

Chaotic based multimedia encryption: a survey for network and internet security

Obaida M. Al-Hazaimeh¹, Ashraf A. Abu-Ein², Malek M. Al-Nawashi¹, Nasr Y. Gharaibeh²

¹Department of Computer Science and Information Technology, Al-Balqa Applied University, As-Salt, Jordan

²Department of Electrical Engineering, Al-Balqa Applied University, As-Salt, Jordan

Article Info

Article history:

Received Dec 22, 2021

Revised May 9, 2022

Accepted Jun 1, 2022

Keywords:

Chaotic maps

Cryptanalysis attacks

Encryption categories

Multimedia data

Security analysis

ABSTRACT

Nowadays the security of multimedia data storage and transfer is becoming a major concern. The traditional encryption methods such as DES, AES, 3-DES, and RSA cannot be utilized for multimedia data encryption since multimedia data include an enormous quantity of redundant data, a very large size, and a high correlation of data elements. Chaos-based approaches have the necessary characteristics for dynamic multimedia data encryption. In the context of dynamical systems, chaos is extremely dependent on the initial conditions, non-convergence, non-periodicity, and exhibits a semblance of randomness. Randomness created from completely deterministic systems is a particularly appealing quality in the field of cryptography and information security. Since its inception in the early '90s, chaotic cryptography has seen a number of noteworthy changes. Throughout these years, several scientific breakthroughs have been made. This paper will give an overview of chaos-based cryptography and its most recent advances.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Obaida M. Al-Hazaimeh

Department of Computer Science and Information Technology, Al-Balqa Applied University

As-Salt, Jordan

Email: dr_obaida@bau.edu.jo

1. INTRODUCTION

It has become increasingly common in recent years for people to use multimedia data, particularly images, video, and audio data. The confidentiality, integrity, and identity or ownership of some multimedia data, such as that found in entertainment, politics, economics, militaries, industries, and educational institutions, must be ensured in order to maintain its value [1], [2]. There are numerous practical uses of cryptology, which looks to be an efficient method of protecting information, in this regard. Despite this, the classical number theory and algebraic concepts that underlie most text or binary data encryption ciphers, such as the data encryption standard (DES), advanced encryption standard (AES), international data encryption algorithm (IDEA), and the rivest-shamir-adleman (RSA) algorithm created by Rivest, Shamir, and Adleman, do not appear to be appropriate for multimedia applications. This is due to the different reasons such as very large-size, strong correlations, similar gray-scale values, and high redundancy [3]-[7].

Recently, there has been a surge in interest to implement the encryption process using chaotic theory. The main advantage of these encryptions stems from the observation that a chaotic signal appears to non-authorized users as noise, regardless of the mechanism used to generate it. Second, the chaotic signal's time evolution is strongly influenced by the initial conditions and the control parameters of the generating functions (i.e., when these quantities are changed even slightly, the temporal evolutions vary dramatically). Furthermore, the cost of generating a chaotic signal is often low, making it suitable for multimedia

applications. For these reasons, chaos-based multimedia encryption algorithms have attracted considerable attention and have made significant development over the past few years [5], [8], [9].

2. CHAOS THEORY FOR CRYPTOGRAPHY

The initial conditions of the deterministic system are extremely sensitive and cannot be described with infinite precision, resulting in an apparently random behavior in the chaotic dynamical system. The chaotic system's is unpredictable behavior, therefore it resembles noise in this respect. Chaos-based cryptographic algorithms are an obvious choice for safe communication and cryptography because of the tight connection between the two fields [10]-[12]. Tight connection between cryptographic algorithms and chaotic maps can be seen in their sensitivity to changes in initial conditions and control parameters, pseudorandom behavior, and unstable periodic orbits with long periods [6], [13], [14]. In the multimedia data such as image can be encrypted using chaos because some dynamic systems are capable of producing random sequences of numbers that are difficult to predict. Encryption of data is accomplished by utilizing these patterns. As a result of pseudorandom behavior, the system's output appears random to the attacker, while it appears defined to the receiver and decryption is possible [1], [15]. Chaos maps, on the other hand, can only be applied to real numbers, whereas encryption transformations can be applied to finite sets. In cryptography, the parameters of a chaos map are equivalent to the encryption key. The equivalent factors of these fields are presented in Figure 1 [2], [16], [17].

A chaotic map can be used in two ways in a cipher system: To begin, use chaotic systems to generate a pseudorandom key stream. Second, as the initial conditions and control parameters, use plain text or the secret key(s). Finally, some chaotic systems iteration is applied to generate the cipher text [10], [18], [19].

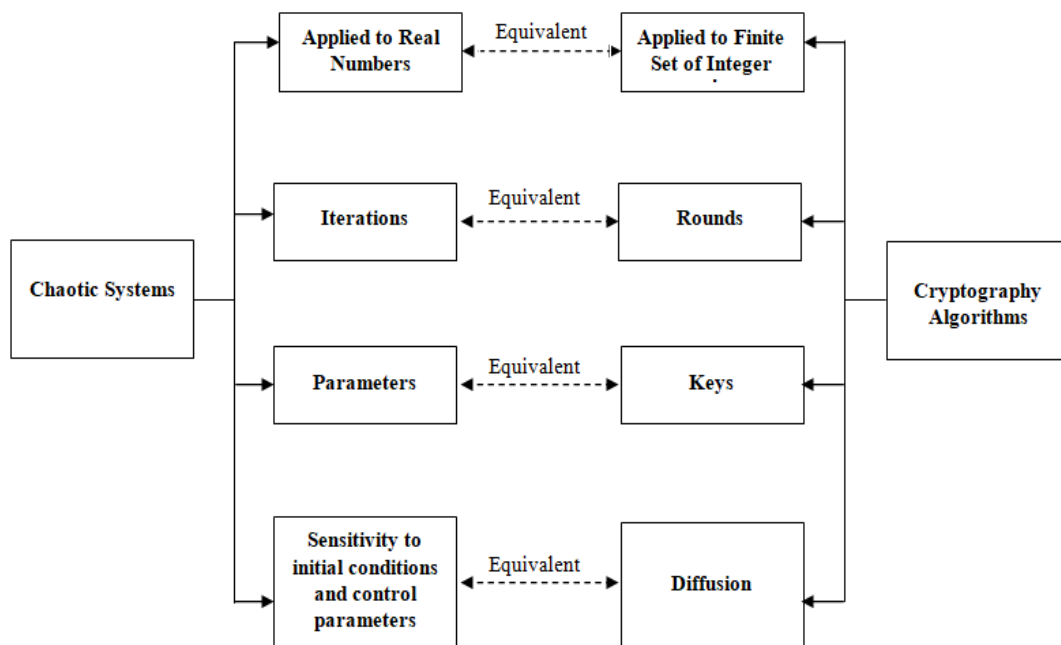


Figure 1. Equivalent factors

3. CHAOTIC MAPS

Chaotic maps are evolution functions that demonstrate some type of chaotic behavior in math. Both discrete-time and continuous-time parameters can be used to parameterize map. Taxonomy of chaotic maps is illustrated in Figure 2 [15]-[20].

Maps of discrete and continuous chaotic systems are frequently used in the study of dynamical systems. The most common chaotic maps are listed in Table 1 [13]. Chaotic cryptosystems have important and profound qualities that can be directly integrated with conventional cryptography to create a resistant statistical test attacks cipher (i.e., secure enough). Figure 3 depicts the features of deterministic chaotic cryptosystems [2], [6].

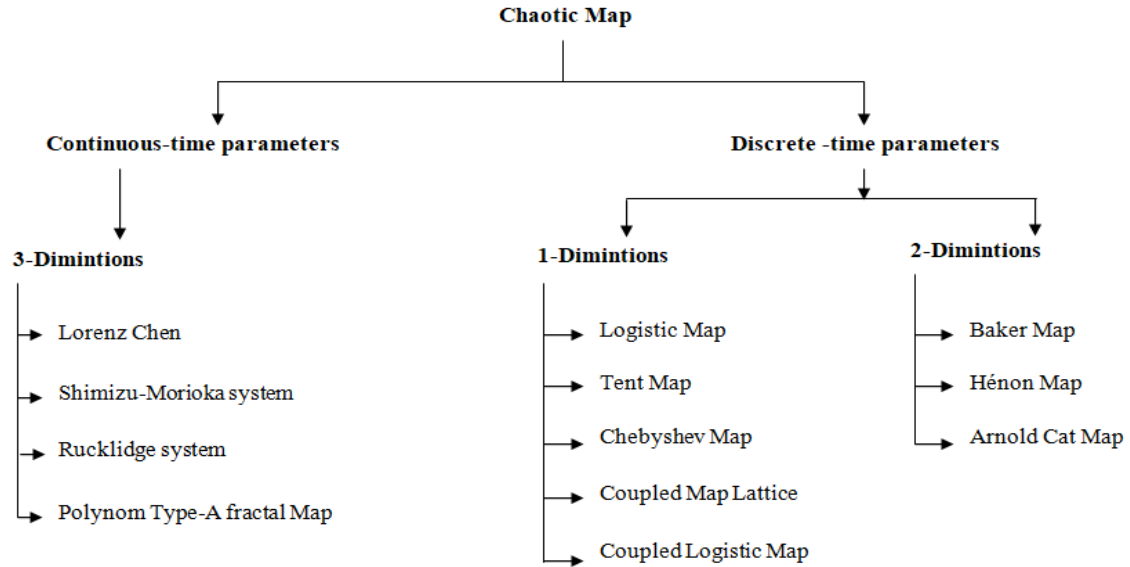


Figure 2. Taxonomy of chaotic maps

Table 1. List of most common chaotic maps

Chaotic map	Time	Space	Dimintion	Parameter	Formula	Ref.
Lorenz map	Continuous	Real	3-D	3	$\dot{x} = a(y - x),$ $\dot{y} = (\sigma - z)x - y,$ $\dot{z} = xy - bz.$	[2]
Bogdanov map	Discrete	Real	2-D	3	$x' = x + y',$ $y' = y + \epsilon y + kx(x - 1) + \mu xy.$	[14]
Hénon map	Discrete	Real	2-D	2	$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2 \\ y_{n+1} = bx_n \end{cases}$	[9]
Logistic map	Discrete	Real	1-D	1	$X_{n+1} = \alpha X_n(1 - X_n)$	[6]
Zaslavskii map	Discrete	Real	2-D	4	$X_{n+1} = [x_n + v(1 + My_n) + \epsilon v M \cos(2\pi x_n)] \% 1$	[15]
Arnold cat map	Discrete	Real	2-D	0	$Y_{n+1} = e^{-r(y_n + \epsilon \cos(2\pi x_n))}$ $(x, y) \rightarrow (2x + y, x + y) \% 1$	[16]
Chebyshev map	Discrete	Real	2-D	2	$(1 - x^2)y^n - xy' + n^2y = 0$ $(1 - x^2)y^n - 3xy' + n(n + 2)y = 0$	[7]
Circle map	Discrete	Real	1-D	2	$\theta_{i+1} = g(\theta_i) + \Omega$	[17]
Chua circuit	Continuous	Real	3-D	3	$\frac{dx}{dt} = \alpha[y - x - f(x)],$ $RC_2 \frac{dy}{dt} = x - y + R_2$ $\frac{dz}{dt} = \beta y$	[19]
Lorenz 96 model	Continuous	Real	2-D	1	--	[18]
Tent map	Discrete	Real	1-D	2	$f_\mu := \min\{x, 1 - x\}$	[1]
Coupled logistic map	Discrete	Real	1-D	2	$x_{n+1} = \epsilon[r x_n(1 - x_n)]s + (1 - \epsilon)[r x_n(1 - x_n)]s - 1$	[13]
Baker map	Discrete	Real	2-D	1	$S(x) = \begin{cases} 2x, & 0 \leq x < 0.5 \\ 2(1 - x), & 0.5 \leq x < 1 \end{cases}$	[1]

Chaos functions are used to develop the mathematical model of nonlinear systems. The chaotic function has a variety of intriguing characteristics. These functions repeatedly generate the random sequence. Ergodicity, sensitivity to initial conditions, and random-like behavior are all characteristics of chaotic systems. As a result, different chaotic maps have different computational demands, key spaces, and key sensitivities[1]. The confusion stage and the diffusion stage are the two most important stages in a chaos-based image cryptosystem. Figure 4 illustrates a typical architecture block diagram [1], [18].

The confusion stage, this stage is called pixel permutation, and it's when all of the image's pixels are scrambled without affecting the values of the individual pixels. Diffusion stage, it is in this step that the pixel values are modified successively by the chaotic system sequence. Confidence and security can only be achieved after several rounds of confusion and diffusion. A chaotic map's unpredictability quality makes it ideal for multimedia data encryption such as image [19].

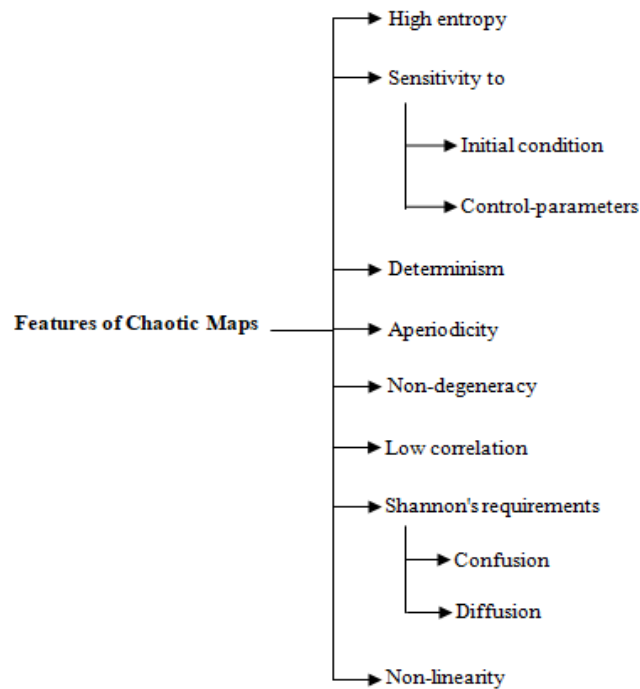


Figure 3. Chaotic cryptosystems features

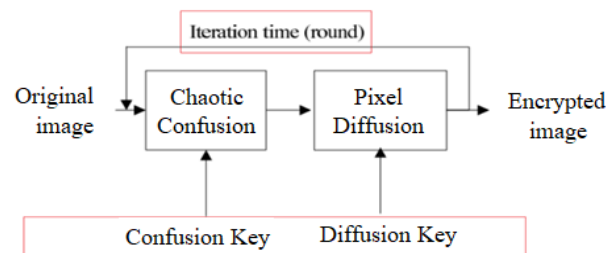


Figure 4. Image encryption architecture based on chaos

4. CHAOS-BASED ENCRYPTION ALGORITHMS

Many different methods of encryption based on chaos have been proposed thus far. Full and partial encryption algorithms are categorized based on the percentage of data that has been encrypted (also called selective encryption) as shown in Figure 5. Block and stream encryption are additional classifications for the two types of encryption, depending on the ciphers used [11], [20].

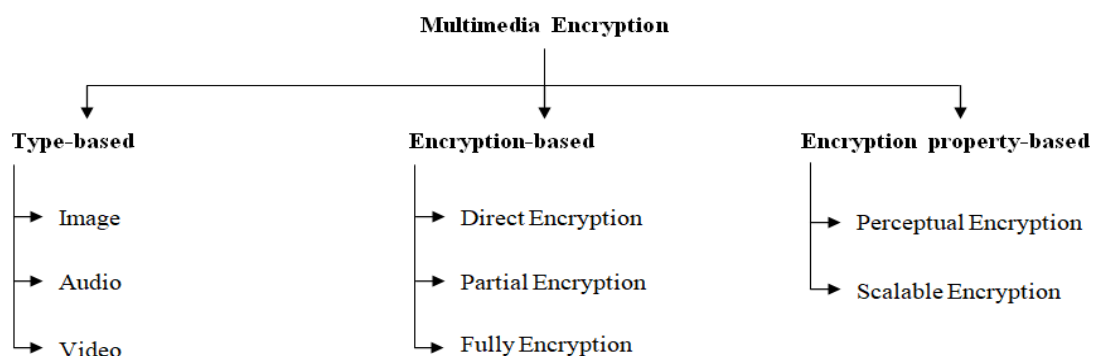


Figure 5. Encryption categories

Sakthidasan *et al.* [21] proposed a new scheme, the proposed cryptosystem scheme comprises of two stages: confusion and diffusion. In all stages of confusion and diffusion, a variety of chaotic systems are applied. To increase the method's complexity even further, we're using complex chaotic maps instead of simple ones, thus enhancing the security. One of the 3D chaotic systems is used for pixel position permutation in the confusion stage. The next step is the diffusion stage, in which the pixel value diffusion is repeated using any of the chaotic systems that were used previously. In both stages, the secret key is the initial conditions and the control parameters used to generate the chaotic sequence.

Anto *et al.* [22] image encryption and decryption utilizing two chaotic maps is proposed in this new algorithm. Lorenz and Baker maps are utilized for the two chaotic systems. The authors use a two-stage encryption method that involves creating confusion and then dispersing that confusion. The pixel values and positions are shuffled throughout the confusion and diffusion stage depending on which of the two chaotic systems, Lorenz or Baker, is used. The chaotic sequence is generated using separate keys in both steps. Reverse operations are carried out in the decryption stage, allowing the original image to be decrypted.

Al-hazaimah *et al.* [2] image encryption is proposed using Lorenz's chaotic map with dynamic secret keys. In this study, a method for encrypting digital images is proposed using the Lorenz system. An image's hash value is included in the proposed cryptosystem during the chaotic key generation process to dynamically update the initial secret keys in order to increase security. Using the experimental results, it can be concluded that the suggested technique is efficient, secure, and acceptable for practical application on insecure networks.

In Al-Maadeed *et al.* [23] a pixel shuffler unit and a stream cipher unit are used in this paper to create a new image encryption method. For image encryption, pixel scrambling has two key advantages. Diffusion not only moves pixels around, but also alters the values of each pixel's value (i.e., confusion). Stream ciphers use non-linear function operations to perform confusion. The pixel shuffler unit has a permutation map that may be applied in both vertical and horizontal directions to reduce the correlation between neighboring pixels. As a pseudorandom number generator, the Hénon map (2D) is used to create a permutation matrix. Now the W7 algorithm is used after pixel permutation. This approach generates a pseudorandom cipher bit stream known as the key stream, which is equivalent to the scrambled image binary sequence. XORing the key stream with the shuffled image binary sequence generates the cipher image.

In Gupta *et al.* [24], three different images (red, green, and blue) are created for the main image of size $M \times N$. During the transformation of the red and green images, the blue image is preserved as it was. One row from each of the three image planes is taken from the rotated image to generate a plane of the three image planes. 2D cat maps are the first level of confusion. The final level of confusion is performed by a cascade of two maps, first a cat map and then a standard map. The diffusion stage follows the confusion stage, and the cipher image is created by XORing each pixel of the confused image with the diffused image. Al-hazaimah *et al.* [14] based on Chen system and Bogdanov map anti-synchronization, a new image encryption technique is proposed. In this paper, to demonstrate the new algorithm's performance and robustness against various cryptanalytic attacks, some of these analyses are presented in this paper. The proposed technique can be used to provide an appropriate application over unsecure networks, according to the security analyses. In addition, Chen's anti-synchronization system and Bogdanov's transformation map can be used in a wide range of different applications, including real-time applications (i.e., video encryption).

Chattopadhyay *et al.* [3] introduced a new chaos –based encryption algorithm. Using a matrix representation, the image has a range of gray levels from 0 to 1. The pixel matrix is transformed into an array. mod is used to convert pixel values to unsigned integers in the range 0-255. Using a circle map with an initial condition and control parameter, a chaotic sequence in the range 0 to 1 is generated. An intermediate cipher is constructed by XORing the pixel array with the chaotic sequence. There are several steps involved in the process of creating the final cipher. To obtain the final cipher image, the resulting cipher array is converted.

Zhang *et al.* [25] applied image encryption based on chaotic map. Images were encrypted using the use of discrete exponential chaotic maps (SDEC). Permutation of plain-image pixels is used in SDEC, as shown in Figure 6, and "XOR plus mod" operations are used. It is also possible to build a key stream that is resistant to statistical assault, differential attack, and linear attack using a time-variable-parameter piece-wise linear map (i.e., TVPPLM) [26].

El-Khamy *et al.* [27] based on Elknz chaotic stream cipher and discrete wavelet transform, a partial image encryption (PDEC) system was proposed as illustrated in Figure 7. A single-level 2-D discrete wavelet transform (2-DDWT) generates four coefficient matrices: the horizontal (ch), approximation (ca), diagonal (cd), and vertical (cv) matrices, respectively. When it comes to encrypting only the image's main matrix, the Elknz cipher is used to scramble all of the other sub-bands of the image. To create the encrypted image, a 2-D inverse discrete wavelet transform is applied to the scrambled ch, cv, and cd matrices and the encrypted ca matrix.

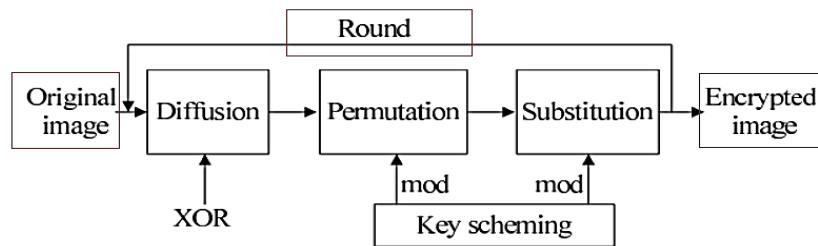


Figure 6. Image encryption architecture

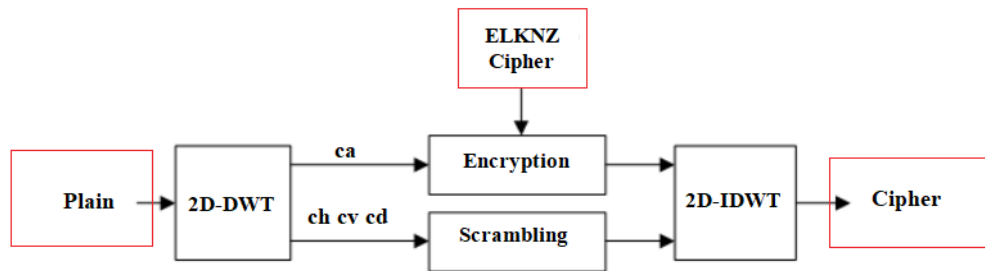


Figure 7. Architecture of image encryption

Ntalianis *et al.* [28] proposed a chaotic encryption method that uses video objects (VOCE). When using VOCE, color information is fused together to automatically identify video objects. The pixels of the lowest resolution level are then encrypted using a complex product cipher that combines a chaotic stream cipher with two chaotic block ciphers, followed by multi-resolution decomposition for each video object. This process is repeated until all of the encrypted regions have been propagated to higher resolution levels. In terms of brute-force and known cryptanalytic attacks, the VOCE is extremely resistant.

Lian *et al.* [29] developed an efficient selective encryption system based on chaos for multimedia data (CSVE) depicted in Figure 8. For each frame, the 2-D coupled map lattice is used to encode only the direct current coefficients the alternating current coefficients (i.e., 2-D CML). DCT transformation and quantization block partitioning (8 x 8 in size each block), color space transformation, and post-encoding are all done before encryption is applied. The CSVE has a high sensitivity to keystrokes and a high degree of security. As a result, its encryption process has a minimal impact on the compression ratio and is much less expensive than video compression.

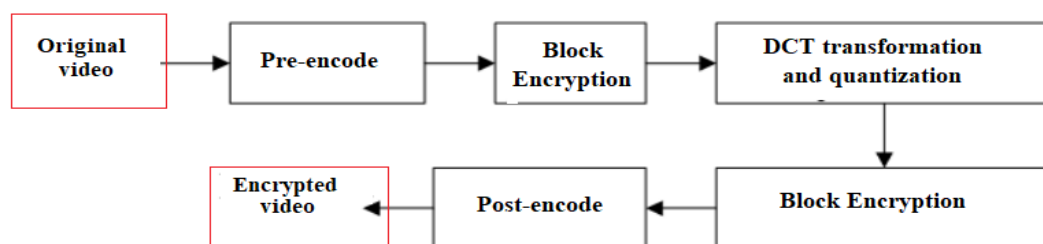


Figure 8. Video encryption scheme

5. SECURITY ANALYSIS

Obtaining the weaknesses in a cryptosystem and retrieving either the whole or portion of a ciphered multimedia data or finding the secret key without knowing the algorithm's decryption key is known as "security analysis". If the analyst has access to the plain-text, cipher-text, or other components of cryptosystem, they can use a variety of approaches to perform analysis [30]-[31]. Table 2 summarizes some of the most popular types of attacks on encrypted multimedia data.

Table 2. List of most common cipher attacks

No.	Analysis	Description
1	Key space	The key space of the cryptosystem expands exponentially with increasing key size, and the number of attempts to find the decryption key by checking all possible keys.
2	Key sensitivity	For a successful multimedia data encryption scheme, the secret key utilized must be extremely sensitive. The encrypted or decrypted image should be absolutely different if a single bit of the secret key is changed.
3	Statistical	The statistical analysis of the multimedia data such as image shows the correlation between the original and ciphered data. Cipher images must therefore be absolutely different from the original.
4	Correlation co-efficient	Coefficient of correlation is a statistical measure of the relationship between the relative movements of two variables. The values range from a negative one to a positive one. In multimedia data such as image, is the cross-correlation between neighboring pixels in the plain image and in the encrypted multimedia data on the vertical, horizontal, and diagonal.
5	Information entropy	Entropy is a measure of how random the data is, and there are no meaningful patterns to be detected. It is possible to anticipate future values if the data is low in entropy.
6	Differential	The goal of this analysis is to find out how sensitive the encryption method is to even the smallest of changes. The encrypted multimedia data such as image should be completely affected if an attacker is able to make a small change (such as one pixel) to the plain image.

6. COMPARISON OF DIFFERENT ENCRYPTION SCHEMES- BASED CHAOTIC MAPS

Encryption systems are tested using a variety of security techniques, including those detailed in previous section (i.e., section 4), to ensure that they perform well and are secure. A table summarizing the security analysis results is presented in Table 3. Using chaos theory, it is possible to analyze each method of multimedia data encryption in the table.

Table 3. Security analysis resultsfor various chaos based cryptography schemes

Ref.	Key space	Key sensitivity	Results							
			Horizontal		Correlation		Diagonal		Entropy	
			Plain	Cipher	Plain	Cipher	Plain	Cipher	NPCR	UACI
[21]	Large	Medium	0.9791	0.0052	0.9357	0.0539	0.9183	0.1141	99.51	32.9
[22]	2 ¹²⁸	High	0.9598	-0.003	0.9763	-0.002	-	-	-	-
[2]	Large	High	0.933323	0.00732999	0.956482	0.00548614	-	-	99.6	33.24
[23]	2 ¹²⁸	High	0.9976	0.0096	0.9924	0.0038	-	-	0.0015	0.0005
[24]	2 ¹⁴⁸	High	0.9156	0.001	0.8808	0.006	0.8603	0.091	99.62	33.19
[14]	Large	High	0.933098	0.00674988	0.956726	0.00527721	0.908045	0.00655692	99.6002	33.4146
[3]	2 ²⁵⁶	High	0.9712	0.0012	0.9698	0.0032	0.9861	0.0058	99.63	33.01
[27]	Large	High	0.9341	0.0014	0.9634	0.0036	0.9402	0.0028	99.52	32.09
[29]	Large	High	0.92.5	0.0021	0.9808	0.0038	0.9601	0.0901	99.43	32.58
[30]	Large	High	0.8991	0.0060	0.8959	0.0493	0.8997	0.1150	99.64	33.02
[31]	Large	High	0.9651	0.0085	0.9652	0.0493	0.9685	0.0984	99.60	33.01

7. CONCLUSION

To communicate via open networks like the internet, security of digital images has become critical. Chaos-based multimedia data encryption techniques have been explored and examined in this study to evaluate their efficacy against a variety of attacks. For real-time application security, all of the encryption techniques are useful, and each one is unique in its own way, which is acceptable for different applications. Using numerous chaotic maps for multimedia data encryption can increase security. Further exploration of the chaotic maps is necessary, as there are many more to be found. As a result, encryption, which can be referred to as a scientific art, should always demonstrate a high level of security.




REFERENCES

- [1] Z. Su, G. Zhang, and J. Jiang, "Multimedia security: a survey of chaos-based encryption technology," *Mutimedia: A Multidisiplinary Approach to Complex Issues, Ed. I. Karydis, InTech*, pp. 99-124, 2012, doi: 10.5772/36036.
- [2] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, pp. 2395-2405, 2019, doi: 10.1007/s00521-017-3195-1.
- [3] D. Chattopadhyay, M. Mandal, and D. Nandi, "Symmetric key chaotic image encryption using circle map," *Indian Journal of Science and Technology*, vol. 4, pp. 593-599, 2011, doi: 10.17485/ijst/2011/v4i5.27.
- [4] O. M. Al-Hazaimeh, N. Alhindawi, and N. A. Otoum, "A novel video encryption algorithm-based on speaker voice as the public key," in *2014 IEEE International Conference on Control Science and Systems Engineering*, 2014, pp. 180-184, doi: 10.1109/CCSSE.2014.7224533
- [5] M. F. Abd Elzaher, M. Shalaby, and S. H. El Ramly, "Securing modern voice communication systems using multilevel chaotic approach," *International Journal of Computer Applications*, vol. 135, no. 9, pp. 17-21, 2016, doi:10.5120/ijca2016908497.





- [6] N. Tahat, A. A. Tahat, M. Abu-Dalu, R. B. Albadarneh, A. E. Abdallah, and O. M. Al-Hazaimeh, "A new RSA public key encryption scheme with chaotic maps," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 1430-1437, 2020, doi: 10.11591/ijece.v10i2.pp1430-1437.
- [7] N. Tahat, A. Alomari, A. Al-Freedi, O. M. Al-Hazaimeh, and M. F. Al-Jamal, "An efficient identity-based cryptographic model for Chebyhev chaotic map and integer factoring based cryptosystem," *Journal of Applied Security Research*, vol. 14, no. 3, pp. 257-269, 2019, doi: 10.1080/19361610.2019.1621513.
- [8] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, pp. 408-419, 2008, doi: 10.1016/J.CHAOS.2006.05.011.
- [9] O. M. Al-hazaimeh, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 3 pp. 2203-2210, 2021, doi: 10.11591/IJECE.V11I3.PP2203-2210.
- [10] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3 pp. 6-21, 2001, doi:10.1109/7384.963463.
- [11] M. Jafarizadeh and S. Behnia, "Hierarchy of one-and many-parameter families of elliptic chaotic maps of cn and sn types," *Physics Letters A*, vol. 310, pp. 168-176, 2003, doi: 10.1016/S0375-9601(03)00343-8.
- [12] K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps," *International Journal of Theoretical Physics*, vol. 58, pp. 3091-3117, 2019, doi: 10.1007/S10773-019-04188-3.
- [13] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1-13, 2019, doi: 10.1016/j.sigpro.2018.11.010.
- [14] O. M. Al-Hazaimeh, M. F. Al-Jamal, A. K. Alomar, M. J. Bawaneh, and N. Tahat, "Image encryption using anti-synchronization and Bogdanov transformation map," *Int. J. of Computing Science and Mathematics*, vol. 15, pp. 43-59, 2022, doi: 10.1504/ijcsm.2022.122144.
- [15] M. Khan and T. Shah, "A novel construction of substitution box with Zaslavskii chaotic map and symmetric group," *Journal of Intelligent & Fuzzy Systems*, vol. 28, pp. 1509-1517, 2015, doi: 10.3233/IFS-141434.
- [16] B. Raj, L. J. Anbarasi, M. Narendra, and V. Subashini, "A new transformation of 3D models using chaotic encryption based on arnold cat map," in *International Conference on Emerging Internetworking, Data & Web Technologies*, 2019, vol. 29, pp. 322-332, doi: 10.1007/978-3-030-12839-5_29.
- [17] Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, "Image encryption algorithm with circle index table scrambling and partition diffusion," *Nonlinear Dynamics*, vol. 103, pp. 2043-2061, 2021, doi: 10.1007/S11071-021-06206-8.
- [18] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 4824-4834, 2020, doi: 10.11591/ijece.v10i5.pp4824-4834.
- [19] R. Brown and L. O. Chua, "Clarifying chaos: Examples and counterexamples," *International Journal of Bifurcation and Chaos*, vol. 6, no. 2, pp. 219-249, 1996, doi: 10.1142/S0218127496000023.
- [20] M. A.-H. Obaida, "Combining audio samples and image frames for enhancing video security," *Indian Journal of Science and Technology*, vol. 8, no. 10, pp. 940-949, 2015, doi: 10.17485/IJST/2015/V8I10/53149.
- [21] K. Sakthidasan and B. S. Krishna, "A new chaotic algorithm for image encryption and decryption of digital color images," *International Journal of Information and Education Technology*, vol. 1, no. 2, pp. 137-141, 2011, doi: 10.7763/IJNET.2011.V1.23.
- [22] A. A. Steffi and D. Sharma, "Modified algorithm of encryption and decryption of images using chaotic mapping," *International Journal of Science and Research (IJSR)*, vol. 2, no. 2, pp. 77-80, 2013.
- [23] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," *Journal of Electrical and computer Engineering*, vol. 2012, 2012, doi: 10.1155/2012/179693.
- [24] K. Gupta and S. Silakari, "New approach for fast color image encryption using chaotic map," *Journal of Information Security*, vol. 2, no. 4, pp. 139-150, 2011, doi: 10.4236/jis.2011.24014.
- [25] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 23, pp. 759-765, 2005, doi:10.1016/J.CHAOS.2004.09.035.
- [26] Y.-h. Qiu, C. He, and L.-g. Jiang, "Construction and analysis of one class of chaotic running key generator," *Journal-Shanghai Jiaotong University-Chinese Edition*, vol. 36, no. 3, no. 1, pp. 0344-347, 2002.
- [27] S. El-Khamy, M. El-Nasr, and A. El-Zein, "A partial image encryption scheme based on the dwt and elknz chaotic stream cipher," *MASJUM Journal of basic and applied sciences*, vol. 1, pp. 389-394, 2009.
- [28] K. S. Ntalianis and S. D. Kollias, "Chaotic video objects encryption based on mixed feedback, multiresolution decomposition and time-variant S-boxes," in *IEEE International Conference on Image Processing 2005*, 2005, pp. II-1110, doi: 10.1109/ICIP.2005.1530254.
- [29] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2509-2519, 2009, doi: 10.1016/J.CHAOS.2007.10.054.
- [30] S.-J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST statistical test suite for randomness," *arXiv preprint nlin/0401040*, 2004, doi: 10.48550/arXiv.nlin/0401040.
- [31] M. Sýs and Z. Říha, "Faster randomness testing with the NIST statistical test suite," in *International Conference on Security, Privacy, and Applied Cryptography Engineering*, 2014, pp. 272-284, doi: 10.1007/978-3-319-12060-7_18.

BIOGRAPHIES OF AUTHORS







Obaida M. Al-Hazaimeh    earned a BSc in Computer Science from Jordan's Applied Science University in 2004 and an MSc in Computer Science from Malaysia's University Science Malaysia in 2006. In 2010, he earned a PhD in Network Security (Cryptography) from Malaysia. He is an associate professor at Al-Balqa Applied University's department of computer science and information technology. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 42 papers in international refereed publications as an author or co-author. He can be contacted at email: dr_obaida@bau.edu.jo.







Ashraf A. Abu-Ein     is an Associate Professor in the Department of Electrical Engineering. He has completed his PhD at National Technical University of Ukraine, Computer Engineering. “Computers, Computing Systems and Networks”, 2007. Now, he is a lecturer at Al-Balqa Applied University-Al-huson University College, Jordan. He can be contacted at email: ashraf.abuain@bau.edu.jo.



Malek M. Al-Nawashi     is an Assistance Professor in the Department of of computer science and information technology. He has completed his PhD at University of Salford Manchester in Computer Science in 2019. Now, he is a lecturer at Al-Balqa Applied University–Al-huson University College, Jordan. He can be contacted at email: nawashi@bau.edu.jo.



Nasr Y. Gharaibeh     is an Assistance Professor in the Department of electrical Engineering. He received his PhD in Electrical engineering in 1990. Now, he is a lecturer at Al-Balqa Applied University–Al-huson University College, Jordan. He can be contacted at email: nas@bau.edu.jo.