Chaos-based Protection Data for Digital Communication

Belqassim Bouteghrine
Lcoms
Université de Lorraine
Metz, France
email:belqassim.bouteghrine@univ-lorraine.fr

Camel Tanougast
Lcoms
Université de Lorraine
Metz, France
email:camel.tanougast@univ-lorraine.fr

Said Sadoudi
Laboratoire Télécommunications
Ecole Militaire Polytechnique
Algiers, Algeria
email:sadoudi.said@gmail.com

Mohammed Rabiai
Laboratoire Télécommunications
Ecole Supérieure Ali Chabati
Reghaia, Algeria
email:mohammed.rabiai2013@gmail.com

***Abstract*—Due to advancements in digital technologies in recent years, the security of exchanged data has become the most attractive topic for many researchers. Consequently, several cryptography schemes have been introduced and proposed for securing the exchanged sensitive data in the network. In this paper, we propose new chaos-based protection in order to secure both the exchanged identity text and the image data. In addition, we applied the proposed encryption to secure the exchanged heterogeneous data inside a C# chat application. The analysis of the simulation results shows that the proposed scheme offers a better performance in terms of security and robustness than some similar schemes.**

***Keywords*—data security; cryptography; chaos; C# application.**

I. INTRODUCTION

With the advent in Internet and networking applications, security becomes a major concern in the current era of information technology. The security threats and attacks are increased due to the huge amount of exchanged data over the network. As a solution to these threats, information security is a well known proposal which provides protection to data availability, privacy, and integrity [1]. Moreover, data encryption is considered as the most traditional technique that secures highly confidential information by using some conventional algorithm, which already exists [2]. Looking for more flexibility and security, Saraf et al. [3] have proposed an AES(Advanced Encryption Standard)-based encryption and decryption for text and image data. For text encryption, 128-bit text inputs are synthesized and simulated using a code composer studio tool in C developing language code. For image encryption, a Java developing language code is synthesized and simulated by Java Application Platform. By combining the AES and the Elliptic Curve Cryptography (ECC), [4] proposes an extension of a public-key-based cryptosystem. To overcome the drawbacks shown in the traditional 128-AES, the introduced scheme proposes a hybrid encryption system including ECC and AES schemes. The optimized technique includes a trade-off between the key space (192 bit) and the number of iterations (12). For text encryption application, a new technique has been proposed in [5]. The proposed new technique addresses the leak of mapping the characters to refine points in the elliptic curve showed in classic techniques. The main idea of this solution is to pair values of plain text and corresponding ASCII to serve as input for the elliptic curve based encryption. The proposed algorithm is designed to be used for encryption and decryption of exchanged text data. In [6], Singh et al. presented a new encryption scheme based on symmetric key encryption. The proposed algorithm converts the plain text to get the corresponding ASCII values, which are considered as the input text of the cryptosystem. Similarly, the decryption process starts also by converting the cipher text to ASCII values which will be the input of this process. In [7], Chandra et al. proposed double encryption, which is a content-based algorithm that implements a folding method and a circular bit-wise operation. In this technique, encryption of plaintext occurs two times with a secret key, providing cipher text by using a circular bit-wise binary addition operation. Another concept based on double encryption is proposed in [8] to provide high level of security. In this technique, the plaintext is encrypted by an encryption technique using a secret key, which is also encrypted by another algorithm. Then, the plaintext is encrypted again using the encrypted secret key. However, all of these proposals suffer from key distribution and resources consumption, which make them less suitable for constrained devices and real time applications [9]. Moreover, more complex schemes have been highlighted by many studies proving their high computational cost, which affects mainly the resource-limited devices that are included in the new networks [10].

One of the advanced cryptography techniques is Attribute-Based Encryption (ABE), which was introduced to overcome the limited functionalities of the traditional public key cryptography schemes [11]. However, in multi-authority systems, many complicated issues can be experienced when the ABE systems are built (revocation problem) [12]. For example, to tie the work of all authorities together, some existing systems use a central authority, which can cause a bottleneck problem and is contradictory to the distributed control principle [12].

Nowadays, chaotic encryption method seems to be much better than traditional encryption methods [13]. Chaos-based schemes have introduced the use of chaotic system properties such as sensitivity to initial condition and loss of information. Therefore, many chaos-based encryption methods have been presented and discussed in the last decades. Moreover, Babaei [14] included a logistic chaotic map as an input of a One-Time-Pad algorithm (OTP) for image encryption application. In addition, for text files encryption, authors have proposed a new algorithm based on a chaotic selection between original message strands and OTP DNA strands [14]. The obtained result of the proposed solution proved the efficiency of the proposed algorithm in both image and text encryption. However; all these schemes have shown some shortcomings regarding the key space offered by the chaotic system and the robustness of the used chaotic system. Hence, unlike all the previous proposals, we introduce through this paper a novel and dynamic chaos-based cryptosystem in order to secure both the exchanged identity text and the image data. In addition, we applied the proposed cryptosystem for secure exchanged heterogeneous data inside a C# application. Therefore, the main contributions of this paper are as follows: (i) A new four-dimensional (4-D) chaotic system that shows good chaotic properties; (ii) A new and a simplified algorithm based on a chaos system and a hash function for multimedia data encryption purpose.

The rest of this paper is organized as follows. Section 2 gives the proposed chaotic system. Section 3 includes the application of the configurable chaos-based cryptosystem. Conclusion and some perspectives are given in Section 4.

II. The Proposed Configurable Cryptosystem

The proposed configurable chaos system is multidimensional system including several systems (2-D, 3-D and 4-D systems) that are extracted from our proposal given in [17].

The first system is a 2-D dimension described as follows:

$$\begin{cases} X(n+1) = 1 - a * X(n)^2 + Y(n) \\ Y(n+1) = d * X(n) \end{cases} \tag{1}$$

The 3-D system defined by five (05) nonlinear terms and three (03) controllers is described as follows:

$$\begin{cases} X(n+1) = 1 - a * X(n)^2 + (Y(n) * Z(n)) \\ Y(n+1) = 1 - b * Y(n)^2 + (X(n) * Z(n)) \\ Z(n+1) = d * X(n) * Y(n) \end{cases} \tag{2}$$

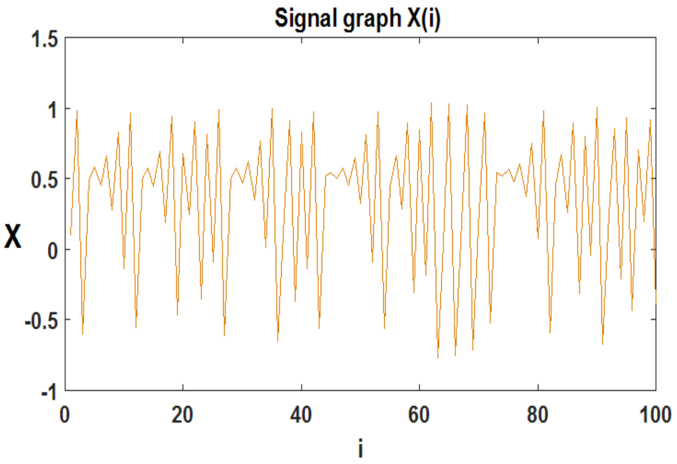


Fig. 1: Signal Graph X(i) of the Proposed Chaotic System.

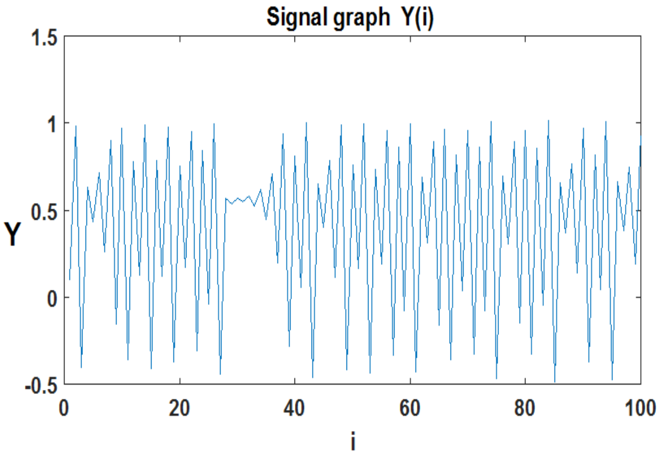


Fig. 2: Signal Graph Y(i) of the Proposed Chaotic System.

Finally, the proposed 4-D map with seven (07) nonlinear terms is given as follows:

$$\begin{cases} X(n+1) = 1 - a * X(n)^2 + (Y(n) * Z(n) * P(n)) \\ Y(n+1) = 1 - b * Y(n)^2 + (X(n) * Z(n) * P(n)) \\ Z(n+1) = 1 - c * Z(n)^2 + (X(n) * Y(n) * P(n)) \\ P(n+1) = d * X(n) * Y(n) * Z(n) \end{cases} \tag{3}$$

where X, Y, Z and P are the state variables and a, b, c and d are the control parameters or the controllers of the system.

To obtain the chaotic behavior of the proposed system (see Figures 1 to 10) , we define the values of the controllers as: a=1.65; b=1.45; c=1.7 and d=0.35; all with initial state of $X(0)$=$Y(0)$=$Z(0)$=$P(0)$ = 0.1. All these values are selected to ensure the chaotic behaviour of the proposed system, using the algorithm presented in [18].

Figures 1 to 4 show the signals of the variables X, Y, Z and P, which confirm the behaviour of the system. Moreover, we used the plan projection of the trajectories obtained through

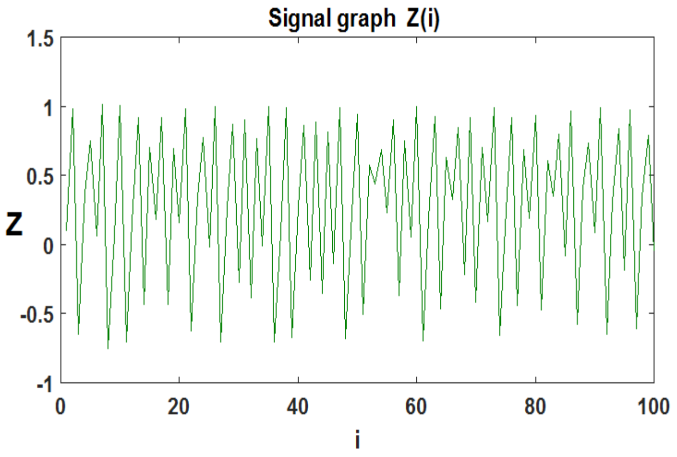


Fig. 3: Signal Graph Z(i) of the Proposed Chaotic System.

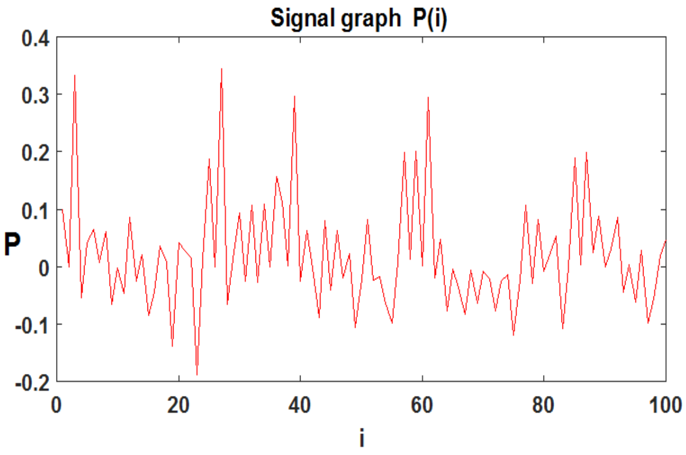


Fig. 4: Signal Graph P(i) of the Proposed Chaotic System.

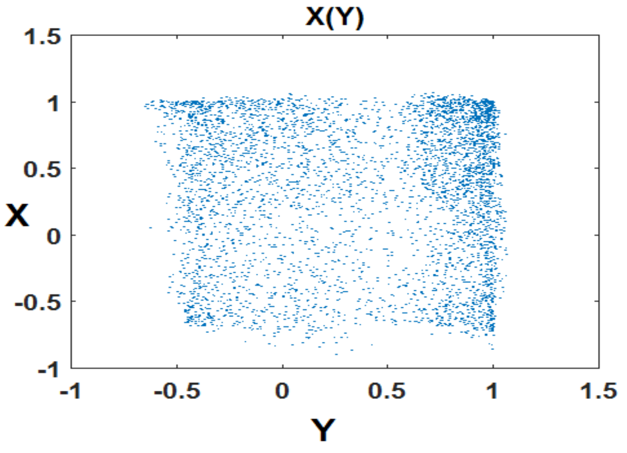


Fig. 5: Trajectory Graph X(Y) of the Proposed Chaotic System.

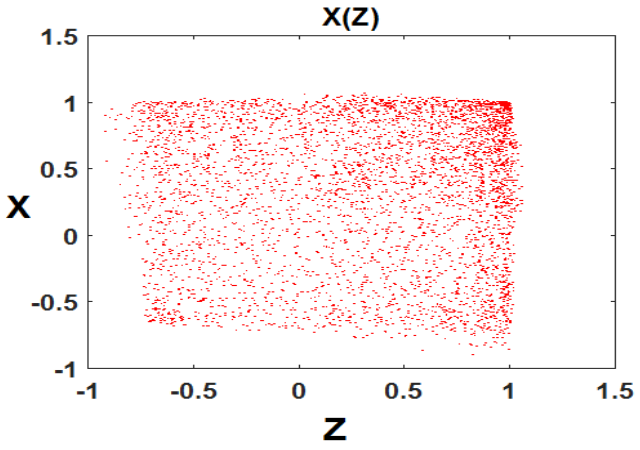


Fig. 6: Trajectory Graph X(Z) of the Proposed Chaotic System.

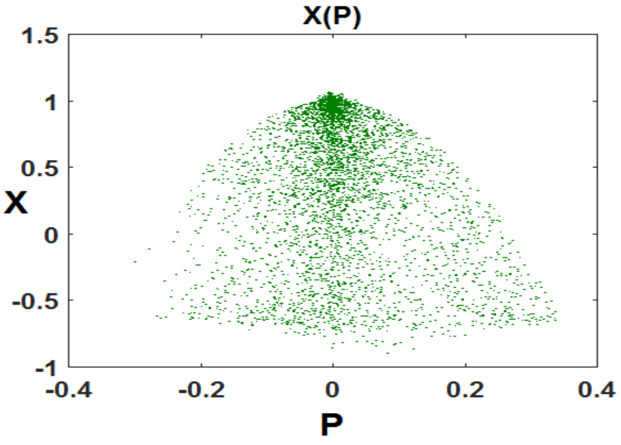


Fig. 7: Trajectory Graph X(P) of the Proposed Chaotic System.

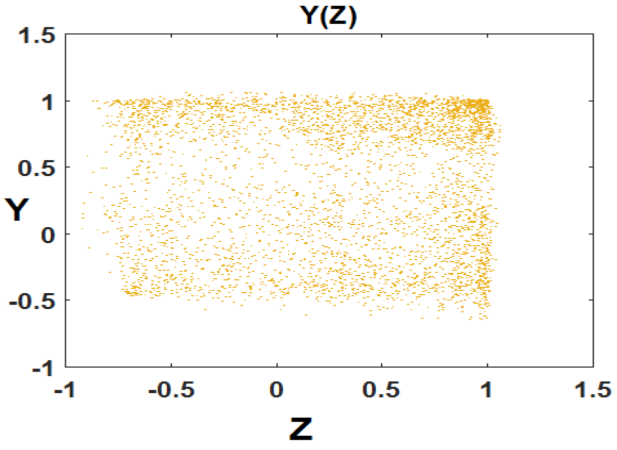


Fig. 8: Trajectory Graph Y(Z) of the Proposed Chaotic System.

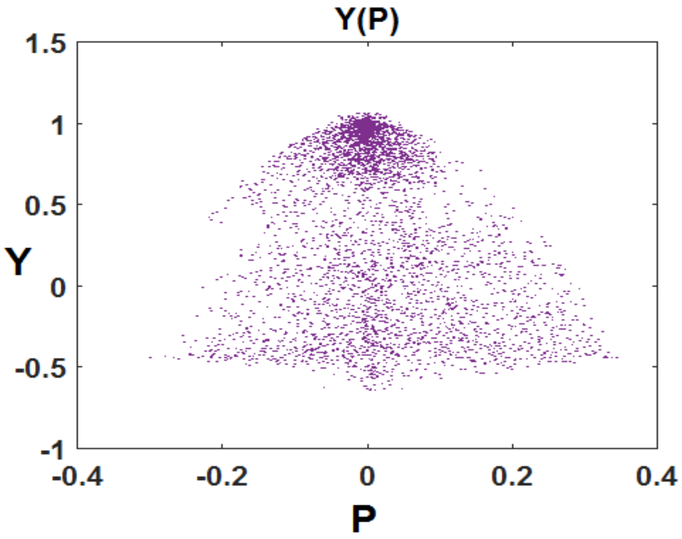


Fig. 9: Trajectory Graph Y(P) of the Proposed Chaotic System.

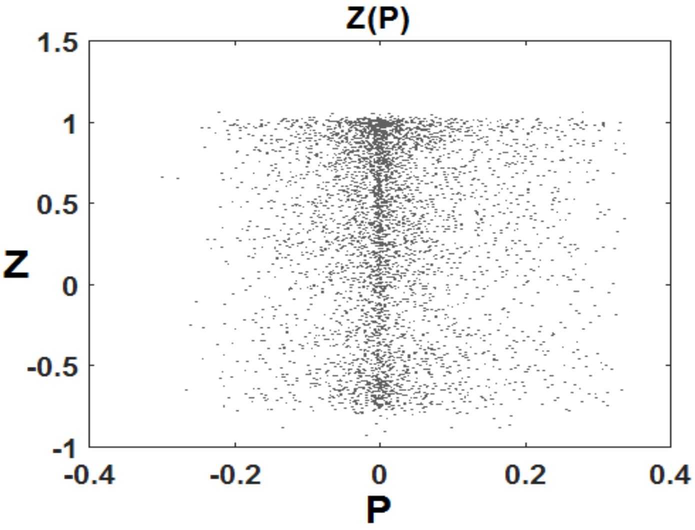


Fig. 10: Trajectory Graph Z(P) of the Proposed Chaotic System.

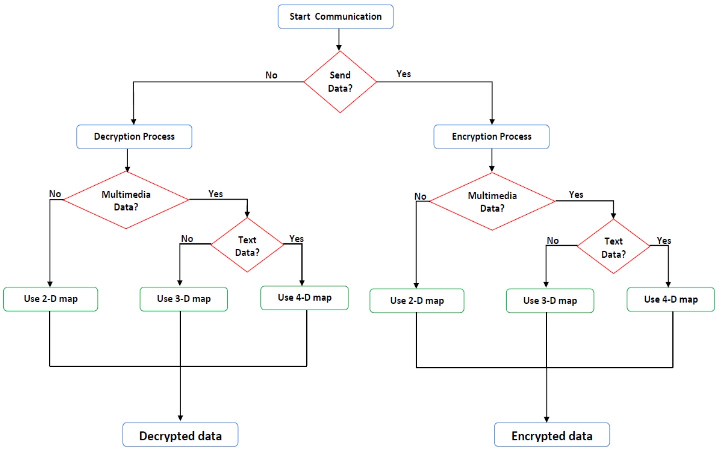


Fig. 11: The Proposed Algorithm Flow Chart.

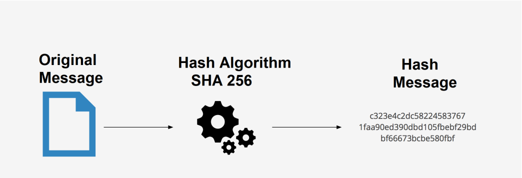


Fig. 12: Hash Function Design.

these variables to confirm the chaotic behaviour, as shown in Figures 5 to 10.

III. Application of the Proposed Cryptosystem

We present an application of the proposed configurable chaos system to secure the exchanged sensitive data in digital communications.

A. *Algorithm Design and Implementation*

A secure communication channel is a software application that includes user's interface and a cryptosystem to ensure data encryption. Due to the variety of the exchanged data and the high demand of lightweight cryptosystem, we introduce a configurable chaos-based cryptosystem using the chaotic maps defined by equations (1), (2) and (3). The proposed algorithm, as shown in the flow chart in 11), runs as follows:

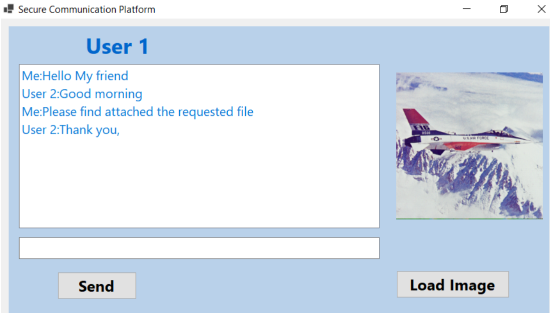
(i) Once the communication is established, we distinguish between two (2) main cases: sending data or receiving data;

(ii) In the case of sending data, we run the encryption process according to the data type. For only text data, we use the 2-D system for the encryption. Then, for only image data, we use the 3-D system. Finally, we use the 4-D system in the case of both image and text data;

(iii) In the case of receiving data, we run the same steps as in (ii) for the decryption process according to the received data type.

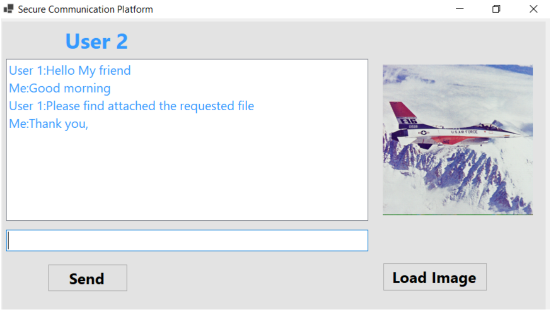
The reason of using the 2-D system for encrypting only text data is that the text data does not require a higher dimensional chaotic system. Moreover, we used the 3-D system only for image encryption in order to follow the approach based on the 3-D chaos system proposed in [18]. Finally, the 4-D system is used for encryption of heterogeneous data (text and image) by allowing three (3) components for the image and one (1) component for the text.

To enhance the security of encrypted text, we include the solution called SHA2 (Secure Hash Algorithm 2) or SHA256 (see Figure 12) as hash function which is considered better than MD5 (Message Digest 5) and SHA1 [15]. The proposed hash function is implemented using some widely used security applications and protocols, including Transport Layer Security (TLS), Secure Sockets Layer (SSL) and Internet Protocol Security (IPsec).



Me:Hello My friend
User 2:Good morning
Me:Please find attached the requested file
User 2:Thank you,

Fig. 13: First User's Interface.

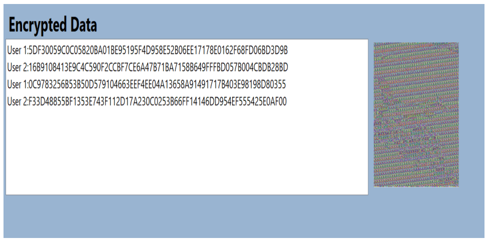


User 1:Hello My friend
Me:Good morning
User 1:Please find attached the requested file
Me:Thank you,

Fig. 14: Second User's Interface.

B. *Performance Analysis*

We use C# programming language to implement the proposed solution and application. The proposed application is composed of two (02) interfaces for exchanging messages (see Figure 13 and Figure 14), and a third separate interface to show the encryption process's results (see Figure 15).



User 1:5DF30059C0C05820BA01BE95195F4D958E52B06EE17178E0162F68FD06BD3D9B
User 2:16B9108413E9C4C590F2CCBF7CE6A47B71BA7158B649FFFBD057B004CBDB28BD
User 1:0C9783256B53B50D579104663EEF4EE04A13658A91491717B403E98198D80355
User 2:F33D48855BF1353E743F112D17A230C0253B66FF14146DD954EF555425E0AF00

Fig. 15: Encrypted Exchanged Data Using the Proposed System.

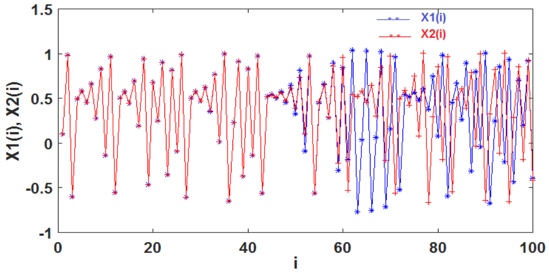


Fig. 16: Sensitivity of the Signal X(i).

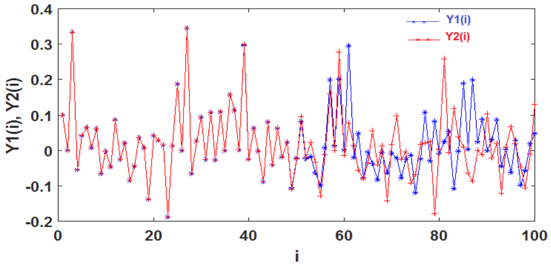


Fig. 17: Sensitivity of the Signal Y(i).

1) Key Sensitivity: To evaluate the sensitivity to initial conditions of the proposed system, we consider a changing by 10^{-10} of the initial values related to the variables $X(0)$, $Y(0)$, $Z(0)$ and $P(0)$. The sensitivity to the slightest changes of the different variables is obtained by generating two trajectories L1($X(0)$,$Y(0)$,$Z(0)$,$P(0)$) and L2($X(0)$+10^{-10}, $Y(0)$+10^{-10}, $Z(0)$+10^{-10}, $P(0)$+10^{-10}) keeping the same control parameters. The results shown in the Figures 16 to 19 prove that, even with the weakest difference in initial values attributed to $X(0)$,$Y(0)$,$Z(0)$ and $P(0)$, we observe significant changes after only around 50 iterations, which confirms the sensitivity dependence on the initial conditions of the proposed maps.

2) Key Space: Usually, chaos-based cryptosystems are made of Pseudo-Random Number Generators (PRNG) used as key streams for ciphering. Among the required conditions for an encryption scheme to be secure, we find the large key space condition to resist against brute-force attacks [16]. Thereby, the analysis of the key space parameter, which is defined by the number of the parameters and the size of the

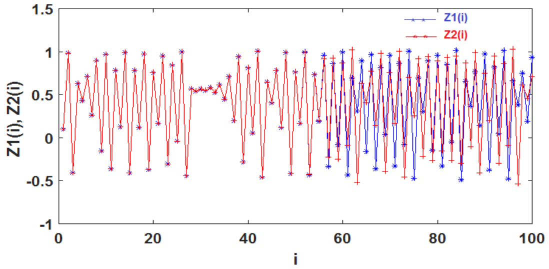


Fig. 18: Sensitivity of the Signal Z(i).

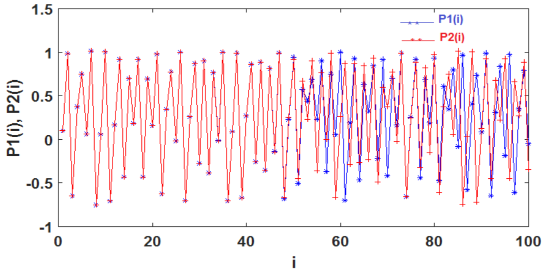


Fig. 19: Sensitivity of the Signal P(i).

ISBN: 978-1-61208-927-0

desired key, is used as a basis of comparison between the proposed system and some existing systems. Therefore, by supposing the generation of cipher keys on 32 bits, the key space parameter is computed for each map and showed in Table I.

TABLE I. KEY SPACE COMPARISON.

Cryptosystems	Key space value
The proposed (2-D)	2^{128}
The proposed (3-D)	2^{192}
The proposed (4-D)	2^{256}
AES	2^{128}
DES (Data Encryption Standard)	2^{56}
3-DES	2^{168}

3) Security of Hash Encryption: In practice, there are two common methods used to attack the hash encryption algorithm.

The first method is based on finding the collision by introducing different characters, which would help to get the same hash values when the collision occurs. Therefore, the attacker could crack the SHA256 by obtaining the same hash value with the one used during the encryption process. However, in our case with 256 bits of SHA256 and 32 bits of the generated chaotic sequence, the task of cracking our algorithm becomes impossible.

The second method found in the literature for attacking the hash encryption algorithm is called exhaustive method. For some short and simple combination, this method is very efficient. Nevertheless, due to the adopted process of this method based on single character scan, and the combination of the words in the dictionary, the exhaustive method is difficult to work with the number of the characters included in the output of the SHA256 hash encryption algorithm.

IV. Conclusion and Future Work

With the development of Internet and digital networking applications, security has become a major concern in the current era of Information Technology.

Unlike all the previous related works, we presented in this paper a novel and dynamic chaos-based cryptosystem in order to secure both the exchanged identity text and the image data. First, we described and analyzed the different dimensional chaotic systems (2-D, 3-D and 4-D). Then, we applied the proposed chaotic systems inside a C# chat application to secure the exchanged data. The encryption/decryption processes are run using the 2-D system for exchanged text data, the 3-D system for only image data and the 4-D system for both text and image data. Results showed that the proposed chaotic maps are very sensitive to initial conditions and provide larger key space to perform secure communication.

As future work, the integration of digital FPGA (Field-Programmable Gate Array) technology for data encryption in an IP-communication with the proposed solution will be investigated. Moreover, the evaluation of the proposed scheme where several input data of different types and complexities will be performed and compared against the results obtained through existing schemes.

References

[1] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, ”Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions,” Journal of Ambient Intelligence and Humanized Computing, pp. 1–18, 2017.

[2] R. R. Salavi, M. M. Math, and U. P. Kulkarni, ”A Survey of various cryptographic techniques: from traditional cryptography to fully homomorphic encryption,” Innovations in Computer Science and Engineering, pp. 295–305, 2019.

[3] K. R. Saraf, V. P. Jagtap, and A. K. Mishra, ”Text and image encryption decryption using advanced encryption standard,” International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), vol. 3, pp. 118–126, 2014.

[4] N. Mathur and R. Bansode, ”AES based text encryption using 12 rounds with dynamic key selection,” Procedia Computer Science, vol. 79, pp. 1036–1043, 2016.

[5] L. D. Singh and K. M. Singh, ”Implementation of text encryption using elliptic curve cryptography,” Procedia Computer Science, vol. 54, pp. 73–82, 2015.

[6] U. Singh and U. Garg, ”An ASCII value based text data encryption system,” International Journal of Scientific and Research Publications, vol. 3, pp. 2250–3153, 2013.

[7] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, ”Content based double encryption algorithm using symmetric key cryptography,” Procedia Computer Science, vol. 57, pp. 1228–1234, 2015.

[8] S. C. Iyer, R. R. Sedamkar, and S. Gupta, ”A novel idea on multimedia encryption using hybrid crypto approach,” Procedia Computer Science, vol. 79, pp. 293–298, 2016.

[9] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, ”Traditional and hybrid encryption techniques: a survey,” Networking communication and data knowledge engineering, pp. 239–248, 2018.

[10] R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat, ”Survey on revocation in ciphertext-policy attribute-based encryption,” Sensors, vol. 19, p. 1695, 2019.

[11] V. H. Kalmani, D. Goyal, and S. Singla, ”An efficient and secure solution for attribute revocation problem utilizing CP-ABE scheme in mobile cloud computing,” International Journal of Computer Applications, vol. 129, pp. 16–21, 2015.

[12] L. Pang, J. Yang, and Z. Jiang, ”A survey of research progress and development tendency of attribute-based encryption,” The Scientific World Journal, vol. 2014, 2014.

[13] M. Philip and A. Das, ”Survey: Image encryption using chaotic cryptography schemes,” IJCA Special Issue on “Computational Science-New Dimensions and Perspectives” NCCSE, pp. 1–4, 2011.

[14] M. Babaei, ”A novel text and image encryption method based on chaos theory and DNA computing,” Natural computing, vol. 12, pp .101–107, 2013.

[15] D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, ”A comparative study of message digest 5 (MD5) and SHA256 algorithm,” Journal of Physics: Conference Series, vol. 978, p. 012116, 2018.

[16] G. Alvarez and S. Li, ”Some basic cryptographic requirements for chaos-based cryptosystems,” International Journal of Bifurcation and Chaos, vol. 16, pp. 2129–2151, 2006.

[17] B. Bouteghrine, C. Tanougast, and S. Sadoudi, ”Design and FPGA implementation of new multidimensional chaotic map for secure communication,” Journal of Circuits, Systems and Computers, p. 2150280, 2021.

[18] B. Bouteghrine, C. Tanougast, and S. Sadoudi, ”Novel image encryption algorithm based on new 3-d chaos map”, Multimedia Tools and Applications, vol. 80, pp. 25583-–25605, 2021.