Secured Transfer and Storage Image Data for Cloud Communications

https://doi.org/10.3991/ijoe.v19i06.37587

Mohammad K. Abdul-Hussein[1(✉)], Haider TH. Salim ALRikabi[2]
[1]Al-Ma'moon University College Baghdad, Baghdad, Iraq
[2]Electrical Engineering Department, College of Engineering, Wasit University, Wasit, Iraq
mohammad.k.abdul-hussain@almamonuc.edu.iq

Abstract—In cloud computing, resources are used to communicate instead of local servers or individual devices. However, sharing resources among several users is a difficult issue in cloud communication. Cryptography and steganography techniques are used for cloud storage to address data security challenges. This paper presents a novel method for securely encrypting image data for transmission and link exchange with a cloud storage service. There are two phases to accomplish the encryption process, the first phase encrypts the image file by XORing it with a random key that is generated by a new hybrid of the chaotic map. The second phase converts the encrypted image format to audio format to add another layer of security and improve secure image data transfer. The random key is generated using a hybrid chaotic map and has the benefit of having more than 10^{256} key spaces and the necessary level of security. Based on a statistical analysis of the encryption, the quality of the image is evaluated using several criteria, and the results demonstrate the algorithm's ability to accomplish resist encryption.

Keywords—cloud storage, image encryption, chaotic map, key management

1 Introduction

Cloud communication, which gives customers a selection of services on demand, has become more significant. One of the key concerns is the security of data kept in cloud data centers. The security of pictures on a transmission medium is the most pressing topic in the field of study. Images are protected against unwanted assaults through the transfer of data using several security mechanisms, including authentication, digital signatures, and cryptographic algorithms [1, 2]. Encryption is a method for preventing unwanted access to or use of data that turns information that can be read (plaintext) into information that can't be read (cipher text). Researchers and businesses have considerably increased the use of encryption to safeguard the confidentiality and integrity of data that has been integrated into products and services [3, 4]. Modern cryptography must offer security and digital keys to ensure that data delivered in cyberspace is safe and unharmed. To provide the maximum level of security for lawful internet users, encryption and decryption techniques must be enhanced. To prevent becoming a victim of cybercrime in the modern world, both the sender and the intended receiver may rest easy. Data must be transformed into unreadable formats to be safeguarded and delivered without incident [5, 6]. The cloud was successfully transformed into an open area thanks to the use of digital technology for a variety of tasks including replication, distribution, and uploading [7]. To confirm the security, privacy, and agreement of data, cloud computing heavily relies on cryptography. However, the current methods are ineffective and unproductive, making them worthless. Despite a considerable reduction in the risk of privacy leaks, cloud storage of encrypted data makes it hard to confirm information control [8, 9].

2 Related works

Several different image or data encryption solutions have been put out, each focusing on data encryption or encrypted data for cloud communications; in the section that follows, a brief synopsis of recently published methods on this subject is given:

A.M. Vengadapurvaja et al. [10] adopted an effective encryption technique to conduct encryption and decryption on medical images while satisfying the homomorphic characteristic. These images may be used to store data in the cloud and to conduct actions on them. Keyspace analysis, histogram analysis, PSNR and MSE analysis, correlation analysis, and result presentation are used in the test analysis. By using the suggested algorithm on the reference images, the analysis techniques are contrasted with the existing findings. S. kurnaz et al. [11], suggested system the DICOM (Digital imaging and communications in Medicine) system, the system deals with a file that includes medical pictures, and the patient's information face is partitioned procedure to extract the medical image and encrypt the image and upload it with patient info to the cloud. In an Oracle database and an encrypted image file that has its keys saved in a database, the cloud stores patient information. The cloud used the Least Significant Bit (LSB) steganography technique to embed the patient's medical information in an encrypted medical image together with the decryption key, and then sends the encrypted image along with the steganography information to the authorized doctor [12, 13]. S. A. Jassim and W. K. Awad. Achieved privacy for the files belonging to data owners that are kept in a public cloud [14]. Additionally, the solution gives data owners the flexibility to remove or add users without changing the master secret key and improves key management. Asymmetric cryptography is employed in their work to exchange keys, whereas symmetric cryptography is utilized to encode and decode large data. V. Kakkad et al. [15], advocated using image encryption and biometric identification to guarantee the security of photos stored in cloud architecture, The notion of employing biometric authentication to secure photos on cloud platforms is presented in their study. Many procedures considered for biometric verification, safe upload, and contact to photographs are described. Finally, all steps are integrated and completed to shed light on the whole process and the approaches that work the best in terms of compatibility and outcomes. The suggested methodology breaks down the notion of authentication of the image into two simple steps: compression of the image using the DWT, and image encryption using the mixture SHA with the blowfish algorithm. S. Li et al. [16]

introduced a cloud image data protection technique with an automatic selection mechanism and layered encryption strategy to ensure the confidentiality of cloud data contents. Their technique is also helpful for securing the upload of private or public data to the cloud server for real-time monitoring, real-time applications, and real-time transmission. The suggested technique to encrypt images used the confusion-diffusion scheme, a fundamental and well-known cryptographic technique, as well as an automated selection mechanism (sliding pixel window), as its major drivers. V. Poduval et al. [17] presented image steganography and hybrid cryptography techniques for safe cloud file storage. Due to the employment of various algorithms for the encryption/decryption process, their technique aids in attaining improved efficiency and better security. To improve outcomes and increase the security of the sent data, additional work on their article uses the 3-DES technique for encryption. In the financial and private sectors, where the suggested technology can be deployed, high-level data protection is necessary. P. V. Lahande and P. R. Kaveri adopted a method for encryption and decryption [18]. Private data is encrypted using the approach, which also creates a cipher picture of the data. This image is then uploaded to the cloud. The user data is given an additional level of protection as a result. Similar to how data is traditionally encrypted; a key may also be used to add a layer of protection. In other words, level one would include converting plain text to cipher text from its original form, and level two would involve using this cipher text to create the cipher image. After applying the suggested encryption and decryption methods on the cloud, data confidentiality has increased. Now, the user may effortlessly keep his or her private, delicate, and confidential text in the form of cipher images without worrying about its security. F. Thabit et al. [19] suggested a technique for applying a cryptographic lightweight algorithm to data improvement in cloud computing. It concentrated on researching the security and performance analysis algorithm architecture which is based on computation time, the sensitivity of key, statistical analysis, histogram of the image, and entropy. All these factors are changed analysis in cloud computing environments. Additionally, it gave a performance assessment of the generic symmetric algorithms used to protect cloud services such as DES, AES, RC4, HIGH, SF, and SIT.

3 Cloud computing and cryptography

The deployment of IT infrastructure is being replaced by the on-demand, self-service, and pay-as-you-go business models offered by cloud computing, an acceptable means of accessing resources, applications, and services through the Internet. Therefore, it is not unexpected that interest in cloud computing has grown over recent years [20–22]. The biggest issue with storing and exchanging data on the cloud is security. Every user wants the privacy of their data to be protected from illegal access. Since attacks and unwanted access are thus prevented, user data is encrypted using encryption techniques. When using cryptography, the original data is first transformed into unintelligible cipher text (encryption), and then the cipher text is transformed back into the original form (Decryption) [23–25]. As is well knowledge, cloud security is an extensive collection of technologies and processes that safeguard data stored in the cloud.

This is accomplished by encrypting each step taken within the cloud, which may be summed up as:

1. Encryption key management: With the help of this tool, administrators may safeguard their databases by providing their encrypted keys or asking someone else to produce a key for them. It supports key files, PFX, and BYOK key encryption.
2. Client-side encryption: This implies that before transmission, user data is encrypted. The text of the encryption key is stored externally as well. such that even if the data is released, the user data is secure and the original data cannot be deciphered.
3. Cloud server encryption: Common encryption techniques include coordinated coding and content-aware coding. The information or formats and codecs used to stop data leakage are employed by a content-aware application. Depending on policy settings, such as those that emailing law enforcement to law enforcement automatically encrypt the credit card details.
4. Cloud password machine service: A cloud server encryption device is a hardware encryption device that creates many virtual encryption devices through virtualization.
5. Key management services: To secure the development of cloud-based apps and services, existing cloud service providers can either offer encryption key schemes or leave it up to the customers. As cloud service providers move closer to implementing critical management strategies.
6. Data encryption: Data security is preserved via encryption technology both during storage and transmission (link encryption technology). Storage systems and technologies that support encryption, like cryptography, are frequently encountered by storage technicians. Encrypt storage or a disk [26, 27].

4 Chaotic cryptography

A dynamical system that is suitable for chaotic cryptography is necessary. Such a system should exhibit chaos over a wide range of initial conditions and parameter values, among other characteristics. Additionally, the distribution of the iterated variable in such systems needs to be flat to prevent statistical analysis from being performed [28]. The two ideas of cryptography and chaos have a significant relationship, according to research [29]. The ease of key production, sensitive reliance on the beginning state, and parameter adjustments are only a few of the positive characteristics of chaotic sequences. Because chaotic sequences have desirable qualities, using chaos in cryptography helps to improve data security. When sending voice data that has to be encrypted, the recipient must be able to locate the general key in the communication system [30]. Chaotic systems have a wide power spectrum and are extremely sensitive to small variations in the initial conditions. As a result, chaotic systems are capable of producing orbits that do not deviate from really random orbits. This has led to increasing interest in Chaotic Pseudorandom Number Generators (CPRNG) [29]. In this paper, hybrid chaotic maps are mixed to generate an encryption key, Arnold cat map, and Duffing Map 2D, the following is a description of each map:

- **Arnold cat map:** is a double-dimensional chaotic system, the Arnold cat map is represented by two distinct equations (1, 2) [31]:

$$X_{n+1} = X_n + (Mod\ N) \tag{1}$$

$$Y_{n+1} = BX_n + (Mod\ N) \tag{2}$$

Where X_n, Y_n are the location of samples in the matrix ($N \times N$), and $n = 1, 2, 3, \ldots, N - 1$ and X_{n+1}, Y_{n+1} are the location which changed after applying cat map. A and B are two positive integer control parameters. The process of encryption is complete through cat map iteration, after execution M iterations, there are T integers that are positive such that $(X_{n+1}, Y_{n+1}) = (X_n, Y_n)$. The parameters A, B, and the size of the sample's matrix (N × N matrix) all affect the time [20]

- **2D Duffing Map:** A discrete-time dynamical system that displays chaotic behavior is the Duffing map [32].
- After taking a point (*Xi, Yi*) off the plane, the 2D Duffing map maps a new point [33]. It is termed as:

$$\mathrm{X}_{\mathrm{i}+1} = \mathrm{Y}_{\mathrm{I}} \tag{3}$$

$$\mathrm{Y}_{\mathrm{i}+1} = -\mathrm{b}\ \mathrm{X}_{\mathrm{i}} + \mathrm{a}\ Y_{\mathrm{i}} - (Y_{\mathrm{i}}^{3}) \tag{4}$$

Where $\mathrm{X_i}$ and $\mathrm{Y_i}$ are the starting values, a and b are the control parameters, and $\mathrm{X_{i+1}}$ and $\mathrm{Y_{i+1}}$ are the new pixel coordinates [34].

5 The proposed encryption algorithm

This paper is focused on the security of image files before storing and sharing these files in the cloud. In this paper, images are encrypted and decrypted without any change in file size through the encryption and decryption process. In addition, another layer of secrecy is applied by converting format image to audio format, thus securing data transfer over networks wherein the entire audio file covers the encrypted image file. In the final process, this encrypted data is stored in the cloud. Also, complex chaotic maps are chosen to generate the key for image encryption, and this will increase the complexity of the algorithm image encryption. Figure 1 shows the block diagram of encrypting image file-sharing in Cloud computing

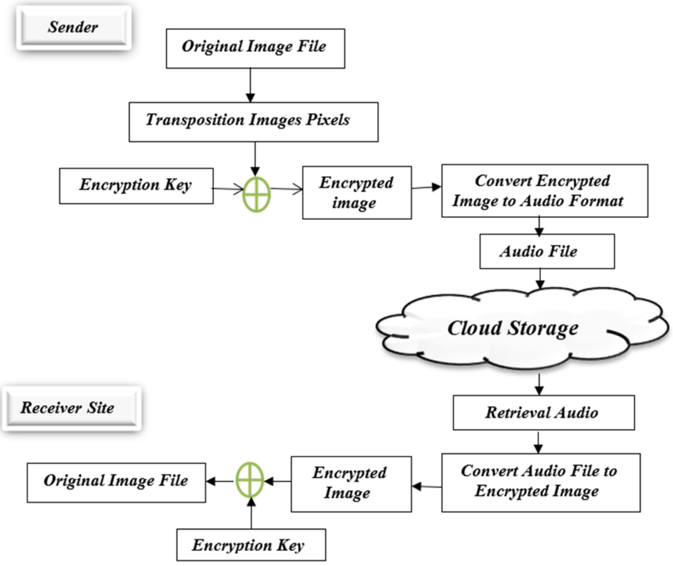


Fig. 1. Block diagram of encrypting image file-sharing in cloud computing

The following steps determine the main process of this paper:

A. Determine image file
B. Transposition of Images blocks
C. Generate Encryption Key
D. Encryption and Decryption Process

A. Determine image file

Cloud-based data storage is vulnerable to cyberattacks. This is especially troublesome when using the cloud since different categories of users store large amounts of data on the same cloud server. Particularly when using cloud computing, picture files become more vulnerable to malicious assaults. Thus, user images must be kept in the cloud in encrypted form to safeguard them.

B. Transposition of images blocks

Position permutation is one of the most straightforward techniques for digital image encryption. The strong connections between the pixels in the image can be weakened by moving the positions at each pixel location. **In this paper, the transposition method is used to permute the columns and rows of photographs and reposition pixels. The image is divided into** 2 × 2 blocks, each block is after interchanging the rows and columns, the resultant transpose of the matrix B^T looks like this Figure 2:

$B = \begin{matrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{matrix}$	$B^T = \begin{matrix} P_{11} & P_{21} \\ P_{12} & P_{22} \end{matrix}$

Fig. 2. Transpose of the matrix B^T

C. Generate encryption key

Private information and sensitive data are protected by encryption keys, which can also increase the communication security between servers and the application of the client. In essence, when data is encrypted, even if an unauthorized person or entity gains access to it, it will not be able to read it. Thus, a basic principle of encryption with the theory of chaos is founded on the same dynamic systems' ability to produce random numbers. To encrypt communications, this random number is utilized. The starting condition that was utilized to generate the random number has a significant impact on its ability to be decrypted. In addition, specific chaos theory and some dynamic systems require several significant properties like sensitive dependency on primary factors, non-periodicity, and pseudorandom assets. As is well known, some chaos-based algorithms offer a good combination of speed, high-security complexity, and low computational overheads. To create an encryption key, a new hybrid of two-dimensional maps (the Duffing and Arnold cat maps) is used in this section. This hybrid of the two chaotic maps is thought of as a piecewise smooth nonlinear chaotic map. This blending creates fresh, delicate chaotic maps that emerge more readily, thus reducing the risk of known-system-based assault. The key space, which represents all possible key combinations utilizing all secret key bits, is a collection of all potential keys. The word "key-size" refers to the quantity n of bits that establishes the size of the complete keyspace 2^n. The recommended solution uses two keys; with the first key serving as the Arnold cat map's starting value. These keys are the result of two chaotic maps; Key_2 has a size of 2^{256} key spaces, making it large enough to withstand a variety of brute-force assaults.

D. Encryption and decryption process

In this section, we develop the new encryption and decryption for images to be stored in the cloud.

1. Encryption module

In this module, the image file is read to be prepared for encryption; this is done by isolating heard from raw data. Raw data is ready to be XORed with a random key. The random key is generated by initially selecting "Initial Value" for the Arnold cat map, after applying this map, Key_1 is the result.

Key_1 is considered the initial value for the Duff map. After estimating the Duff map according to Equation 2, the output is a random key Key_2. The block diagram of the Encryption module is shown in Figure 3.

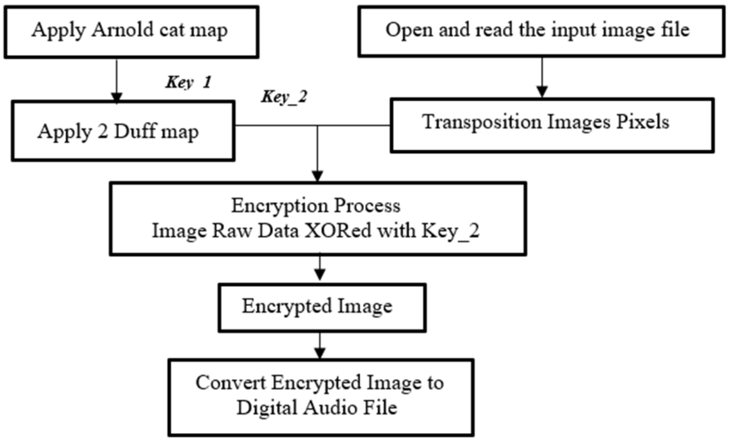

Apply Arnold cat map
Open and read the input image file
Key 1
Key_2
Apply 2 Duff map
Transposition Images Pixels
Encryption Process
Image Raw Data XORed with Key_2
Encrypted Image
Convert Encrypted Image to
Digital Audio File

Fig. 3. Module of image encryption

In this module, two chaotic maps are used to generate two random keys used to encrypt images; this will increase the key robustness. The other one is converting the encrypted image to an audio format, and this increases the undetected of an encrypted file.

2. Decryption module

The audio file is converted back to a plain image file in this section. It is the opposite of the encryption module, but it's not identical in reverse. In the beginning, the audio file is converted to an image, then the encrypted image is XORed with Key_2. To obtain the original image, the encrypted image pixels are transposition of images pixels in reverse order. Thus, overall module steps are accomplished in reverse order. The block diagram of the decryption module is shown in Figure 4.

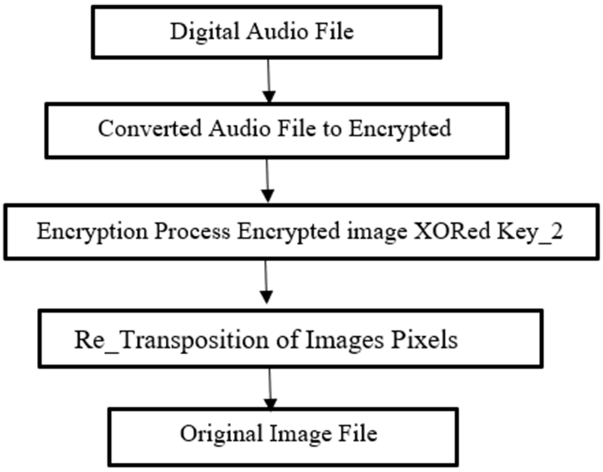

Digital Audio File
Converted Audio File to Encrypted
Encryption Process Encrypted image XORed Key_2
Re_Transposition of Images Pixels
Original Image File

Fig. 4. Module of image decryption

In the decryption module, the digital audio file is converted to an image format, which means the audio file is converted to an encrypted image. In this paper, the encryption systems used Key_2 which is communicated by the sender and the recipient. Both parties must possess the key, which is used by the sender to encrypt the communication, and by the recipient to decode It, thus encrypted image at the receiver side is XORed with Key_2 to obtain an original image.

6 Results and discussion

In this proposal, the decrypted image is encrypted with a key derived from a hybrid of two chaotic maps (the Arnold cat map and the Duff map), to strengthen the cipher's defenses against attacks, the encrypted image is converted into an audio file format, which adds another layer of cover for attackers. The suggested image encryption strategy offers an effective and secure method for image encryption and cloud storage, according to the findings of many experimental, statistical analyses, and key sensitivity tests. In this paper, three images sample is used to demonstrate the implementation of the encryption process: Test_1 with a size of 116 KB, Test_2 with a size of 184 KB, and Test_3 with a size of 256 KB. Figure 5 shows the three test images with their histogram, Figure 6 shows Three samples of images after encryption with their histogram, and Figure 7 shows Test_1, Test_2, and Test_3 audio signals after converting the image to audio format.

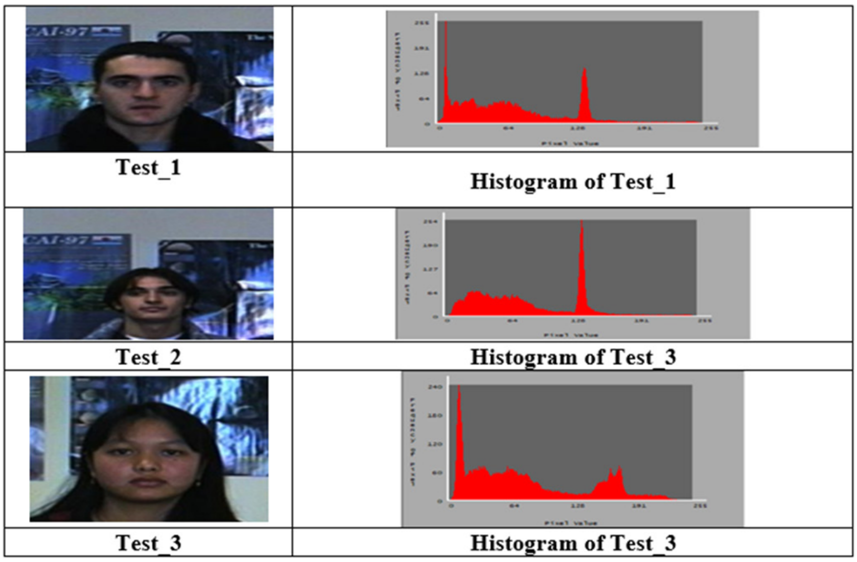
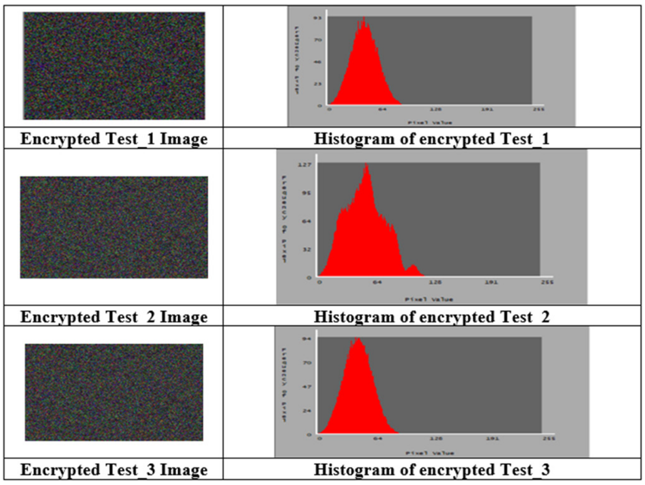


Fig. 5. Three original test images and their histograms



Encrypted Test_1 Image

Histogram of encrypted Test_1

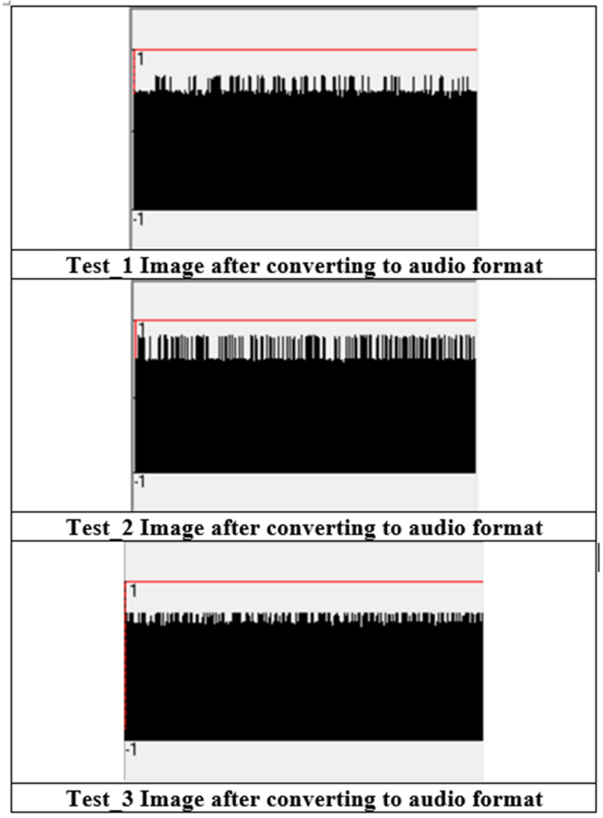
Encrypted Test_2 Image

Histogram of encrypted Test_2

Encrypted Test_3 Image

Histogram of encrypted Test_3

Fig. 6. Three encrypted test images and histograms



Test_1 Image after converting to audio format

Test_2 Image after converting to audio format

Test_3 Image after converting to audio format

Fig. 7. Test_1, Test_2, and Test_3 audio signal (after converting image to audio format)

To verify the unpredictability of the sequence produced by chaotic maps, five bench tests are utilized. These tests have assessed the unpredictability of quantity sequences generated by cryptographic pseudo-random or random number generators; the tests comprise a statistical set. Table 1 provides the assessment outcomes of five bench tests produced by key_2. Results demonstrate that we outperformed the five benchmark tests, achieving a high level of randomness.

Table 1. Generate Key_2 performance in NIST benchmark tests

Test of Randomness	P_Value	P_Value >0.01
Frequency	0.8027	Pass
Runs	0.3214	Pass
Serial	0.5451	Pass
Entropy	0.6011	Pass
Cumulative Sums	0.8811	Pass

A suitably safe cipher has a computational complexity equal to the key space. The total number of permutations using all secret key bits is reflected in the key space. As was already mentioned, the proposed technique uses two secret keys: Key_1 created by the chaotic Arnold Cat Map, and Key_2 obtained from the Duff Map, with Key_1 serving as the beginning vector for the Duff Map. The final key is 2^{256}; this key space is sufficiently wide to fend off several types of brute-force attacks.

Mean Square Error (MSE), Signal to Noise Ratio (PSNR), Peak to Signal Ratio (PSNR), Number of pixel changes (NPCR), and Unified Average Change Intensity (UACI) measurements are made for encrypted images. The results of this quality measurement are displayed in Table 2.

Table 2. Quality measurement for encrypted image

Test_Image	MSE	PSNR	NPCR	UACI
Test_1	8. 4333e + 003	5.432	99.799	25.5221
Test_1	8. 8216e + 003	5.277	99.224	24.5671
Test_1	7.17891e + 003	4.336	99.231	22.1112

Based on the results shown in Table 2, it would appear that MSE has a high value, indicating a bigger difference between the original picture and the encrypted image. Without knowing the secret key, it is challenging to extract the plain picture from the cipher image, as seen by the poor PSNR values in Table 2. A high NPCR measurement % suggests that the placements of the pixels were altered at random. According to UACI values, nearly every pixel intensity value in the encrypted image has been altered from what it was in the original or plain image, making the pixels in the original and encrypted-images more different.

7 Conclusion

Safe Communication denotes the state where the information or data is transferred between two parties; this information can't be accessed by an adversary. An Adversary in Cryptography is a spiteful entity, which intends to repossess valuable information or data thereby undermining the principles of information security. In this paper, a new chaos-based image cryptosystem has been presented. The encryption is passed through two phases, the first phase image file is initially encrypted by XORing it with a random key produced using a Duff map. This key is generated based on the initial value that is taken from another Arnold Cat Map to make encryption keys more random. In the second phase, the encrypted image is transformed into another format (audio format) to increase the robustness and difficulty of detection. This work is evaluated in terms of security tests and the outcomes demonstrated a solid balance between security and performance for image encryption in a cloud computing context.

8 References

[1] J. Mahalakshmi and K. Kuppusamy, "An Efficient Image Encryption Method Based on Improved Cipher Block Chaining in Cloud Computing as a Security Service," *Australian Journal of Basic and Applied Sciences*, vol. 10, no. 2, pp. 297–306, 2016.

[2] H. T. ALRikabi and H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[3] H. Salim and H. Tauma, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[4] H. A. Naman and M. Al-dabag, "Encryption System for Hiding Information Based on Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[5] M. T. Gençoğlu, "Importance of Cryptography in Information Security," *IOSR J. Comput. Eng*, vol. 21, no. 1, pp. 65–68, 2019.

[6] V. M. Shokalo, A. Strelnitsky, M. Abdul-Hussein, and E. Yagudina, "Refined Model for Calculation of Limiting Secret Efficiency of Wi-Fi Communication Channel," *Telecommunications and Radio Engineering*, vol. 71, no. 16, 2012. https://doi.org/10.1615/TelecomRadEng.v71.i16.30

[7] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design a System for an Approved Video Copyright Over Cloud Based on Biometric Iris and Random Walk Generator using Watermark Technique," *Periodicals of Engineering Natural Sciences*, vol. 10, no. 1, pp. 178–187, 2021. https://doi.org/10.21533/pen.v10i1.2577

[8] A. J. S. Bhargav and A. Manhar, "A Review on Cryptography in Cloud Computing," 2020. https://doi.org/10.32628/CSEIT206639

[9] O. Strelnitskiy, V. Shokalo, E. Yagudina, and M. Abdul-Hussein, "The Method of Calculating Detection Areas of Digital Communication Systems," in *Proceedings of International Conference on Modern Problem of Radio Engineering*, *Telecommunications and Computer Science*, 2012: IEEE, pp. 268–268.

[10] A. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security," *Procedia Computer Science*, vol. 115, pp. 643–650, 2017. https://doi.org/10.1016/j.procs.2017.09.150

[11] A. A. Jasım, “Cloud System for Encryption and Authentication Medical Images,” Altınbaş Üniversitesi, 2018.

[12] S. H. Abbood, M. S. Rahim, and A. M. Alaidi, “DR-LL Gan: Diabetic Retinopathy Lesions Synthesis using Generative Adversarial Network,” *International Journal of Online and Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28005

[13] M. K. Abdul-Hussein and H. Alrikabi, “Evaluation of the Interference’s Impact of Cooperative Surveillance Systems Signals Processing for Healthcare,” *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 03, pp. 43–59, 2022. https://doi.org/10.3991/ijoe.v18i03.28015

[14] S. A. JASSIM and W. K. AWAD, “Searching Over Encrypted Shared Data Via Cloud Data Storage,” *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 12, 2018.

[15] V. Kakkad, M. Patel, and M. Shah, “Biometric Authentication and Image Encryption for Image Security in Cloud Framework,” *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, 2019. https://doi.org/10.1007/s41939-019-00049-y

[16] S.-Y. Li, M. A. Benalcazar Hernandez, L.-M. Tam, and C.-S. Chen, “A Cloud Image Data Protection Algorithm with Multilevel Encryption Scheme and Automated-Selection Mechanism,” *Applied Sciences*, vol. 9, no. 23, p. 5146, 2019. https://doi.org/10.3390/app9235146

[17] V. Poduval, A. Koul, D. Rebello, K. Bhat, and R. M. Wahul, “Cloud Based Secure Storage of Files using Hybrid Cryptography and Image Steganography,” *Int J Recent Technol Eng (IJRTE)*, vol. 8, no. 6, 2020. https://doi.org/10.35940/ijrte.F7227.038620

[18] V. Lahande, “ Increasing Data Secrecy In Cloud by Implementing Image Cryptography,” *International Journal of Scientific & Technology Research*, vol. 9, no. 04.

[19] F. Thabit, S. Alhomdy, and S. Jagtap, “Security Analysis and Performance Evaluation of a New Lightweight Cryptographic Algorithm for Cloud Computing,” *Global Transitions Proceedings*, vol. 2, no. 1, pp. 100–110, 2021. https://doi.org/10.1016/j.gltp.2021.01.014

[20] K.-K. R. Choo, J. Domingo-Ferrer, and L. Zhang, “Cloud Cryptography: Theory, Practice and Future Research Directions,” *Future Gener. Comput. Syst.*, vol. 62, pp. 51–53, 2016. https://doi.org/10.1016/j.future.2016.04.017

[21] A. Strelnitskiy, V. Shokalo, E. Yagudina, and M. K. Abdul-Hussein, “Method of Calculating the Detection Zone Boundaries of the Rayleigh Wi-Fi Wireless Channel with Quasi-Static Fading,” *Radioelectronics and Communications Systems*, vol. 55, no. 10, pp. 452–457, 2012. https://doi.org/10.3103/S0735272712100032

[22] J. Q. Kadhim and I. A. Aljazaery, “Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT,” *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 02, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[23] J. Kaur, E. S. Sharma, and M. Tech, “Secure Image Sharing on Cloud using Cryptographic Algorithms: Survey,” *International Journal on Future Revolution in Computer Science & Communication Engineering*, vol. 4, no. 2, pp. 319–325, 2018.

[24] I. A. Aljazaery and A. H. M. Alaidi, “Encryption of Color Image Based on DNA Strand and Exponential Factor,” *International Journal of Online & Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[25] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, “Dark Web Illegal Activities Crawling and Classifying using Data Mining Techniques,” *International Journal of Interactive Mobile Technologies*, vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[26] W. Z. M. Al-Humadi, “Cryptography in Cloud Computing for Data Security and Network Security,” *Solid State Technology*, vol. 63, no. 4, pp. 6965–6973, 2020.

[27] N. Alseelawi and H. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT" *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 3, pp. 114–133, 2021. https://doi.org/10.3991/ijoe.v18i03.28011

[28] M. Lawnik and M. Berezowski, "New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography," *Symmetry*, vol. 14, no. 5, p. 895, 2022. https://doi.org/10.3390/sym14050895

[29] M. S. Mahdi, R. A. Azeez, and N. F. Hassan, "A Proposed Lightweight Image Encryption using ChaCha with Hyperchaotic Maps," *Periodicals of Engineering Natural Sciences*, vol. 8, no. 4, pp. 2138–2145, 2020.

[30] N. F. Hassan, A. Aladhami, and M. S. Mahdi, "Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps," *Iraqi Journal of Science*, pp. 830–842, 2022. https://doi.org/10.24996/ijs.2022.63.2.36

[31] B. Mondal and T. Mandal, "A Light Weight Secure Image Encryption Scheme Based on Chaos & DNA Computing," *Journal of King Saud University-Computer and Information Sciences*, vol. 29, no. 4, pp. 499–504, 2017. https://doi.org/10.1016/j.jksuci.2016.02.003

[32] M. F. A. Elzaher, M. Shalaby, and S. H. El Ramly, "An Arnold Cat Map-Based Chaotic Approach for Securing Voice Communication," in *Proceedings of the 10th International Conference on Informatics and Systems*, pp. 329–331, 2016. https://doi.org/10.1145/2908446.2908508

[33] O. Rabie, J. Ahmad, and D. Alghazzawi, "Modified SHARK Cipher and Duffing Map-Based Cryptosystem," *Mathematics*, vol. 10, no. 12, p. 2034, 2022. https://doi.org/10.3390/math10122034

[34] S. Singh, R. Parida, and C. Pradhan, "Comparative Analysis of Image Encryption using 2d and 3d Variations of Duffing Map," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018: IEEE, pp. 0751–0754. https://doi.org/10.1109/ICCSP.2018.8524385

9 Authors

Dr. Mohammad K. Abdul-Hussein: He received the MSc. degree in 1983 and was specified in automatic electric and instrument equipment of aircraft from Kiev Air Force Engineer institute of Higher Military Education in USSR. The Ph.D. degree in 2014 and specified in the communication of engineering from Kharkov National University of Radio Electronics in UKR. Interest areas of study are network communication, electrical circuits, and electronics.

Haider Th. Salim ALRikabi: He is presently Asst. Prof and one of the faculty College of Engineering, Electrical Engineering Department, Wasit University in Al Kut,Wasit, Iraq. He received his B.Sc. degree in Electrical Engineering in 2006 from the Al Mustansiriya University in Baghdad, Iraq. His M.Sc. degree in Electrical Engineering focusing on Communications Systems from California state university/Fullerton, in USA in 2014. His current research interests include Communications systems with the mobile generation, Control systems, intelligent technologies, smart cities, the Internet of Things (IoT), Renewable Energy, Smart Cities, Security Systems,and Communication Networks. Al Kut city–Hay ALRabee, Wasit, Iraq. E-mail: hdhiyab@uowasit.edu.iq. The number of articles in national databases–20, and the number of articles in international database-65.

Article submitted 2022-12-13. Resubmitted 2023-01-23. Final acceptance 2023-01-24. Final version published as submitted by the authors.