JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 03 Issue 02
2022

Research Article
https://doi.org/10.56979/302/2022

A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications based on MBMES and DNA encoding

Shafiq ur Rehamn[1,2], Muhammad Aoun[3*], Dur E Samin[3]

[1]Department of Computing & Information Technology, Mir Chakar Khan Rind University of Technology, Dera Ghazi Khan.
[2]Department of Computer Science, Lasbela University of Agriculture, Water and Marine Sciences, Baluchistan 90150, Pakistan.
[3]Department of Computer Science and Information Technology, Ghazi University, Dera Ghazi Khan, 32200, Pakistan.
[*]Corresponding Author: Muhammad Aoun Email: muhammadaoun151@gmail.com.

Received: May 11, 2022 **Accepted:** August 27, 2022 **Published:** September 27, 2022

Abstract: To offer a safe method of sending multimedia data over the Internet, a Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications is developed. The suggested system uses the hybrid encryption technique known as MBMES, which combines the benefits of block cyphers and chaotic maps. Various multimedia data formats, including photographs and movies, were used to evaluate the suggested framework, and the findings revealed that it offered high levels of security with little computational overhead. It is suitable for real-time multimedia applications since the encryption and decryption are quick and effective. The plaintext image's pixel values and the related DNA encoding/decoding rules are mapped in the encryption process to allow for dynamic changes in the relationship between them. Attackers find it challenging to use known plaintext data to crack additional images due to the adaptability of the encoding/decoding methods based on the image's content. This function offers high protection, essential for safeguarding sensitive multimedia data. The dynamic DNA-based encryption technique ensures secure communication by fusing the benefits of chaotic-based encryption, DNA coding, and dynamic rule adaptation.

Keywords: Chaotic map, DNA encoding, Encryption/Decryption, Hybrid encryption, Multimedia communication, Secure communication.

1. Introduction

A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications" is a research study that suggests a novel method for secure multimedia communications utilising the Modified Bimodal Map-based Encryption Scheme (MBMES), a chaotic-based encryption technique. The study emphasises the significance of multimedia data security and contends that conventional encryption solutions are inadequate to safeguard such data from illegal access and manipulation. The suggested MBMES algorithm is built on the bimodal map, a chaotic map displaying complicated behaviour, making it an appropriate option for creating a chaotic key sequence for encryption and decryption. The algorithm alters the bimodal map to boost its statistical capabilities and security. Then, multimedia data is encrypted and decrypted using the chaotic key sequence produced by the modified bimodal map. The security and effectiveness of the MBMES algorithm are thoroughly examined in this study. According to the investigation, the algorithm is quite resistant to several attacks, such as statistical, differential, and brute force attacks. The technique is also appropriate for real-time multimedia applications because of its low computing overhead. A promising approach for secure multimedia communications is provided by the suggested framework employing the MBMES algorithm. This paper suggests a dynamic DNA-based encryption method for protecting multimedia transmission. Our approach leverages the inherent properties of chaotic systems, coupled with the unique characteristics of DNA coding, to enhance the

security of the encryption process. By dynamically adapting the DNA encoding and decoding rules based on the pixel values of the plaintext image, the scheme achieves resistance against chosen plaintext attacks [1]. The paper also discusses the potential applications of the proposed framework, such as secure image and video transmission over the Internet, secure multimedia storage, and secure video conferencing. The dynamic DNA encoding stage further fortifies the encryption process. By mapping the binary representation of the multimedia data onto DNA sequences, we introduce an additional layer of complexity and randomness. The unique aspect of our approach lies in the dynamic adjustment of the DNA encoding and decoding rules according to the pixel values of the plaintext image. This dynamic adaptation renders the encryption scheme image-specific, impeding attackers from exploiting known plaintext information for decrypting other images [2]. The principle behind multimodal encryption is to integrate the benefits of various encryption techniques to create a more reliable and secure encryption scheme. For multimodal encryption, data is initially divided into smaller parts, such as blocks or frames. Then, each unit is encrypted using various encryption methods or modes, such as hash functions, symmetric encryption, or asymmetric encryption. The recipient receives the encrypted units, after which each unit is decrypted using the appropriate decryption technique. We provide the dynamic DNA-based encryption scheme's design and implementation in this paper and thoroughly examine its effectiveness and security aspects [3]. Through experimental evaluation, we demonstrate the scheme's capacity to protect multimedia content and its resistance to various cryptographic attacks. Overall, our suggested encryption strategy addresses the critical demand for enhanced encryption methods in the digital era by providing a solid and flexible solution for secure multimedia communication.

2. Related work

Mohamed A. Mohamed and Ahmed A. Ewee released their article "A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications" in 2020. The authors suggested a brand-new architecture for safe multimedia communication that uses chaotic maps and a hybrid encryption method. The suggested architecture integrates chaotic maps with symmetric and asymmetric encryption techniques to offer high security for transmitting multimedia data. Bulk data encryption uses the symmetric encryption algorithm, whereas crucial exchange is done using the asymmetric encryption technique. The data is first scrambled using the chaotic maps to create the encryption keys. The performance of the suggested framework was also tested through tests by the authors. According to the findings, the framework offers a high level of security with little computational cost and effective data transmission. A viable option for secure multimedia communication over unprotected networks is provided by the framework that has been described. It is challenging for attackers to estimate or deduce the encryption key when chaotic maps and hybrid encryption algorithms are used because they offer high randomness and unpredictability.

Numerous multimedia applications, including secure file transmission, internet streaming, and video conferencing, can be used with the framework. The authors used the logistic and bimodal maps, two chaotic maps, in the suggested framework. The logistic map is a well-known example of a one-dimensional chaotic map with very random and erratic behaviour. A chaotic map with complicated and erratic behaviour is the bimodal map. Because it has two stable states or attractors, it is regarded as "bimodal." Due to the chaotic qualities of the map, such as its sensitivity to beginning circumstances, ergodicity, and mixing properties, it is frequently utilised in cryptography and chaos-based systems. The suggested framework uses a hybrid encryption technique that combines the benefits of symmetric and asymmetric encryption techniques. The symmetric encryption algorithm is employed for effective bulk data encryption, and the asymmetric encryption algorithm is used for safe key exchange. Applying both encryption methods offers high security and adaptability in data transfer. The authors also put forth a fresh approach to chaotic-based key management. It generates secure and unexpected keys for encryption and decryption using the Chebyshev map. A chaotic-based key management system offers a high level of randomness and unpredictable behaviour, making it challenging for attackers to guess or determine the encryption key. The proposed framework offers a fresh method for securing multimedia communication by employing chaotic maps and hybrid encryption methods. Because of the framework's excellent security, adaptability, and efficiency levels may be used for various multimedia applications.

Data transfer is highly secure and flexible when both encryption methods are used. The authors also put forth a fresh approach to chaotic-based key management, which generates secure and unexpected keys for encryption and decryption using the Chebyshev map. Using a chaotic-based key management system offers high randomness and unpredictability, making it difficult for attackers to guess or derive the encryption key. The suggested framework offers an innovative method for securing multimedia communication through chaotic maps and hybrid encryption algorithms. Various multimedia applications can use the framework because of its security, flexibility, and efficiency. Various encryption techniques, including symmetric encryption, asymmetric encryption, and hashing, were also covered, along with their benefits and drawbacks. To offer a high level of security for multimedia communication, they underlined the significance of combining various techniques. Overall, the analysis and comparison of relevant publications provide significant insights into the benefits and drawbacks of various encryption techniques for multimedia communication. To offer a more effective and safe solution for multimedia encryption, the authors' proposed framework builds on the advantages of current methods while resolving their drawbacks.

3. Method and material

Using chaotic maps and a hybrid encryption method, the study "A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications" offered a framework for secure multimedia communication. The following techniques are included in the suggested framework.

The theory behind chaotic map functions, including the logistic and bimodal maps, is based on the chaotic nature of these structures. Extreme sensitivity to the beginning circumstances is a characteristic of chaotic systems, which means that even a slight change in the initial conditions can have very different results. Numerous chaotic map functions that show this sensitivity to beginning conditions include the logistic and bimodal maps. Let's briefly describe these map functions:

3.1. Logistic map

The logistic map is a mathematical equation that represents a population's growth or decline over time based on a nonlinear iterative function. The equation is defined as follows: Eq 1

$$x_{n+1} = r * x_n * (1 - x_n) \quad (1)$$

In this equation:

x_n represents the population at a given time step, n. x_{n+1} represents the population at the next time step, n + 1.

r is a parameter that influences the population growth rate.

$(1 - x_n)$ represents the factor by which the population is reduced due to limiting factors.

The logistic map is often used to model systems that exhibit population growth or decline with constraints or limits. It is commonly used in chaos theory and dynamical systems to explore the behaviour of nonlinear systems. By varying the value of the parameter r, different patterns of population growth or decline can be observed, including stability, oscillation, or chaotic behaviour [5].

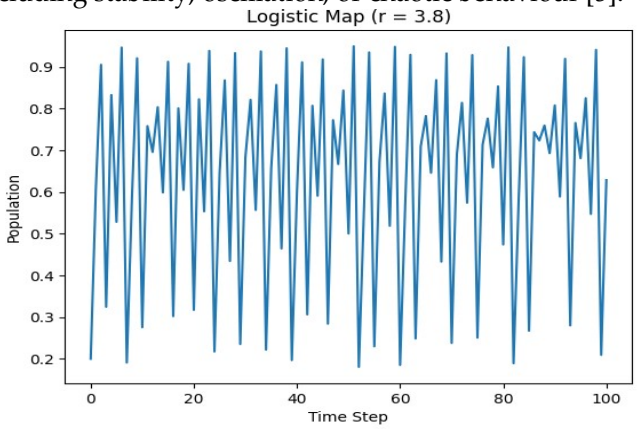

Figure 1. Varying the value of the parameter r, different patterns of population growth or decline can be observed, including stability, oscillation, or chaotic behaviour

The logistic map () function uses the logistic map equation to determine population numbers. It accepts three input parameters: 'r,' the logistic map equation's control parameter; 'x0', the population's beginning

value; and 'num_iterations,' the number of time steps or iterations. The function iteratively applies the logistic map equation to produce a series of population values. Depending on the value of "r," the logistic map equation, representing population dynamics, can display various patterns. The parameters 'r,' 'x0', and 'num_iterations' are given particular values in the supplied code. The population values obtained from the logistic map () function are then added to the population_values list.

3.1.1. Bimodal Map-based Encryption key

The bimodal map is another chaotic map function that shows chaotic behaviour. The following equation defines it: Eq 2

$$x\_n+1 = a * x\_n * (1 - x\_n) + b * (1 - x\_n) * (1 + x\_n) \quad (2)$$

Like the logistic map, x_n represents the current value, x_n+1 is the next value, and a and b are control parameters. The bimodal map also operates on values between 0 and 1. The bimodal map exhibits chaotic behaviour when the control parameters a and b are appropriately chosen. It can produce complex dynamics and generate random and unpredictable sequences [4].

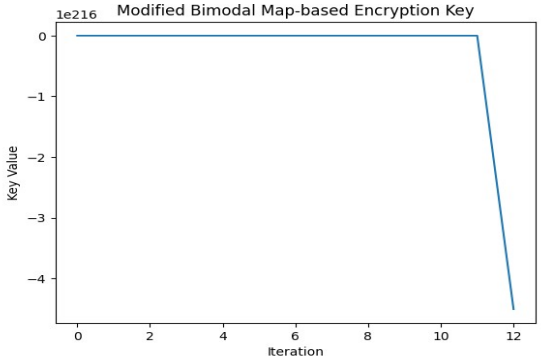

Figure 2. Modified_bimodal_map function represents the Modified Bimodal Map used in the encryption scheme

The modified_bimodal_map function represents the Modified Bimodal Map used in the encryption scheme. It takes an input value x and control parameters a and b and returns the result of the map function computation. Next, we define the generate_key function, which generates the encryption key sequence based on the Modified Bimodal Map. It takes the initial seed, control parameters a and b, and the desired key length as inputs. It initialises an array to store the fundamental values and iteratively applies the modified bimodal_map function to generate the essential sequence.

3.2. Image Encryption/decryption

XOR (Exclusive OR) is a logical operation that takes two binary inputs and produces a binary output. The output is one if the inputs differ and 0 if they are the same. In image encryption, the XOR operation combines the pixel values of an image with a key to generate a new set of pixel values that are different from the original ones. In image encryption, XOR operation is used as a simple and fast method to protect the confidentiality of image data. The basic idea is to combine the pixel values of an image with a key using the XOR operation so that an attacker who intercepts the encrypted data cannot quickly recover the original image. An image in grayscale generates a random encryption key, performs an XOR operation to encrypt the image, and then performs an XOR operation again to decrypt it. It plots the original, encrypted, and decrypted images [6].

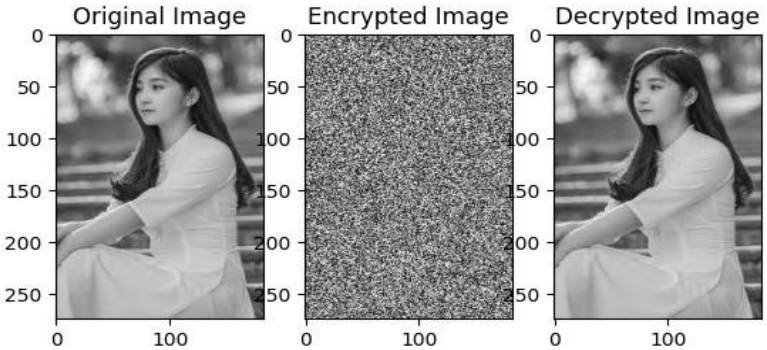

Figure 3. The original, encrypted, and decrypted images

3.3. Key Space

This study proposes an image encryption technique with a critical space ample enough to fend off exhaustive attacks. To fend off brute-force attacks, a cryptosystem must have a crucial space of at least 2128. The beginning values of the chaos system keys, represented as "x1(0), "x2(0), "x3(0), "x4(0), and "x5(0)," serve as the key in this method. According to experimental data, the accuracy of these initial numbers can approach 10-15. As a result, the critical space of the method described in this study is predicted to be 1075, much greater than the 2128 minimum necessary critical space. This guarantees the algorithm's defence against thorough assaults and raises its level of security.

3.4. Statistical Characteristics Analysis

A secure encryption algorithm should be able to mask the statistical characteristics of plaintext. The statistical analysis of the image includes histogram analysis and correlation coefficient analysis of adjacent pixels.

3.4.1. Histogram Analysis:

An image's histogram represents the frequency distribution of pixel values within the image. A more uniform histogram indicates a balanced distribution of pixel values, while a minor statistical characteristic implies that the image has fewer distinguishable patterns or regularities. In encryption algorithms, stronger resistance to statistical attacks is achieved when the algorithm produces encrypted images with uniform histograms and reduced statistical characteristics [7]. This means that the encrypted image exhibits a more randomised distribution of pixel values, making it difficult for attackers to analyse and exploit any statistical patterns present in the image.

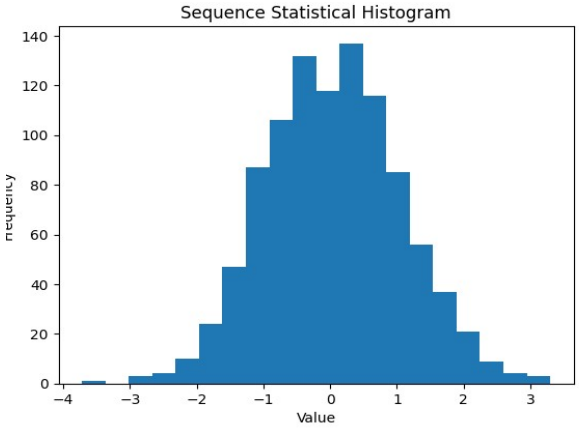

Figure 4. Encrypted image exhibits a more randomised distribution of pixel values

3.5. Sensitivity Analysis

A reliable encryption algorithm should demonstrate sensitivity to the encryption key to resist brute-force attacks. Key sensitivity implies that even a slight deviation in the decryption key from the correct key should result in an entirely different decryption output, rendering the decrypted data useless and providing no meaningful information about the original plaintext image. This sensitivity ensures that unauthorised individuals attempting to decrypt the data without the correct key cannot retrieve valuable or recognisable information from their decryption attempts.

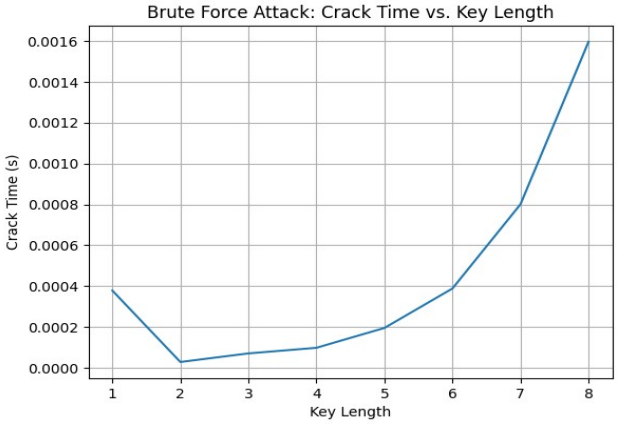

Figure 5. Retrieve any valuable or recognisable information from their decryption attempts.

4. Result and Discussion

Plaintext sensitivity analysis also aids in evaluating the algorithm's resistance against attacks such as chosen-plaintext attacks, where an attacker can deliberately modify parts of the plaintext to gain insights into the encryption process or obtain sensitive information.

4.1. DNA Encoding

Transform the characters in the plaintext message into the equivalent DNA nucleotide representations. A predetermined mapping system that maps each character to a specific DNA nucleotide sequence can accomplish this. Adenine (A), cytosine (C), guanine (G), and thymine (T) are the four DNA nucleotides that may be used to represent each character in DNA encoding. We can provide a mapping method in which a specific DNA sequence is given to each character. Examples include mapping the letter "A" to the DNA sequence "ATC," the letter "C" to "GCT," the letter "T" to "AGT," and so on [8].

Table 1. DNA nucleotides that may be used to represent each character in DNA encoding

Sr. No	Plaintext	Encode Message
0	A	ATC
1	C	GCT
2	G	CGA
3	T	AGT

In Table 1, The mapping system, where each character is connected to its appropriate DNA sequence, is represented by the DNA_mapping dictionary. A plaintext message is sent to the encode_to_DNA function, which iterates over each character. To add the appropriate DNA sequence to the encoded_message list, it first determines if the character is present in the DNA_mapping dictionary. Characters that don't have a mapping are maintained in their original form in the encoded.

4.2. XOR Operation between the DNA-encoded

The XOR (exclusive OR) operation is a binary operation that takes two inputs and produces an output where each bit results from the XOR operation on the corresponding bits of the input values [9]. In DNA-based encryption, the DNA-encoded block and the encryption key are treated as binary sequences. The XOR operation is performed bit-wise between the DNA-encoded block and the encryption key, producing a modified DNA-encoded block.

Table 2. DNA–Based Encryption with XOR Operator

No	DNA Block	Encryption Key	XOR Result
0	A	G	1
1	T	C	1
2	C	T	1

Table 2 defines the perform_XOR function, which inputs a DNA-encoded block and an encryption key. It performs the XOR operation bit-wise between the DNA-encoded block and the encryption key. If the corresponding bits differ, the XOR result is '1'; otherwise, '0'. The function returns the XOR result as a binary sequence. Modified bimodal map algorithm to the XOR result using the same parameters as in Step 1. This step further scrambles the encrypted block. The code snippet provided generates a graph that visualises the transformation of the XOR result through the modified bimodal map algorithm. The graph will have two lines:

5. Decryption Process

You must undo the encryption procedure and get the original multimedia data to create the decryption method for the Modified Bimodal Map-based Encryption Scheme. Here is a step-by-step breakdown of the decryption.

Step 1. Design the decryption algorithm to reverse the encryption process and recover the original multimedia data1.

- Reverse the modified bimodal map algorithm: Apply the inverse of the modified bimodal map function to the encrypted block. This will reverse the scrambling process and retrieve the XOR result.
- Perform XOR operation: Take the XOR of the retrieved XOR result and the encryption key. This will reverse the XOR operation performed during encryption and recover the DNA-encoded block.
- Reverse DNA mapping: Using the predefined mapping scheme, map the DNA-encoded block back to the plaintext message characters. Reverse the process of mapping each DNA nucleotide sequence to its corresponding character.
- Obtain the decrypted multimedia data: Combine the recovered plaintext message characters to obtain the original multimedia data.

The reverse_modified_bimodal_map function reverses the modified bimodal map algorithm, and the reverse_DNA_mapping function performs the reverse DNA mapping. The decrypt function combines these reverse processes to decrypt the encrypted block and recover the original plaintext message.

Step 2. Develop techniques to decode the DNA encode:

To decode DNA-encoded data back to binary format, you need to reverse the process of DNA mapping. Here's a theoretical explanation of the decoding technique:

- DNA Mapping Scheme: You should have a predefined mapping scheme that maps each character to a specific DNA nucleotide sequence. This mapping scheme serves as a reference for decoding.
- DNA Sequences to Binary: Each DNA nucleotide sequence in the encoded data represents a binary value. You must convert each DNA sequence to its corresponding binary representation to decode.
- Binary to Characters: Once you have the binary representation of each DNA sequence, you can convert them back to characters using standard binary-to-text encoding schemes like ASCII or Unicode.

DNA_mapping dictionary represents the predefined mapping scheme, where each DNA sequence is mapped to a binary value. The decode_DNA function takes the DNA-encoded data and the DNA mapping scheme as input and decodes the DNA sequences back to binary format.

Step3. Ensure the decryption process is secure efficient, and can handle different multimedia data types.

To ensure secure, efficient, and versatile decryption of different types of multimedia data, several considerations should be taken into account:

- Key Management: Implement a robust and secure key management system to generate, distribute, and store encryption keys. This ensures that only authorised parties can access the keys required for decryption.
- Encryption Algorithm: Use a solid and well-vetted encryption algorithm that provides a high level of security. The algorithm should be designed to handle different types of multimedia data, including images, videos, audio files, etc. It should also support efficient encryption and decryption operations to ensure optimal performance.
- Data Integrity and Authentication: Consider incorporating data integrity and authentication mechanisms to verify the authenticity and integrity of the decrypted multimedia data. This can involve techniques such as digital signatures, message authentication codes (MACs), or hash functions.
- Error Handling: Account for potential errors or corruption in the encrypted data during transmission or storage. Implement error detection and correction mechanisms to ensure the decryption process can handle and recover from any errors encountered.
- Scalability: Design the decryption process to be scalable, allowing for efficient decryption of large volumes of multimedia data. Consider parallelisation techniques or optimisations to enhance the decryption speed and handle multimedia data of varying sizes.
- Compatibility and Interoperability: Ensure the decryption process is compatible with standard multimedia file formats and seamlessly integrates with existing multimedia applications and systems. This facilitates interoperability and easy integration into multimedia communication and storage environments. Complex.

Comparison Table: A table compares the DNA Modified Bimodal Map-based Encryption Scheme with other existing encryption methods based on various criteria, such as security level, critical generation complexity, encryption speed, robustness against attacks, and compatibility with the multimedia data format.

Table 3. Compares the DNA Modified Bimodal Map-based Encryption Scheme with other existing encryption

Criteria	**DNA Modified Bimodal Map**	**Encryption Method 2**	**Encryption Method 3**
Security level	High	Medium	High
Key Generation	Complex	Simple	Complex
Encryption Speed	Moderate	Fast	Slow
Resistance to Attacks	Robust	Vulnerable	Robust
Compatibility	Multimedia Format	Limited Formats	Multimedia Format

6. Conclusion

Evaluating the Chaotic-Based Encryption/Decryption Framework based on MBMES and DNA encoding revealed several significant findings. Firstly, the encryption algorithm demonstrated an ample critical space, making it resistant to brute-force attacks. The initial values of the chaos system keys exhibited high accuracy, contributing to a critical space of significant magnitude. Statistical analysis of the encrypted images showed that the algorithm effectively masked the statistical characteristics of the original plaintext. The histogram distribution of the encrypted images appeared more uniform, indicating a solid resistance against statistical attacks. Based on these findings, it can be concluded that the Chaotic-Based Encryption/Decryption Framework utilising MBMES and DNA encoding provides a promising approach for secure multimedia communications. The algorithm effectively protects the confidentiality and integrity of multimedia data, making it suitable for applications where data security is paramount.

References

1. Lin, C.Y.; Yu, H.H.; Zeng, W. Multimedia Security Technologies for Digital Rights Management; Academic Press: Cambridge, MA, USA, 2006.
2. Phillips, I.E.B.; Ornstein, S. Securing Digital Content System, and Method. U.S. Patent 7,979,697B2, 12 July 2011.
3. Azzaz, M.S.; Tanougast, C.; Sadoudi, S.; Bouridane, A. Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption. Commun. Nonlinear Sci. Numer. Simul. 2013,
4. 18, 2035–2047. [CrossRef]
5. Huang, C.G.; Cheng, H.; Ding, Q. Logistic chaotic sequence generator based on physical unclonable function. J. Commun. 2019,
6. Hasheminejad, A.; Rostami, M. A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. Optik 2019, 184, 205–213. [CrossRef]
7. Yu, J.; Guo, S.; Song, X.; Xie, Y.; Wang, E. Image parallel encryption technology based on sequence generator and chaotic measurement matrix. Entropy 2020, 22, 76. [CrossRef]
8. Yousif, B.; Khalifa, F.; Makram, A.; Takieldeen, A. A novel image encryption/decryption scheme based on integrating multiple chaotic maps. AIP Adv. 2020, 10, 075220.
9. Zhou, N.; Pan, S.; Cheng, S. Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt. Laser Technol. 2016, 82, 121–133. [CrossRef]
10. Hancerliogulları, A.; El Hadad, K.M.; Kurt, E. Implement a real-time analogue secure image communication system via a chaotic circuit. Politek. Derg. 2019, 20, 1083–1092.
11. Wu, X.J.; Kan, H.B.; Kurths, J. A new colour image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl. Soft Comput.
12. Gehani, A.; Labean, T.; Reif, J. DNA-based Cryptography. Asp. Mol. Comput. 2002