. *Bulletin of Electrical Engineering and*

- Informatics, 10(6): 3385-3392. <https://doi.org/10.11591/eei.v10i6.3129>
- [6] Gong, L., Wang, M., Zuo, X., Li, S., Wang, D. (2019). Using transposition padding to get CCA2 security from any deterministic encryption schemes. *IEEE Access*, 7: 6765-6773. <https://doi.org/10.1109/ACCESS.2019.2891075>
- [7] Zhang, Y., Xu, C., Ni, J., Li, H., Shen, X.S. (2019). Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage. *IEEE Transactions on Cloud Computing*, 9(4): 1335-1348. <https://doi.org/10.1109/TCC.2019.2923222>
- [8] Ma, M., He, D., Khan, M.K., Chen, J. (2018). Certificateless searchable public key encryption scheme for the mobile healthcare system. *Computers & Electrical Engineering*, 65: 413-424. <https://doi.org/10.1016/j.compeleceng.2017.05.014>
- [9] Thinn, A.A., Thwin, M.M.S. (2019). Modification of AES algorithm by using the second key and modified subbytes operation for text encryption. In: Alfred, R., Lim, Y., Ibrahim, A., Anthony, P. (eds) *Computational Science and Technology. Lecture Notes in Electrical Engineering*, vol 481. Springer, Singapore. https://doi.org/10.1007/978-981-13-2622-6_42
- [10] Al-Khateeb, Z.N., Jader, M.F. (2020). Encryption and hiding text using DNA coding and hyperchaotic system. *Indonesian Journal of Electrical Engineering and Computer Science*, 19(2): 766-774. <https://doi.org/10.11591/ijeecs.v19.i2.pp766-774>
- [11] Azhar, S., Azam, N.A., Hayat, U. (2022). Text encryption using Pell sequence and elliptic curves with provable security. *Computers, Materials & Continua*, 71(3): 4972-4989. <https://doi.org/10.32604/cmc.2022.023685>
- [12] Murillo-Escobar, M.A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R.M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, 42(21): 8198-8211. <https://doi.org/10.1016/j.eswa.2015.06.035>
- [13] Singh, L.D., Singh, K.M. (2015). Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, 54: 73-82. <https://doi.org/10.1016/j.procs.2015.06.009>
- [14] Kumari, A., Kapoor, V. (2020). Competing secure text encryption in intranet using elliptic curve cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, 23(2): 631-641. <https://doi.org/10.1080/09720529.2020.1729509>
- [15] Mushtaq, M.A., Sultan, A., Afrasayab, M., Zubair, T. (2019). New cryptographic algorithm using ASCII values and gray code (AGC). In *Proceedings of the 2019 4th International Conference on Big Data and Computing*, pp. 242-246. <https://doi.org/10.1145/3335484.3335540>
- [16] Wadisman, C., Nozomi, I., Rahmawati, S. (2021). Implementation of cryptography Merkle-Hellman knapsack combination, discrete algorithm and ASCII table modification for PHP source code security. In *IOP Conference Series: Earth and Environmental Science*, 704(1): 012044. <https://doi.org/10.1088/1755-1315/704/1/012044>
- [17] Thakral, P., Goyal, K., Kumar, T., Garg, D. (2018). Transfusion of extended Vigenere table and ASCII conversion for encryption contrivance. In: Abraham, A., Gandhi, N., Pant, M. (eds) *Innovations in Bio-Inspired Computing and Applications. IBICA 2018. Advances in Intelligent Systems and Computing*, vol 939. Springer, Cham. https://doi.org/10.1007/978-3-030-16681-6_4
- [18] Dharshini, M., Gayathri, K., Devi, S.R., Gopalakrishnan, B. (2021). Refined imbricate cryptography with the addition of polygram substitution cipher method: An enhanced tool for security. In *Journal of Physics: Conference Series*, 1767(1): 012048. <https://doi.org/10.1088/1742-6596/1767/1/012048>
- [19] Hassan Aziz, E. (2020). Two stage text encryption using a private table of the Sumerian system. *Kirkuk University Journal-Scientific Studies*, 15(1): 18-33. <https://doi.org/10.32894/kujss.2020.15.1.2>
- [20] Elshoush, H.T., Ali, I.A., Mahmoud, M.M., Altigani, A. (2021). A novel approach to information hiding technique using ASCII mapping based image steganography. *Journal of Information Hiding and Multimedia Signal Processing*, 12(2): 65-82.
- [21] Jirjees, S.W., Mahmood, A.M., Nasser, A.R. (2022). Passnumbers: An approach of graphical password authentication based on grid selection. *International Journal of Safety and Security Engineering*, 12(1): 21-29. <https://doi.org/10.18280/ijss.120103>
- [22] Cai Q.R. (2019). A secure image encryption algorithm based on composite chaos theory, *Traitement du Signal*, 36(1): 31-36. <https://doi.org/10.18280/ts.360104>
- [23] Salman, L.A., Hashim, A.T., Hasan, A.M. (2022). Selective medical image encryption using polynomial-based secret image sharing and chaotic map. *International Journal of Safety and Security Engineering*, 12(3): 357-369. <https://doi.org/10.18280/ijss.120310>
- [24] Murillo-Escobar, M.A., Abundiz-Pérez, F., Cruz-Hernández, C., López-Gutiérrez, R.M. (2014). A novel symmetric text encryption algorithm based on logistic map. In *Proceedings of the International Conference on Communications, Signal Processing and Computers*, pp. 49-53.
- [25] Naji, M.A., Hammood, D.A., Atee, H.A., Jebur, R.S., Rahim, H.A., Ahmad, R.B. (2020). Cryptanalysis cipher text using new modelling: Text encryption using elliptic curve cryptography. In *AIP Conference Proceedings*, 2203(1): 020003. <https://doi.org/10.1063/1.5142095>
- [26] Singh, L.D., Singh, K.M. (2015). Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, 54: 73-82. <https://doi.org/10.1016/j.procs.2015.06.009>
- [27] Jiao, S., Lei, T., Gao, Y., Xie, Z., Yuan, X. (2019). Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging. *IEEE Access*, 7: 119557-119565. <https://doi.org/10.1109/ACCESS.2019.2936119>