# Introducing Chaos and Chaos Based Encryption Applications to University Students - Case Report of a Seminar

Lazaros Moysis*, Denis N. Butusov†, Aleksandra Tutueva†‡, Valerii Ostrovskii†, Ioannis Kafetzis*, Christos Volos*
* Laboratory of Nonlinear Systems - Circuits & Complexity, Physics Department, Aristotle University of Thessaloniki, Thessaloniki, Greece. {lmousis,kafetzis,volos}@physics.auth.gr
† Department of Computer-Aided Design, Saint Petersburg Electrotechnical University 'LETI', Saint Petersburg 197376, Russia. {dnbutusov,avtutueva,vyostrovskii}@etu.ru
‡ Youth Research Institute, Saint Petersburg Electrotechnical University 'LETI', Saint Petersburg, 197376, Russia.

***Abstract*—During the fall semester of 2021-2022 academic year, a seminar series on 'Chaotic Cryptography' was delivered at the Department of Computer Aided Design (CAD), St. Petersburg Electrotechnical University 'LETI', Russia. The seminar aimed at introducing students to state of the art research topics that connect chaos theory to various applications relating to encryption and security. This work constitutes a case report on this seminar. First, the seminar syllabus is presented. Then, future goals are discussed for annual reruns of the seminar.**

***Index Terms*—chaos, encryption, applications, secure communications, education, physics education, STEM education.**

## I. Introduction

Chaos theory is a well established field of mathematics and physics, that has attracted the attention of scientists for over 60 years [1], [2]. Their study remains a state of the art topic, with new phenomena constantly emerging, like hidden attractors [3], coexisting attractors [4] and more. Chaos theory is applied in the modelling of physical or digital systems in physics [1], engineering [5], and electronics [6], among others. In addition to modelling physical phenomena though, chaos is also used as a tool in many applications, as a low cost, easy to implement source of randomness, that can increase the security, or in general, the efficiency of a design. Such applications include path planning and surveillance [7], [8], optimization [9], data encryption [10], [11], secure communications [12] and more [2]. It seems that chaos theory is constantly growing, both in the modelling direction, as well as in the application areas.

As chaos theory is a state of the art topic of research with future potential, it is important to introduce it in Natural and Applied Sciences Departments. This has previously been considered for different education levels, from secondary to higher. In [13], studies were conducted to assertate the possibility of teaching the interplay of chance and determinism in upper secondary students. In [14], a 12 lecture syllabus was developed for introducing chaos theory at senior high school level. In [15], a three course seminar to engage students with chaos theory was designed.

At the University level, in [16], a magnetic pendulum with chaotic behavior was developed for physics laboratories. In [17], a course for Nonlinear Dynamics was developed for first year students of Chemical Engineering, Environmental Sciences, and Computer Sciences Departments. In [18], a Graphical User Interface (GUI) was developed for image, text, or audio encryption, that can be used as an educational tool in courses of 'Data Security' and 'Chaotic Systems and Chaos Based Information Security'. Finally in [19], [20], circuit and microcontroller implementations of chaotic systems have been developed, for use in courses related to nonlinear circuits.

Motivated by the above, a seminar on 'Chaotic Cryptography' was delivered at the Department of Computer Aided Design (CAD), St. Petersburg Electrotechnical University 'LETI', in Russia. The lectures presented a collection of introductory topics relating to security, encryption, and relevant chaos based applications, ending up each lecture with a discussion of state of the art research problems. The goal was to help the participants gain a spherical understanding of the numerous chaos related applications, and provide them with a collection of trending topics they could choose for their future research.

This paper presents a report on the seminar. First of all, the syllabus of each lecture is presented, along with the references used to cover each topic. Moreover, as the authors' interest is to establish this seminar as an annual event, goals are set for future reruns. The authors hope that this can serve as a reference for educators and researchers who are interested in delivering similar workshops in the future.

The rest of the work is as follows: In Section II, the seminar syllabus is presented. In Section III, future plans are discussed. Section IV concludes the work with an overview of the presented subject.

## II. The Seminar Syllabus

In this section, the contents of each lecture are presented, along with their corresponding literature resources. The seminar was broken down to eight lectures, delivered twice a week. Each lecture consisted of two hours, so the overall length was sixteen hours, over the span of four weeks. Each lecture ended with a discussion on open research problems. The syllabus is outlined in Table I.

The lectures were delivered virtually, using the Pruffme platform. The main reason behind this option was the current pandemic situation, which posed limitations to travelling, and additional security measures in Universities. The second reason was to give the opportunity to students from different Universities to participate in the lectures. The audience consisted of participants from LETI and A.U.TH. Universities.

TABLE I
SEMINAR SYLLABUS

| Lecture | Subject |
|---|---|
| 1st | – Introduction to chaos theory.<br>– Discrete chaotic systems. |
| 2nd | – Continuous chaotic systems.<br>– Chaotic area exploration. |
| 3rd | – Chaotic surveillance.<br>– Pseudo Random Bit Generators (PRBGs). |
| 4th | – Security requirements. |
| 5th | – Text and image encryption. |
| 6th | – Chaos synchronization and secure communications. |
| 7th | – Constructing new chaotic maps. |
| 8th | – Nonlinear systems identification. |

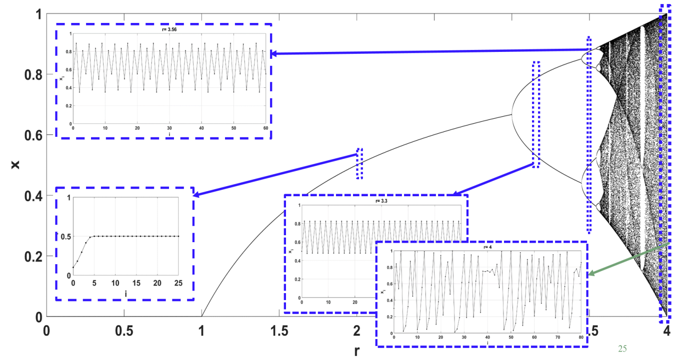



Fig. 1. Bifurcation diagram of the logistic map, with subfigures illustrating different behaviors.

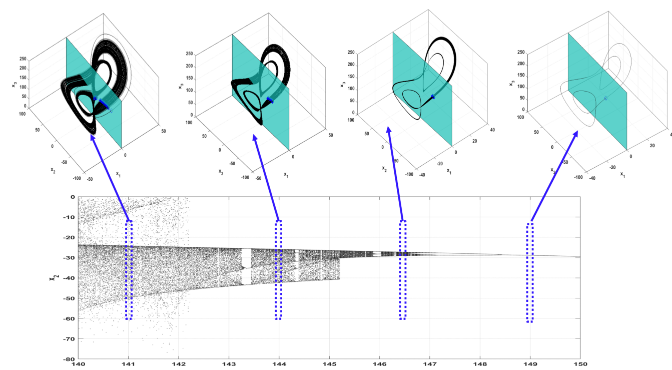


Fig. 2. Bifurcation diagram of the Lorenz system, with subfigures illustrating different behaviors, and the Poincaré section on the $x_1 = 0$ plane, with $\dot{x}_1 > 0$.

### A. Introduction to Chaos Theory - Discrete Chaotic Systems

In the first Lecture, a general introduction to the topic of chaos theory was provided [1]. The concept of sensitivity to initial conditions was explained through multiple examples and simulations, like the double pendulum.

The analysis of chaotic systems started from discrete time models, using the well known logistic map [1]. Through a collection of simulations, the bifurcation diagram of the map was provided and explained, see Fig. 1. Cobweb diagrams were also illustrated, which constitute another tool for the analysis of discrete maps, and the visualization of their trajectories. Then, the Lyapunov exponent of a map was provided, which serves as a measure of the system's sensitivity, and can indicate whether a system behaves chaotically or not [21]. Using the above tools, other chaos related phenomena where illustrated, like crisis, expansion of the attractor shape, antimonotonicity, and coexisting attractors [3], [22], [23].

### B. Continuous Chaotic Systems

On Lecture 2, the introduction continued on continuous time systems. The Lorenz and Rössler systems were given as examples. The Poincaré section was explained, as a tool to construct the bifurcation diagram, see Fig. 2. Another method for computing bifurcation diagrams by plotting the local maxima of a state was also described. Continuation diagrams were also explained. Finally, systems with coexisting attractors were discussed [22].

### C. Chaotic Area Exploration

On the second part of Lecture 2, the first application of chaotic systems related to security was presented, that of area exploration [7], [24], [25]. Chaotic area exploration, or chaotic path planning, refers to the problem of using a chaotic system as a source to generate a chaotic trajectory for a ground vehicle or UAV, see Fig. 3 for a simulation example. The autonomous agent is tasked with exploring an area, but an additional requirement is to generate an unpredictable trajectory. This may be useful in several different scenarios, for example in cases where the agent is tracked by an adversary and wants to move unpredictably, in hostile environments where the area must be traversed repeatedly, as in fire fighting, or even in simpler domestic applications, like floor cleaning [7].

After the motivation behind this application was provided, several simulations were given, for different ground vehicle models. Optimization techniques were then discussed to improve performance, as well as the case of multiple robots exploring an area [24], [25]. The lecture ended with a discussion on future topics of research, like the development of hybrid techniques, and the experimental testing using off the shelf programmable robotic kits [26].

### D. Chaotic Surveillance

On Lecture 3, a topic relevant to chaotic area exploration was presented, that of chaotic surveillance. This problem refers to the safe monitoring of a secure area, by deploying agents that move unpredictably, as an extra measure against

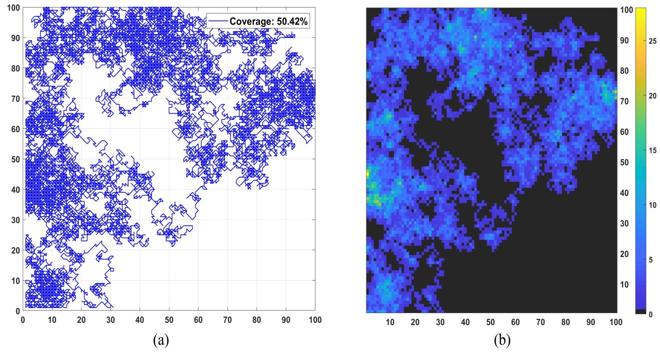



Fig. 3. Simulation example of (a) chaotic motion and (b) colour-coded graph depicting the amount of area revisiting.

adversaries or intruders [8]. The use of UAV agents equipped with chaotic moving cameras was discussed [27], [28], see Fig. 4. The section ended with a discussion of future goals, which include the experimental implementation, and the development of hybrid techniques to make the motion energy efficient.

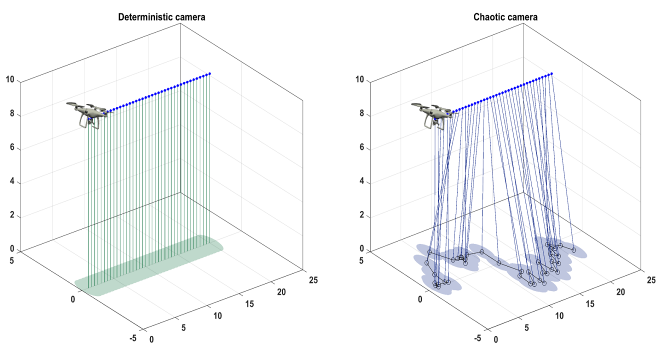



Fig. 4. Example of two scenarios of a UAV mounted with a camera. (a) the camera has a fixed position looking directly down to the ground and (b) the camera strafes chaotically, guided by the values of a chaotic map.

## *E. Pseudo Random Bit Generators (PRBGs)*

On the second half of Lecture 3, a new topic was presented, that of bit generation [29], [30]. This is of fundamental importance in encryption, as PRBGs are implemented to encrypt information. This holds for any type of information, since all data can be represented and transmitted in binary format.

For this application, one-dimensional discrete maps were considered, due to their low computational cost and implementability. Different techniques were presented to generate one or multiple bits per iteration of the chaotic maps, as well as similar techniques to generate random integers [10], [29], [31]–[35].

## *F. Security Requirements*

After techniques for PRBGs were presented, on Lecture 4 the different security requirements for PRBGs were presented. First of all, the suites used for testing the statistical randomness of PRBGs were considered, like the National Institute of Standards and Technology (NIST) suite and the ENT suite [36], [37]. Short definitions were given for each statistical test, and interpretation of the resulting P-value was provided.

Moreover, some other cryptographic requirements were explained, as the requirement of a well defined key space, that can resist brute force attacks [38]. Also key sensitivity as another requirement, which is essential for secure designs. Finally, the speed of bit generation was discussed, as a function of the number of operations required to generate a single bit.

The above were illustrated through an application of a password generator, that was developed as a Graphical User Interface [18]. The GUI took as an input a set of answers provided by the user to some simple identifying questions. Those ASCII answers were then used to define the key values of a PRBG that generated random characters to be used as a secure password, using a simple binary to ASCII conversion. The GUI used is depicted in Fig. 5.

The lecture ended with a discussion on trending topics related to chaos based PRBGs, like the problem of dynamical degradation [39], the use of delay terms to improve complexity [10], as well as the problem of their microcontroller implementation [19], [30].

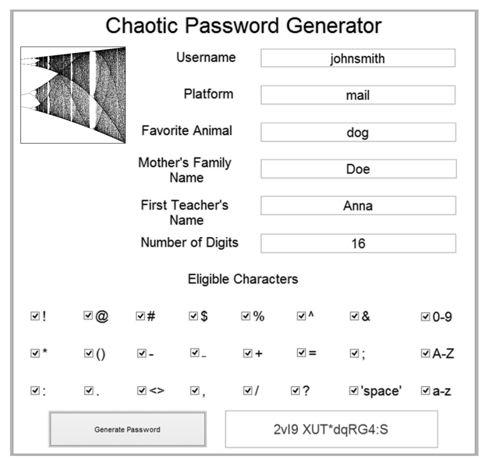
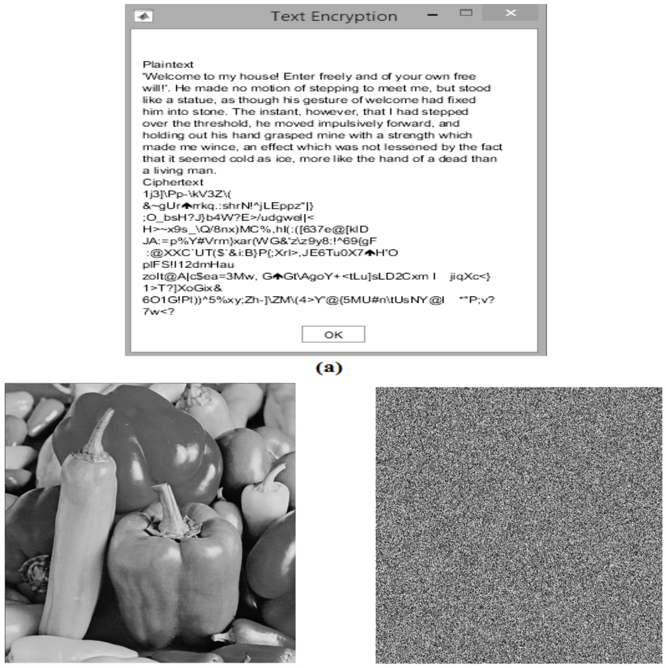



Fig. 5. Password generator GUI used to illustrate the use of PRBGs.

## *G. Text and Image Encryption*

Lecture 5 presented the problem of chaos based text and image encryption [30], [40], see illustrative Fig. 6. The concepts of confusion, diffusion and pixel/character permutation were explained, and showcased through examples.

Special attention was given to the topic of image encryption [11], [40]–[43], as the simulation results are easier to visualize. The various statistical tests used to evaluate the security of a design were provided and discussed, such as the histogram analysis, pixel correlation, global and local information entropy, the NPCR and UACI measures used to test differential attacks, cropping attacks, noise corruption, and key sensitivity. Finally, a collection of trending research topics was provided, like the combination of encryption and compression [44], the use of different image representations like the YCbCr [45], the problems of watermarking [46] and steganography [47], and the encryption of 3D objects [48].




**(b)**

Fig. 6. Example of original (plaintext) and encrypted (ciphertext) (a) text and (b) image.

## *H. Chaos Synchronization and Secure Communications*

During Lecture 6, the problem of chaos control and synchronization was presented [49]. First, the fundamental concept of feedback stabilization and feedback linearization was described. Then, the problem of master-slave synchronization between two chaotic systems was presented, where the slave system needs to synchronize its state trajectories to those of a master system, see an illustrative example at Fig. 7. The problem of observer design was also explained [12], which is similar to that of master-slave synchronization, but here the only information about the master system is through a measurable output.

Using the synchronization between two systems, the application of secure communications was presented [12], [50]. Here, an information signal is masked through its combination with a chaotic system, and then safely transmitted through a channel. Then at the receiver end, by successful synchronization of the master and slave systems, the information signal can be accurately reconstructed. Several approaches for this were considered, like the reformulation to descriptor form [51], or the adaptive approach, were an information signal is passed through a system's time varying parameter, which is estimated at the receiver end [52].

Several state of the art future topics were discussed, for example the different types of syncrhonization, like anti-synchronization [53], phase synchronization [54], projective syncrhonization and function-projective synchronization [55]. Also, different cases control were discussed, for example adaptive control, where some parameters of the master system may be unknown [56].

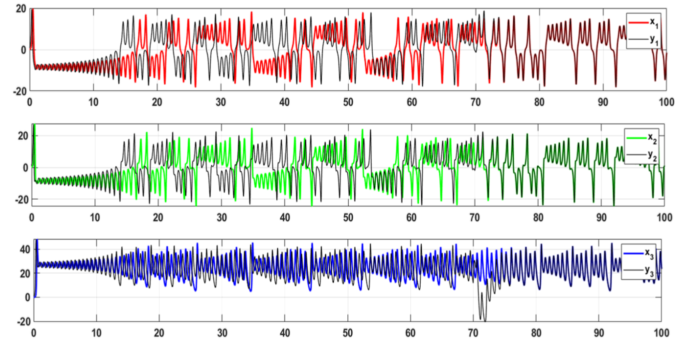



Fig. 7. Synchronization between the master and slave (black) systems, where control activates at $t = 70$ seconds.

## *I. Constructing New Chaotic Maps*

Lecture 7 was devoted to the problem of designing new chaotic maps. This is a trending problem, since new applications of chaotic systems are constantly reported, and hence there is the need to develop new chaotic maps to utilize in them. Especially for encryption, there are several additional requirements, for example having maps with a high key space, and also a constant chaotic behavior, over large regions of their parameter space.

The construction of new chaotic maps is usually performed by considering existing maps, and modifying them using one of the following approaches [31], [57]. The first is to generalize the map by increasing its parameter space, by scaling up the terms of the map, for example replacing the term $x_i$ by $ax_i$, where $a$ is a parameter. The second approach is to replace a term by another term, for example a sine function by an exponential function. The third approach is to add more nonlinear terms in the difference equation describing the map. The forth approach is to combine existing maps, through linear combination, switching, composition or other techniques. All of the above approaches aim at increasing the complexity of the original map, which can be verified by comparing the bifurcation diagrams and Lyapunov exponent diagram between the original and modified map. For the above approaches, many examples were given, using well known maps like the sine, Chebysev, Renyi and more [58]. An example of the considered approaches is shown in Fig. 8.

Several emerging techniques were also discussed, like the sine chaotification [59], and the modulo chaotification [60].

## *J. Nonlinear System Identification*

In the final Lecture, the problem of system identification was presented, following the methodology proposed in [61]. This problem consists of reconstructing the set of differential or difference equations that describe a system, using a set of measurements of the system's states. This problem can be of use in several different applications, including encryption and

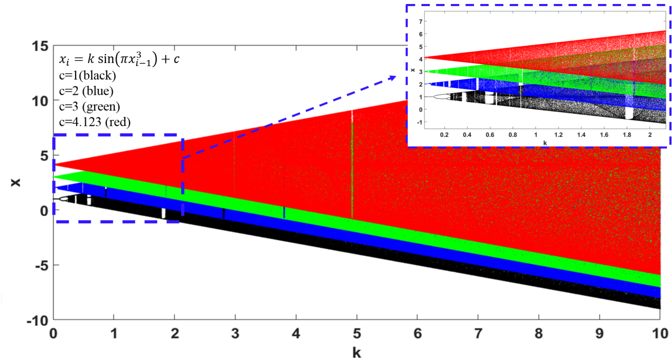



Fig. 8. Examples of modifications of the Sine map $x_i = k\sin(\pi x_{i-1})$.

secure communications. If we assume that a set of system data may be available to an adversary, then by reverse engineering, they may be able to reconstruct the system's structure, which could compromise the design.

Examples where given from continuous systems, like the Lorenz, different systems with coexisting attractors [3], [22], as well as discrete time maps, like the logistic, sine, Chebysev and more. Based on the simulation results, many future problems were discussed, regarding the identification of physical systems, the utilization in systems with coexisting attractors, and the use of nonlinear functions that could counter the identification approach, like the modulo operator.

## III. Future Plans

Several goals can be set for future reruns of the seminar. First of all, the inclusion of more participants will be aimed. For this, a wider spread through social media platforms will be considered, so that people from different countries will be notified about the event. Another option is to share the seminar with Department and Lab Heads, so they can directly notify master and PhD students using their mailing lists.

Regarding the syllabus, it can be enhanced with several new topics. Fore example, a lecture can be included on systems with hidden attractors [3], and their use in applications. Moreover, a lecture on fractional order systems can be added, which have attracted a lot of attention over the decades. Also, quantum systems can be discussed, which have recently been addressed through chaos theory, and will attract much attention in the future [32]. In addition, one more application that can be considered is that of chaos based optimization [9]. Circuit realizations of chaotic systems can also be presented [19], [20].

Finally, other actions can be taken to enhance the seminar. For example, inviting established researchers from collaborating Universities to deliver key lectures on relevant topics. Also, the Seminar could be transformed into a workshop, by guiding groups of students to develop illustrative applications on the topics covered, and demonstrate their results through presentations or posters.

## IV. Conclusions

This paper constituted a report on a series of lectures on the topic of Chaos Based Encryption, delivered virtually during the winter semester of 2021-2022 at the Department of Computer Aided Design (CAD), on St. Petersburg Electrotechnical University 'LETI', in Russia. During the seminar, various aspects of chaos based applications related to security and encryption were presented, with emphasis on trending topics of research.

The goal of the authors is to establish this Seminar as a yearly occurrence, with an international audience. Goals are set to improve future reruns of the seminar, and enhance it with new material. The authors hope that this report can motivate fellow researchers to organize similar seminars in the future, to expand the outreach of chaos theory and its applications in Natural Sciences and Engineering Departments.

## Supplementary Material

All of the lecture slides used in the seminar are available from the first author upon request.

## References


[1] S. H. Strogatz, *Nonlinear dynamics and chaos with student solutions manual: With applications to physics, biology, chemistry, and engineering*. CRC press, 2018.

[2] G. Grassi, "Chaos in the real world: Recent applications to communications, computing, distributed sensing, robotic motion, bio-impedance modelling and encryption systems," *Symmetry*, vol. 13, no. 11, p. 2151, 2021.

[3] Y. Wang, Z. Wang, D. Kong, L. Kong, and Y. Qiao, "Multifarious chaotic attractors and its control in rigid body attitude dynamical system," *Mathematical Problems in Engineering*, vol. 2020, 2020.

[4] Q. Lai, C. Chen, X.-W. Zhao, J. Kengne, and C. Volos, "Constructing chaotic system with multiple coexisting attractors," *IEEE Access*, vol. 7, pp. 24 051–24 056, 2019.

[5] Y. Chen and A. Y. Leung, *Bifurcation and chaos in engineering*. Springer Science & Business Media, 2012.

[6] C. K. Volos, V.-T. Pham, H. E. Nistazakis, and I. N. Stouboulos, "A dream that has come true: chaos from a nonlinear circuit with a real memristor," *International Journal of Bifurcation and Chaos*, vol. 30, no. 13, p. 2030036, 2020.

[7] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Experimental investigation on coverage performance of a chaotic autonomous mobile robot," *Robotics and Autonomous Systems*, vol. 61, no. 12, pp. 1314–1322, 2013.

[8] P. S. Gohari, H. Mohammadi, and S. Taghvaei, "Using chaotic maps for 3d boundary surveillance by quadrotor robot," *Applied Soft Computing*, vol. 76, pp. 68–77, 2019.

[9] S. Saremi, S. Mirjalili, and A. Lewis, "Biogeography-based optimisation with chaos," *Neural Computing and Applications*, vol. 25, no. 5, pp. 1077–1097, 2014.

[10] L. Liu, S. Miao, M. Cheng, and X. Gao, "A pseudorandom bit generator based on new multi-delayed chebyshev map," *Information Processing Letters*, vol. 116, no. 11, pp. 674–681, 2016.

[11] M. Z. Talhaoui, X. Wang, and M. A. Midoun, "A new one-dimensional cosine polynomial chaotic map and its use in image encryption," *The Visual Computer*, pp. 1–11, 2020.

[12] T.-L. Liao and N.-S. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 46, no. 9, pp. 1144–1150, 1999.

[13] D. Stavrou, R. Duit, and M. Komorek, "A teaching and learning sequence about the interplay of chance and determinism in nonlinear systems," *Physics Education*, vol. 43, no. 4, p. 417, 2008.

[14] T. Meszéna, "Chaos at high school," *Scientia in educatione*, vol. 8, 2017.

[15] T. Tél, "Chaos physics: what to teach in three lessons?" *Physics Education*, vol. 56, no. 4, p. 045002, 2021.

[16] J. R. Claycomb and J. H. Valentine, "The butterfly effect for physics laboratories," *Physics Education*, vol. 50, no. 2, p. 170, 2015.

[17] J. M. Seoane, S. Zambrano, and M. A. San Juan, "Teaching nonlinear dynamics and chaos for beginners," *Latin-American Journal of Physics Education*, vol. 2, no. 3, p. 10, 2008.

[18] A. Akgul, S. Kacar, I. Pehlivan, and B. Aricioglu, "Chaos-based encryption of multimedia data and design of security analysis interface as an educational tool," *Computer Applications in Engineering Education*, vol. 26, no. 5, pp. 1336–1349, 2018.

[19] A. Giakoumis, C. K. Volos, I. N. Stouboulos, I. M. Kyprianidis, H. E. Nistazakis, and G. S. Tombras, "Implementation of a laboratory-based educational tool for teaching nonlinear circuits and chaos," in *Advances and Applications in Chaotic Systems*. Springer, 2016, pp. 379–407.

[20] D. Clemente-Lopez, L. Moysis, C. Volos, J. M. Munoz-Pacheco, S. Jafari, and I. Stouboulos, "An arm-fpga-based co-design for implementing chaotic systems," in *2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2021, pp. 1–4.

[21] J. Bovy, "Lyapunov exponents and strange attractors in discrete and continuous dynamical systems," *Theoretica Phys. Project, Catholic Univ. Leuven, Flanders, Belgium, Tech. Rep*, vol. 9, pp. 1–19, 2004.

[22] Q. Lai, P. D. Kamdem Kuate, H. Pei, and H. Fotsin, "Infinitely many coexisting attractors in no-equilibrium chaotic system," *Complexity*, vol. 2020, 2020.

[23] L. Moysis, E. Petavratzis, M. Marwan, C. Volos, H. Nistazakis, and S. Ahmad, "Analysis, synchronization, and robotic application of a modified hyperjerk chaotic system," *Complexity*, vol. 2020, 2020.

[24] L. Moysis, E. Petavratzis, C. Volos, H. Nistazakis, and I. Stouboulos, "A chaotic path planning generator based on logistic map and modulo tactics," *Robotics and Autonomous Systems*, vol. 124, p. 103377, 2020.

[25] E. Petavratzis, L. Moysis, C. Volos, I. Stouboulos, H. Nistazakis, and K. Valavanis, "A chaotic path planning generator enhanced by a memory technique," *Robotics and Autonomous Systems*, p. 103826, 2021.

[26] H. He, Y. Cui, C. Lu, and G. Sun, "Time delay chen system analysis and its application," in *International Conference on Mechanical Design*. Springer, 2019, pp. 202–213.

[27] I. Kafetzis, L. Moysis, C. Volos, I. Stouboulos, and K. Valavanis, "Area surveillance using a uav with mounted chaotic camera," in *2021 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2021, pp. 53–62.

[28] C.-T. Cheng and H. Leung, "A chaotic motion controller for camera networks," in *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*. IEEE, 2011, pp. 1976–1979.

[29] V. Patidar, K. K. Sud, and N. K. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," *Informatica*, vol. 33, no. 4, 2009.

[30] A. Giakoumis, C. K. Volos, J. M. Munoz-Pacheco, L. del Carmen Gomez-Pavon, I. N. Stouboulos, and I. M. Kyprianidis, "Text encryption device based on a chaotic random bit generator," in *2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS)*. IEEE, 2018, pp. 1–5.

[31] M. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.

[32] D. Lambić, "Security analysis and improvement of the pseudo-random number generator based on quantum chaotic map," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1117–1126, 2018.

[33] Z. Zhang, Y. Wang, L. Y. Zhang, and H. Zhu, "A novel chaotic map constructed by geometric operations and its application," *Nonlinear Dynamics*, vol. 102, no. 4, pp. 2843–2858, 2020.

[34] M. Ahmad, M. N. Doja, and M. S. Beg, "A new chaotic map based secure and efficient pseudo-random bit sequence generation," in *International symposium on security in computing and communication*. Springer, 2018, pp. 543–553.

[35] Z. Wang, A. Akgul, V.-T. Pham, and S. Jafari, "Chaos-based application of a novel no-equilibrium chaotic system with coexisting attractors," *Nonlinear Dynamics*, vol. 89, no. 3, pp. 1877–1887, 2017.

[36] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, Tech. Rep., 2001.

[37] J. Walter, "Ent: A pseudo random number sequence test program, available at https://www.fourmilab.ch/random/," 2008.

[38] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[39] L. Liu and S. Miao, "Delay-introducing method to improve the dynamical degradation of a digital chaotic map," *Information Sciences*, vol. 396, pp. 1–13, 2017.

[40] R. I. Abdelfatah, M. E. Nasr, and M. A. Alsharqawy, "Encryption for multimedia based on chaotic map: Several scenarios," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 19 717–19 738, 2020.

[41] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," *IEEE Access*, vol. 7, pp. 99 470–99 480, 2019.

[42] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16-17, pp. 3895–3903, 2011.

[43] L. Moysis, I. Kafetzis, C. Volos, A. V. Tutueva, and D. Butusov, "Application of a hyperbolic tangent chaotic map to random bit generation and image encryption," in *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*. IEEE, 2021, pp. 559–565.

[44] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Optics & Laser Technology*, vol. 99, pp. 238–248, 2018.

[45] X. Jin, S. Yin, X. Li, G. Zhao, Z. Tian, N. Sun, and S. Zhu, "Color image encryption in ycbcr space," in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*. IEEE, 2016, pp. 1–5.

[46] S. Thakur, A. K. Singh, S. P. Ghrera, and A. Mohan, "Chaotic based secure watermarking approach for medical images," *Multimedia Tools and Applications*, vol. 79, no. 7, pp. 4263–4276, 2020.

[47] J. Sharafi, Y. Khedmati, and M. Shabani, "Image steganography based on a new hybrid chaos map and discrete transforms," *Optik*, vol. 226, p. 165492, 2021.

[48] X. Wang, M. Xu, and Y. Li, "Fast encryption scheme for 3d models based on chaos system," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 33 865–33 884, 2019.

[49] M. Yassen, "Chaos synchronization between two different chaotic systems using active control," *Chaos, Solitons & Fractals*, vol. 23, no. 1, pp. 131–140, 2005.

[50] T.-L. Liao and S.-H. Tsai, "Adaptive synchronization of chaotic systems and its application to secure communications," *Chaos, Solitons & Fractals*, vol. 11, no. 9, pp. 1387–1396, 2000.

[51] M. K. Gupta, N. K. Tomar, V. K. Mishra, and S. Bhaumik, "Observer design for semilinear descriptor systems with applications to chaos-based secure communication," *International Journal of Applied and Computational Mathematics*, vol. 3, no. 1, pp. 1313–1324, 2017.

[52] H. Zhang, W. Zhang, Y. Zhao, M. Ji, and L. Huang, "Adaptive state observers for incrementally quadratic nonlinear systems with application to chaos synchronization," *Circuits, Systems, and Signal Processing*, vol. 39, no. 3, pp. 1290–1306, 2020.

[53] L. Ren and R. Guo, "Synchronization and antisynchronization for a class of chaotic systems by a simple adaptive controller," *Mathematical problems in engineering*, vol. 2015, 2015.

[54] J. Ma, F. Li, L. Huang, and W.-Y. Jin, "Complete synchronization, phase synchronization and parameters estimation in a realistic chaotic system," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 9, pp. 3770–3785, 2011.

[55] H. Du, Q. Zeng, C. Wang, and M. Ling, "Function projective synchronization in coupled chaotic systems," *Nonlinear Analysis: Real World Applications*, vol. 11, no. 2, pp. 705–712, 2010.

[56] J. H. Park, "Adaptive synchronization of rossler system with uncertain parameters," *Chaos, Solitons & Fractals*, vol. 25, no. 2, pp. 333–338, 2005.

[57] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik*, vol. 181, pp. 779–785, 2019.

[58] L. Moysis, A. Tutueva, K. Christos, and D. Butusov, "A chaos based pseudo-random bit generator using multiple digits comparison," *Chaos Theory and Applications*, vol. 2, no. 2, pp. 58–68, 2020.

[59] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1273–1284, 2018.

[60] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," *IEEE Transactions on Signal Processing*, vol. 68, pp. 1937–1949, 2020.

[61] S. L. Brunton, J. L. Proctor, and J. N. Kutz, "Discovering governing equations from data by sparse identification of nonlinear dynamical systems," *Proceedings of the national academy of sciences*, vol. 113, no. 15, pp. 3932–3937, 2016.