ISSN: 0067-2904

Robust Password Encryption Technique with an Extra Security Layer

Qusay Zuhair Abdulla*, Mustafa Dhiaa Al-Hassani
Computer Science Dept., Collage of science, Mustansiriyah University, Baghdad, Iraq

Received: 19/3/2022 Accepted: 26/7/2022 Published: 30/3/2023

Abstract

People are comfortable with e-banking services, but they are exposed to a great deal of danger these days due to fraudulent acts such as password hacking and personal information theft. Everything individuals do online relies heavily on passwords. Using a password protects one's identity online, in forums, and through email. Online transactions are vulnerable to identity theft if they do not have a secure password. Internet users with critical statements are vulnerable to various assaults, including the theft and exploitation of user IDs and passwords. This paper introduces novel password encryption by fingerprint and a random number to make each password unique and robust against attacks, with a magnificent time elapsed of under 40 milliseconds. This paper uses global password datasets with different stages of password complexity. This method protects the bank's clients' password accounts inside the bank database.

Keywords: E-banking, cybersecurity, Encryption, Decryption, Security, Authentication.

تقنية تشفير كلمات مرور قوية مع طبقة أمان إضافية

قصي زهير عبدالله*, مصطفى ضياء الحسني
قسم علوم الحاسوب, كلية العلوم, الجامعة المستنصرية, بغداد, العراق

الخلاصة

يشعر الناس بالراحة تجاه الخدمات المصرفية الإلكترونية ؛ ولكن يتعرضون لقدر كبير من الخطر هذه الأيام بسبب أعمال احتيالية مثل اختراق كلمة المرور وسرقة المعلومات الشخصية. كل ما يفعله الأفراد عبر الإنترنت يعتمد بشكل كبير على كلمات المرور. يؤدي استعمال كلمة مرور إلى حماية هوية الفرد عبر الإنترنت وفي المنتديات وعبر البريد الإلكتروني. تكون المعاملات عبر الإنترنت عرضة لسرقة الهوية إذا لم يكن لديها كلمة مرور آمنة. مستخدمو الإنترنت الذين لديهم بيانات انتقادية معرضون للاعتداءات المختلفة ، بما في ذلك سرقة واستغلال معرفات المستخدمين وكلمات المرور. تقدم هذه الورقة تشفيرًا جديدًا لكلمة المرور عن طريق بصمة الإصبع ورقم عشوائي لجعل كل كلمة مرور فريدة وقوية ضد الهجمات ، مع مرور وقت رائع أقل من 40 مللي ثانية. يستعمل هذا البحث مجموعة بيانات كلمات مرور عالمية بمراحل مختلفة من تعقيد كلمة المرور. تحمي هذه الطريقة حسابات كلمات المرور لعملاء المصارف داخل قاعدة بيانات المصرف.

*Email: qusayzuhairabdulla@gmail.com

1. Introduction

In recent years, people have utilized the Internet to send and store critical information such as medical records and banking accounts. The Internet is a convenient means of data transmission. However, it is risky since the data is accessible and may be obtained by hackers for illicit reasons such as fraud and theft. Critical information needs to be safe, and just the authorized person can access it; that means using the password to protect the information and authentication the owner of this information [1] [2].

E-banking is the most critical sector in daily business operation, with massive money exchange in this sector; banks use the internet to make these operations more fixable and more manageable; however, when using the internet, all the critical information will be un-secure the unauthorized party trying to hack this information [3]. The essential information is the clients' password; this means it needs to be secure and more confidential [4]. According to the importance of this sector, many threads and vulnerabilities appear [5]. Biometric and knowledge-based procedures are now the primary means of securing access to information. Smart cards and key cards are tokens; biometrics, on the other hand, are those features that are unique to each individual. While these systems are effective, their principal drawback is the high cost of deployment.

In order to safeguard sensitive data from eavesdroppers and intruders, an individual's identity must be verified and validated. In the same way, hackers may readily guess them, making them vulnerable to dictionary assaults and other common attacks [6] [7]. Biometrics is a term used to describe measures that may identify an individual, either manually or automatically [8]. A computerized system that can identify people is the primary objective of biometric identification or verification. A fingerprint is one such biometric that has all of these characteristics. As a result, fingerprint recognition systems are among the most widely used and widely deployed biometric identification or verification systems [9] [10].

It is possible to categorize random integers depending on where they are generated from. Natural events like radioactive decay, the makeup of gases in the air, and electrical noise produce random numbers. Algorithms with high complexity and unpredictability may also produce random numbers. Deterministic sequences, which create deterministic sequences that are not random but may substitute random numbers in specific cases, are also available as LCG (Linear congruential generator) [11] [12].

A password is essential to give authentication to a person who has it. Still, when saved in a database or password file, the plain password is easy to hack and use by unauthorized people. However, many researchers work on password encryption to improve the security of stored passwords. This paper introduces a novel method to encrypt the password and add an extra layer of protection. The proposed method applies to a global dataset filtered by a multi-stage of complexity. This paper uses passwords with a length of between 8 and 48 characters. This dataset contains real-world passwords used by clients and is available on the Kaggle site. The following sections explain the methodology, the proposed method structure, and the results in the discussion.

2. Related work

Neither the idea nor its execution is novel nor innovative in any way. After proposing the Authentication Method for Password Encryption, we found that several existing implementations are very similar to our proposed system. Finding a viable solution to data encryption is the goal of our research. This paper did enough research to back up our findings. AES, DES, RSA, Diffie-Helman, play fair method, discrete algorithm attack, Man-in-the-

middle assault, Guess attack, Dictionary attack, Random sequences, etc., have all been explored in depth by our team.

A technique for creating three-dimensional things using the Unity 3D software is proposed. Epic motion software then watches the user's hand or finger on these selected/chosen things and provides a visual representation. As a result of this selection process, a unique client password was generated by a proprietary algorithm [13].

After completing all the procedures, they have encrypted and decrypted a text file (a user-supplied encrypted text file). Their method is highly effective. The deciphered message (text) is identical to the original message. They have produced a fruitful outcome. It is complicated to match the three parameters (randomization number, encryption number, and shift parameter) for two different texts. In order to break the encryption method, an intruder must confirm the exact pattern of the text key. Even if someone implements the BFS method, he must provide trail 256! Absurd Times. Because the matrix of the encryption key is 16 by 16, the total number of elements in the matrix is 16*16 = 256 [14].

In [15], the researchers present a two-step verification mechanism for smartphone user identification. First is the standard text-based graphic password. Second, as a password, a session-based 3D graphic in which items move. In order to prevent guessing and dictionary attacks, which are disadvantages of standard text-based authentication, they have incorporated a 3D visual environment and movement as an extra step in securing passwords.

3. Proposed method

As mentioned in the previous section, the possibility of applying attacks to hack the password and gain the authentication to access critical information leads to the introduction of a robust method to encrypt the password with an extra security layer. The proposed method structure contains several steps and sub-methods. It begins with entering the plain password and reading the fingerprint from the customer's hand. The second step applies the password equation that contains the ASCII code of characters from the plain password sum with character index; the result becomes the right part, and the left part comes from the Forward District Cosine Transform (FDCT); the AC value is taken to become the left side. Now the right and left sides are available for summation. They generate a seed for the next step. The third step is to apply the LCG algorithm to generate a random number; in this paper, it is five digits only as a PIN code, and then convert it to binary. The fourth step contains a fixed binary string 400 bits in length; approximately equal zeros and ones will concatenate with the binary pin code; the final string is a concatenation between the binary PIN and the fixed binary string. The final step converts the plain password to binary form, then XORs it with the binary string that comes from the previous step, producing an encrypted password. Figure 1 shows the method structure:

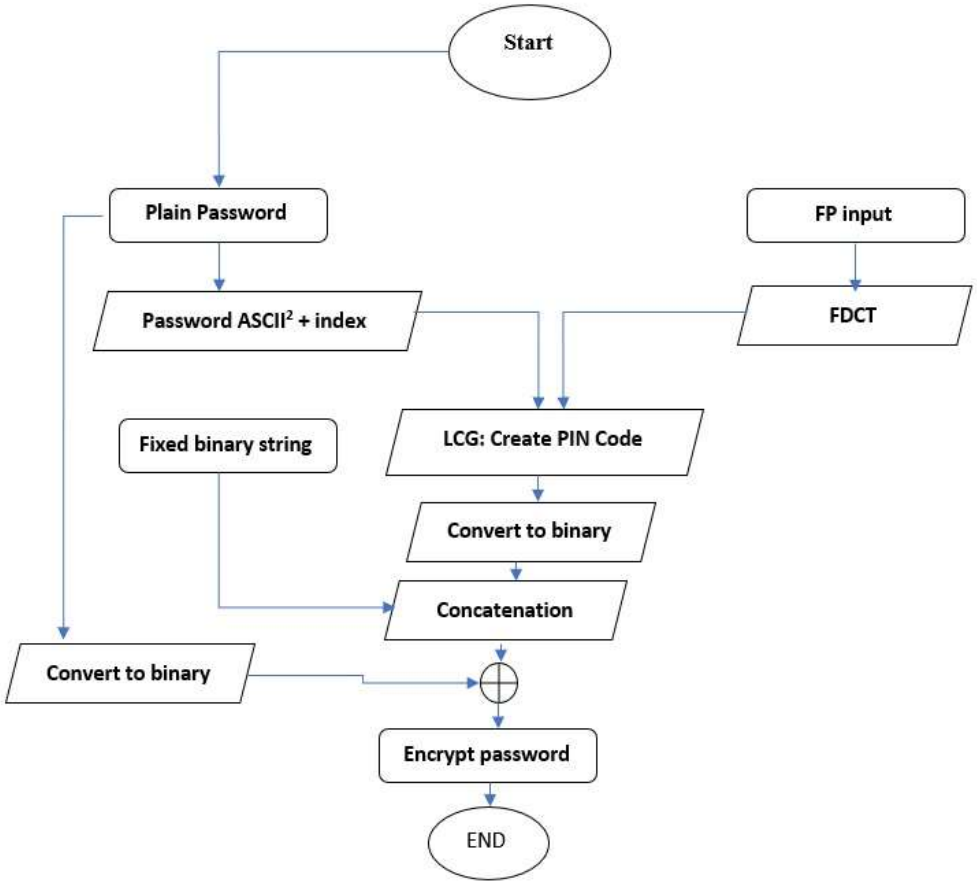

Figure 1: Proposed method Encryption Mode

Proposed method Encryption Mode
Input: Password, Fingerprint
Output: Encrypted Password
Begin Step 1: Read password Plain_Psw Step 2: Read fingerprint Step 3: Calculate the equation: Seed_1 = (ASCII_Psw_Val) ^{2} + Index_Psw Step 4: Apply FDCT on fingerprint image return AC value as Seed_2 Step 5: Generate PIN Code (Personal Identification Number) as PIN_Code by LCG with Seed: Seed = Seed_1 + Seed_2 Step 6: Convert PIN_Code value to binary as PIN_Code_Bin Step 7: Generate PIN_Key_Bin by Concatenation between binary PIN_Code_Bin and Fixed binary string Fix_Bin Step 8: Convert Plain_Psw to binary as Plain_Psw_Bin Step 9: XOR between Plain_Psw_Bin with PIN_Key_Bin Step 10: Encrypted password Enc_Psw End

Where:
Plain_Psw: Plain password get from the user
Seed_1: First part of LCG Seed
ASCII_Psw_Val: ASCII code value of each character
Index_Psw: Value of individual character index
Seed_2: Second part of LCG Seed

Fix_Bin: 400 bits approximately equally zeros and ones

The algorithm's proposed method had a different step (password handling, fingerprint handling, fixed binary string, PIN Code Generator). The following section explains all these steps in detail.

2.1 Password handling Equation

The password should be written according to the most common standard, and the password should be more than eight characters and a combination of (numbers, upper letters, special characters). Each character should be handled by extracting the ASCII (American Standard Code for Information Interchange) code for each character and its index, as shown in equation 1, with the ASCII Code table in [16] applied as a reference.

$$Password\ Handeled = \text{ASCII\_Psw\_Val}^2 + \text{Index\_Psw} \quad (1)$$

This equation handled the index of the character to give the unique way for generating the final number by incremental the result of the equation for each character. To provide a clear view of the equation, table 1 shows the unique number even if it had the same character but in a different order written in the password field:

Table 1: Password handled behavior

Password	$Password\ Handeled = \text{ASCII\_Psw\_Val}^2 + \text{Index\_Psw}$
Dr123@00	33862
Dr321@00	67788
Dr00@123	101778
Dr00@321	135832

These unique numbers shown in Table 1 provide strong randomness to be used later as part of the seed in the LCG method to generate the random PIN code.

2.2 Fingerprint handled

Handling Pearson's fingerprint is based on steps according to [17]. The DCT used for this method is one-dimensional. Because one-dimensional processing of the block is faster than two-dimensional processing, the compression and decompression processes are accelerated. The coefficients for each block that has undergone DCT transformation are arranged according to their significance, with coefficients holding the most valuable information being designated as the DC component and being located in the block's upper left corner; the remaining coefficients, which are represented as AC, hold the block's less critical information [17] [18]. The 1D-DCT can be generated by applying the equation (2) to convert the pictures, and then applying the equation (3) to reverse the transformation to yield the reconstructed image.

$$F(u) = C(u) \sum_{x=0}^{N-1} f(x) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (2)$$

Where, N is the input block length, u=0, 1, ……. N-1

$C(u)=\sqrt{\frac{2}{N}}$ when u≠0 $C(u)=\sqrt{\frac{1}{N}}$ when u=0

$$F(x)=C(u)\sum_{u=0}^{N-1} F(x)\cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (3)$$

$C(u)=\sqrt{\frac{2}{N}}$ when u≠0 $C(u)=\sqrt{\frac{1}{N}}$ when u=0

Where f(x) is the input matrix.

AC value combined with value came from Password handling to be the seed for next step.

2.3 Create PIN Code

The most crucial step is to create a PIN code; it is an extra security layer to increase the robustness of the proposed encryption method. This PIN is used later in decryption mode. As mentioned, the LCG method should generate the PIN code according to the seed produced from a combination of two values explained previously. LCG generates a massive number. This paper requires just five digits only. Table 2 shows the behavior of the PIN code for ten different passwords for the same fingerprint:

Table 2: PIN code behavior

Password	PIN code
kzde5577	17876
kino3434	21412
megzy123	89030
u6c8vhow	78611
v1118714	38479
as326159	39636
asv5o9yu	54525
idofo673	46093
fk9qi21m	31768
fahad123	20411

According to the results in Table 2, PIN code behaviors are unique in each password for the same fingerprint, increasing the proposed method's robustness. However, at this point, we have checked over 100 different passwords with different stages of complexity, and the proposed method is stable with a unique PIN code generator.

4. Decryption mode

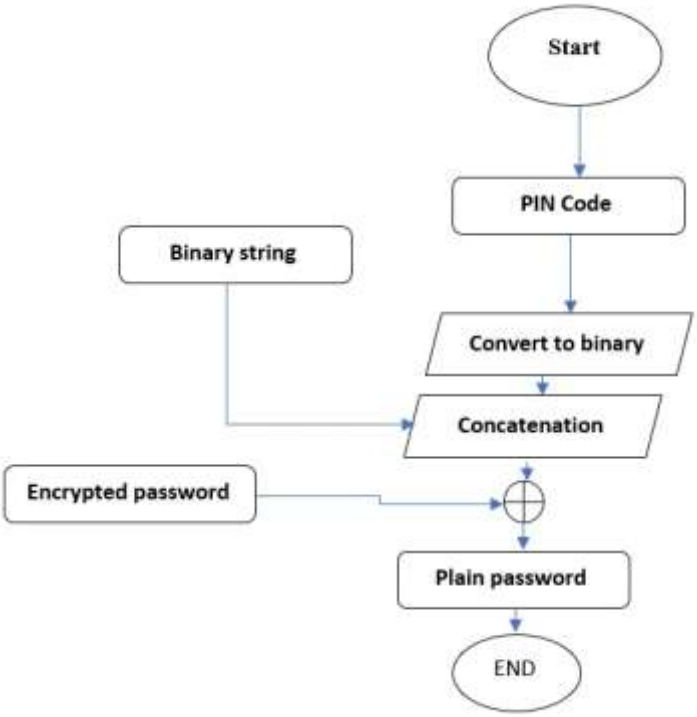

Figure 2: Decryption Mode

Proposed method Decryption Mode
Input: Encrypted Password, PIN Code
Output: Plain Password
Begin Step 1: Encrypted Password Enc_Psw Step 2: Enter PIN_Code Step 3: Convert PIN_Code to binary as PIN_Code_Bin Step 4: Concatenation between PIN_Code_Bin and Fix_Bin to create PIN_Key_Bin Step 5: Convert Enc_Psw to binary as Enc_Psw_Bin Step 6: XOR Enc_Psw_Bin with PIN_Key_Bin Step 7: Plain Password Plain_Psw End

In decryption mode, applying the algorithm steps begins with an encrypted password and PIN code as an input, then converts the PIN code to binary and concatenates with a fixed binary string, converts the encrypted password to binary, and finally XORs with the combination of PIN and fixed binary string to produce the plain password.

5. Result discussion

After explaining the proposed method steps and requirements in detail, it is now time to discuss the result according to two metrics (Hamming distance and Balanced Output).

4.1 Hamming distance

When two strings of identical length are compared, the Hamming distance is the number of spots where the related symbols differ. Another way of looking at it is to measure the lowest number of substitutes or the smallest number of faults that may have allowed that to happen.

[19] [20]. Table 3 shows the hamming distance applied to the result by using the same passwords in Table 2 to calculate Hamming distance based on the ASCII code of the plain and encrypted passwords.

Table 3: Hamming distance result

Plain password ASCII	Encrypted password ASCII	hamming distance
107,122,100,101,53,53,55,55	224,211,33,48,40,96,125,221	8
107,105,110,111,51,52,51,52	204,32,43,58,46,97,121,222	8
109,101,103,122,121,49,50,51	192,134,54,47,62,100,96,137	8
117,54,99,56,118,104,111,119	236,191,178,109,49,61,61,205	8
118,49,49,49,56,55,49,52	224,126,147,155,182,157,148,65	8
97,115,51,50,54,49,53,57	251,167,145,152,184,155,144,76	8
97,115,118,53,111,57,121,117	181,142,212,159,225,147,220,0	8
105,100,111,102,111,54,55,51	221,105,205,204,225,156,146,70	8
102,107,57,113,105,50,49,109	158,90,124,36,116,103,123,135	8
102,97,104,97,100,49,50,51	249,22,45,52,121,100,120,217	8

According to Table 3, hamming distance had the best result for the proposed method between plain and encrypted passwords. These passwords are for the same person using the same fingerprint. This means each time a password is changed, it should produce different encrypted passwords even with the same fingerprint. This gave more robustness to the proposed method and resistance against attacks.

4.2 Balanced Output

The output with a mixture of 1s and 0, the quantity of 1s and 0s should be nearly equal [21]. Calculate the Balanced output for Encrypted passwords. An ASCII code should be converted to a binary value. Table 4 is built based on Table 3 encrypted password ASCII code information.

Table 3: Balanced Output results

Encrypted password	Binary Value	Zero's count	One's count
224,211,33,48,40,96,125,221	11100000110100110010000100110000001010000110000001111101111011101	36	28
204,32,43,58,46,97,121,222	11001100001000000010101100111010001011100110000101111001111011110	33	31
192,134,54,47,62,100,96,137	11000000100001100011011000101111001111100110010001100001001001	37	27
236,191,178,109,49,61,61,205	11101100101111111011001001101101001100010011111011001101111001101	25	39
224,126,147,155,182,157,148,65	11100000011111101001001110011011101101101001110110010100001000001	31	33
251,167,145,152,184,155,144,76	11111011101001111001000110011000101110001001101110010000001001100	32	32
181,142,212,159,225,147,220,0	10110101100011101101010010011111111000011001001111011100000000000	32	32
221,105,205,204,225,156,146,70	11011101011010011100110111001100111000011001110010010010000110	31	33
158,90,124,36,116,103,123,135	10011110010110100111110000100100011101000110011011111000000111	29	35
249,22,45,52,121,100,120,217	11111001000101100010110100110100011110010110010011110001100001	31	33

Based on the results in table 4, the proposed method had an approximately equal output of zeros and ones. This metric shows promising outcomes with approximately mixed binary values.

6. Conclusion

Passwords are the most significant way to apply authentication and recognize the authenticated person, making unauthorized parties seek to gain these passwords. The importance of passwords in real-world work includes personal accounts, E-mail accounts, and E-banking accounts. The E-banking industry is the most significant organization to protect clients' accounts from unauthorized parties gaining access to their passwords. As mentioned early in this paper, the researchers recommended encryption to secure the passwords and gain more confidentiality. This paper introduces a novel method with an extra security layer to encrypt passwords using a biometric feature (fingerprint) to generate a PIN code as an extra security layer. The point of the PIN code is that if an unauthorized party gains the password, it is not helpful because, without a PIN code, the encrypted password cannot be decrypted. The proposed method works on a global dataset with real-world passwords filtered by the level of complexity. To evaluate the proposed method in this paper, we apply the Hamming distance and balanced output as evaluation metrics. The metric that evaluates the results shows promising results.

References

[1] J. H. C. V. O. P. a. S. F. Bonneau, "The quest to replace passwords: a framework for comparative evaluation of web authentication schemes," *IEEE Symposium on Security and Privacy* (SP), p. 553–567, 2012.

[2] E. S. I. Harba, "Advanced Password Authentication Protection by Hybrid Cryptography & Audio Steganography," *Iraqi Journal of Science*, vol. 59, no. 1C, pp. 600-606, 2018.

[3] A. H. M. Sajaa G. Mohammed, "Efficient Plain Password Cryptanalysis Techniques," *Iraqi Journal of Science*, vol. 58, no. A4, pp. 1946-1954, 2021.

[4] M. P. L. A. Vrîncianu, "Considerations regarding the security and protection of e-banking services consumers' interests," *The Amfiteatru Economic Journal*, vol. 12, no. 28, p. 388–403, 2010.

[5] L. H. M. D. D. B. M. D. F. G. T. d. S. R. Peotta, "A formal classification of internet banking attacks and vulnerabilities," *International Journal of Computer Science and Information Technology*, vol. 3, no. 1, p. 186–197, 2011.

[6] V. S. Sanket Prabhu, "Authentication Using Session Based Passwords," *Procedia Computer Science*, vol. 45, pp. 460-464, 2015.

[7] N. Ali, "A four-phase methodology for protecting web applications using an effective realtime technique," *Int. J. Internet Technology and Secured Transactions*, vol. 6, no. 4, p. 303–323, 2016b.

[8] M. a. R. M. a. S. J. H. a. Y. M. a. F. S. L. Sharif, "*An overview of biometrics methods," Handbook of Multimedia Information Security: Techniques and Applications*, pp. 15--35, 2019.

[9] C. L. a. J. K. Yeegahng Song, "A new scheme for touchless fingerprint recognition system," Proceedings of 2004 *International Symposium on Intelligent Signal Processing and Communication Systems*, 2004, pp. 524-527, 2004.

[10] W. a. W. S. a. H. J. a. Z. G. a. V. C. Yang, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.

[11] D. M. S. Naik, "Generation of Random Numbers Using LCG and Faure Sequence," *International Journal of Research and Analytical Reviews*, vol. 7, no. 2, pp. 840-843, 2020.

[12] B. Tiwari, "Image Encryption using Pseudo Random Number Generators," *International Journal of Computer Applications*, vol. 67, no. 20, pp. 1-8, 2013.

[13] I. a. L. H.-n. a. F. C. Olade, "A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays," 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 1997-2004, 2018.

[14] A. S. G. a. M. A. M. Nath, "Symmetric Key Cryptography Using Random Key Generator," in Proceedings of the 2010 *International Conference on Security & Management, Las Vegas, Nevada*, USA, pp. 234-242, 2010.

[15] B. S. a. F. I. Q. Yerne, "Design 3D Password with session based technique for login security in Smartphone.," *Online International Conference on Green Engineering and Technologies* (IC-GET). IEEE, pp. 1-4, 2016.

[16] Y. B. R. A. a. W. A. A. Elmogy, "A New Cryptography Algorithm Based on ASCII Code," *International Conference on Sciences and Techniques of Automatic Control and Computer Engineering* (STA), pp. 626-631, 2019.

[17] E. K. H. S. G. M. a. F. G. M. L. E. George, "Selective Image Encryption Based on DCT, Hybrid Shift Coding and Randomly Generated Secret Key," *eijs*, vol. 61, no. 4, pp. 920-935, 2020.

[18] D. C. Transform, *Ochoa-Dominguez, Humberto and Rao, Kamisetty Ramamohan, CRC Press*, 2019.

[19] J. M. G. Maram K Balajee, "Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output," *TEM Journal*, no. 1, pp. 67-75, 2016.

[20] A. a. K. V. A. a. R. T. Bookstein, "Generalized hamming distance," *Information Retrieval*, vol. 5, no. 4, pp. 353--375, 2002.

[21] H. V. L. D. V. V. Halagali B P, "Designing The S Boxes of Blowfish Algorithm using Linear Congruential Generator," *ASM's International e-journal of Ongoing Research in Management and IT*, pp. 1-13, 2013.