Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2526

CyberCraft : Encryption and decryption tool for images using AES, DES, and chaotic logistic map

Pooja Bagane *
Sonali Kothari †
Ankur Goyal §
Krisha Joshi ‡
Mudit Garg @
Nandita Namboodiri #
P. Karthik Krishna $
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Symbiosis International (Deemed University)
Lavale
Pune 412115
Maharashtra
India

Abstract

This work demonstrates a comprehensive study in the field of image encryption with varied techniques adopted which includes Chaotic Logistic Map, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) . Methods for how the techniques of encryption and decryption should be carried out are described. Extra features such as watermarking for ownership are also considered, and strength comparisons are made of the different methods using entropy, Chi-square, and key space analysis. This paper demonstrates the necessity of using robust encryption algorithms, blending aspects of cybersecurity and digital forensics. Information about how well each algorithm protected the digital images was also learned through this work. Results indicate that while AES is somewhat extremely strong and useful, Chaotic Logistic Map is lighter but its security varies depending on its

* *E-mail:* **pooja.bagane@sitpune.edu.in (Corresponding Author)**
† *E-mail:* **sonali.kothari@sitpune.edu.in**
§ *E-mail:* **Ankur_gg5781@yahoo.co.in**
‡ *E-mail:* **krisha.joshi.btech2021@sitpune.edu.in**
@ *E-mail:* **mudit.garg.btech2021@sitpune.edu.in**
# *E-mail:* **nandita.namboodiri.btech2021@sitpune.edu.in**
$ *E-mail:* **karthik.krishna.btech2021@sitpune.edu.in**

mode of usage. This paper intends to let people understand how the encryption method works and the importance behind it in protecting digital assets.

Subject Classification: *Primary 94A60, Secondary 37D45.*

Keywords: *Cyber security, Encryption, Decryption, AES, DES, Chaotic logistic map, Digital forensic.*

1. Introduction

Keeping sensitive information secure in today's digital world is a great concern [1]. As data breaches and cyberattacks become more frequent, encryption is proving to be one of the best methods to secure digital assets [2]. This research work explores image encryption, which is an important concept in cybersecurity of how images can be ensured to be private and safe using many algorithms [3].

Encryption is very important in digital forensics. In that, the key goal is to keep evidence safe [4]. With more and more multimedia data, the encryption of images is now, very frequently, used in all secure communications, data storage, and cloud computing [5]. However, watermarking provides additional protection by adding all details on ownership to the image, thus being useful for intellectual property rights and forensic use [6]. It deals with protecting digital assets and also investigates how robust the applied cryptographic techniques are by applying entropy analysis and comparing metrics such as Chi-square and key space analysis [7]. Thus, it provides better insight into how these techniques function in real life [8].

The main objective of this research work is the encryption and decryption of images using AES, DES, and the Chaotic Logistic Map. Another objective would be to embed watermarking techniques to protect intellectual property, and then to compare the strengths of these algorithms in terms of entropy and other measures of performance.

This paper helps the field of digital forensics and cybersecurity workers by investigating whether different algorithms work well and this aids in the selection of proper encryption methods for varied use [9]. Understanding the powers and weaknesses of these algorithms is necessary to make secure systems that can resist unauthorized access and prove the truth of the digital evidence [10].

2. Literature Review

Along with growing dependence on digital communication and data transmission, the security of data has been an essential issue [11]. This literature review looks upon the different encryption techniques used while emphasizing their importance in protecting sensitive information from unnecessary access. Established techniques like AES and DES will be reviewed, but more recent approaches will also help in bringing out the present scenario of how data security measures are being evolved to respond to the current advanced threats of cybersecurity.

Since data security measures have become an important aspect regarding increased data vulnerability, encryption has risen to the position of being vital for secure communicational systems. The paper by Padate and Patel [12] published in 2015 focuses on the viability of adopting AES as an algorithm for image encryption and decryption. AES uses feature expansion which enables variable 128-bit key transformations per pixel set. Whereas DES has old-style features like limited key length and weak encryption algorithms, AES has strong features of new style and longer key length. Therefore, from this research, it is apparent that AES provides a better solution, especially for real-time applications because it's time to encrypt is less as compared with DES.

In a comparative study regarding the performance of encryption algorithms, Mahajan and Sachdeva [13] evaluated three encryption algorithms, AES, DES and RSA. In the study, AES is defined as the fastest in both encryption and decryption speeds particularly when compared to RSA, which requires more time and computational resources due to its use of asymmetric keys. AES encrypts data blocks of 128 bits using 10, 12, 14 rounds depending upon the key size (128, 192 or 256 bits). In comparison, DES operates on 64-bit blocks with a fixed 56-bit key, making it less secure than AES. The study overall concludes that AES provides a good balance of security as well as performance.

3. Methodology

The CyberCraft research approach consists of a number of successive and interconnected stages:

a. User Interaction via GUI: The system starts with a GUI where a user has an opportunity to input an image and to select an operation: encryption or decryption. The user can also select between employ watermarking or not.

b. Algorithm Selection: According to user input, the system offers three encryption methods like AES – Advanced Encryption Standard, DES - Data-Encryption Standard, Chaotic Logistic Map

c. Key Generation: All approaches differ in the key generation method: They are all just symmetric crypto key generation schemes (128/192/256-bit for AES, and 56-bit for DES FTR). The key generation scheme in Chaotic Logistic Map employs initial conditions (x0, r) defined by chaos theory.

d. Encryption Process: The input image is encrypted with the selected method. XOR operations, with the generated key sequence, are performed in logistic map encryption.

e. Decryption Process: The encrypted image can be decrypted to obtain the original image by the same keys and parameters.

f. Watermarking (Optional): Users have the option to use a digital watermark to indicate ownership of the image. This is very important for forensics, to add authenticity and traceability.

g. Performance Evaluation: The encryption and decryption lead to the system:
   - Chi-Square Test: To judge the randomness of the images in the cipher.
   - Entropy Analysis: To measure the randomness of the keys.
   - Keyspace Analysis: To determine vulnerability to a brute-force.

4. Implementation Details

The implementation of encryption and decryption was done with the use of Node.js, leveraging different modules of JavaScript files toward making the solution robust and efficient. This setup lends itself to modular organization of code, which is much easier to maintain and extend.

The following libraries were used in this work:

- Tkinter: This was an application in which the GUI was done with Tkinter. It is a GUI that does not allow easy manipulation of the encryption and decryption operations.
- jimp: Powerful library for image processing and supports loading and processing images in several different formats.

- crypto: the built-in Node.js library provides cryptographic functionality; the module includes various encryption algorithms such as AES and DES.
- mathjs: Powerful tool in doing complex mathematical calculations to compare the running times of algorithms.
- fs- it is an intrinsic library that offers facilities for file system operations, like reading from and writing to files. These are critically important for handling images and key files.

The code used the logistic map function to create the key sequence, encryption and decryption images and management of the key file. In logistic encryption method, XOR operation is applied based on the generated key sequence such that the output will always be secured.

Finally, the general workflow seamlessly integrates both GUI and command line interfaces. The GUI presents users with a number of buttons representing actions of encryption and decryption. When a user clicks on any of the buttons, the corresponding .js file is executed, thus triggering the chosen operation.

- User Interaction: Users click menus and options to encrypt or decrypt an image.
- Execution: Once the program is selected, an appropriate function for encryption and decryption will be called from a JavaScript file.

Messages of success are printed through the GUI, and also the command-line interface keeps track of status for the operations-that gives the user full feedback. This has the effect of having the user still have an uninterrupted experience but offers flexibility and power of command-line operations in the background.

5. Results & Discussion

This research work involves encrypting and decrypting images using AES, DES, and Chaotic Logistic Map algorithms. Additionally, it presents watermarking, which will safeguard ownership and compare the strengths of these algorithms. In this chapter, we explain the steps involved in encryption and decryption plus watermarking. Then we will analytically consider the entropy and strength of the algorithms. Hence, this study focuses on the performance as well as security from each encryption to

make a comprehensive comparison of understanding practical applicability in terms of securing digital data.

Encryption & Decryption: The encryption and decryption functions were implemented through a GUI as shown in Figure 1. Users can encrypt images using AES, DES, or the Chaotic Logistic Map by just a click of button. Input images are transformed, leading to encrypted and decrypted images, allowing users to test how well the algorithms work. The GUI also supports batch processing. Users can encrypt multiple images and then decrypt them all in one go, a procedure that proves especially useful in forensic investigations.

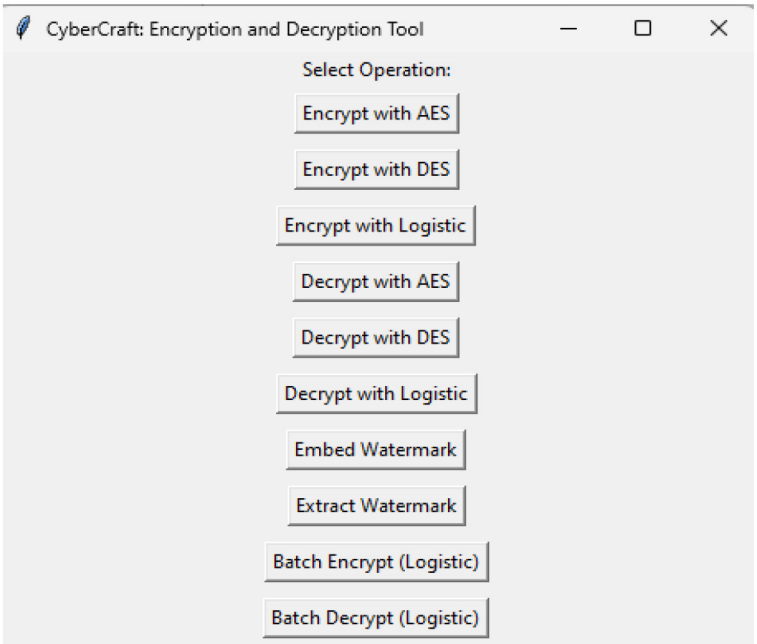


Figure 1

GUI of CyberCraft with all the features

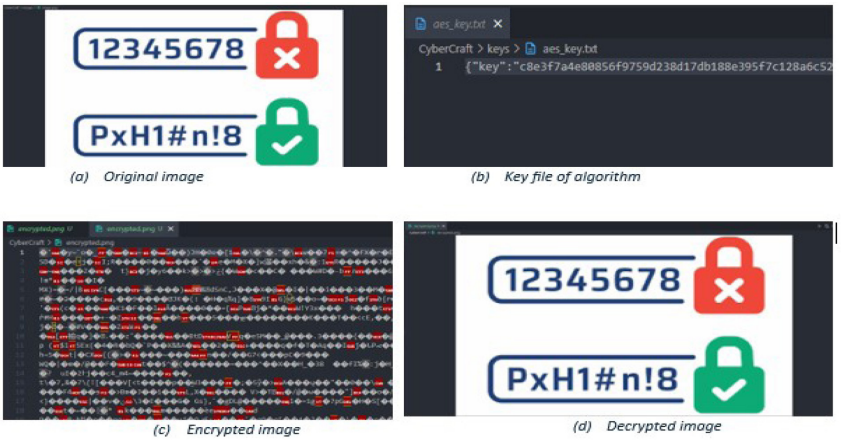
Figure 2 illustrate how encryption works and decryption. It starts with the source image, using a key file to encrypt the image and produce a secure version that is coded. This coded copy is then again turned into its original form by using the same key.

Watermarking Process: Watermarking has been built into the work so that images may be made more secure. This approach allows users to

prove ownership and protect their ideas through the addition of a particular watermark to images. This is a very sensitive aspect in legal cases where the authenticity of a digital proof becomes a contentious issue. Extraction ensures the presence of a watermark that can be verified, and this improves the credibility of the images involved in research investigation.

Entropy and Strength Study: To check how robust the encryption algorithms are, the following measures were used:

- Chi-Square Test: This test is just to show how much the ciphertext resembles random data. The higher the value of Chi-Square, the better is the encryption method. The results also indicated that AES performed well in comparison to DES and Chaotic Logistic Map regarding randomness in ciphertext.



(a) Original image (b) Key file of algorithm

(c) Encrypted image (d) Decrypted image

Figure 2

Encryption & Decryption Process

- Entropy Analysis: This measure how random encryption keys are. The greater the entropy, the stronger and safer are the keys. Results showed that AES and Chaotic Logistic Map have higher entropy than DES which means they are less likely to be attacked.
- Block Entropy and Keyspace Analysis: These tests measured how secure each algorithm was. The block entropy measure looks at how random parts of the ciphertext are, and keyspace analysis counts how many possible keys are. A greater keyspace implies greater

resistance to attacks via brute force. Comparison of results showed that AES has a much larger key space than DES, making it a leading encryption standard.

Table 1 demonstrates comparative analysis of different algorithms. With each comparison brought up was the good points and bad points of each encryption method. AES, more than others, was the strongest choice, with security and speed in mind. DES still is important; however, it is seen as old fashioned because it has a shorter key and is weaker to today's attacks. Chaotic Logistic Map is an interesting option wherein it gives light-level encryption that will be quite useful to some apps. Its security is volatile and changes with its use.

Table 1

Comparative analysis of different algorithms

Algorithm	Performance	Security	Key Size (in bits)	Entropy
AES	Faster for large data	Highly secure	128, 192, 256	4.297
DES	Moderate performance	Less Secure	56	4.285
Chaotic Logistic	Efficient and Fast	Secured with advanced technology	At least 128	3.392

6. Conclusion

This paper demonstrates how images can be encrypted and decrypted using three different methods: AES, DES, and the Chaotic Logistic Map. These illustrate possibilities in how they can be used in cybersecurity and digital forensics. AES was the strongest and most widely utilized method because it has a strong key, high randomness, and the number of possible keys is very large, which makes it great for protecting important digital information. DES is important in history, but its shorter key length and weakness to modern attacks make it less good for today's use. The Chaotic Logistic Map is light and doesn't need many resources, but its security can vary based on how it is set up, which makes it good for certain uses where computing power is limited.

Furthermore, this work had the watermarking feature very helpful in protecting intellectual property and authenticating digital evidence to enable forensic investigations, thus showing how important it is to have incorporated many security measures for the protection of the digital assets.

The algorithms were compared using entropy and key strength analyses by this research work. This provided very useful insights into the strengths and weaknesses of the same. The findings show how important it is to choose the right encryption method based on what the application needs for security. It keeps sensitive data safe in today's changing digital world.

References

[1] B. Bhat, A. W. Ali, and A. Gupta, "DES and AES performance evaluation," in *Proc. Int. Conf. Computing, Communication & Automation (ICCCA)*, pp. 887–890 (May 2015).

[2] M. A. B. Younes, "A survey of the most current image encryption and decryption techniques," *Int. J. Adv. Res. Comput. Sci.*, vol. 10, no. 1 (2019).

[3] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *J. Discrete Math. Sci. Cryptography*, vol. 22, no. 4, pp. 491–498 (2019).

[4] H. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "New comparative study between DES, 3DES and AES within nine factors," arXiv preprint arXiv:1003.4085 (2010).

[5] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms," *3D Res.*, vol. 8, pp. 1–35 (2017).

[6] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *J. Discrete Math. Sci. Cryptography*, vol. 22, no. 4, pp. 499–507 (2019).

[7] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *J. Electron. Imaging*, vol. 21, no. 1, pp. 013014 (2012).

[8] S. Bowne, *Hands-On Cryptography with Python: Leverage the Power of Python to Encrypt and Decrypt Data*. Birmingham, U.K.: Packt Publishing (2018).

[9] O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree, and F. Y. Ahmed, "A survey and analysis of the image encryption methods," *Int. J. Appl. Eng. Res.*, vol. 12, no. 23, pp. 13265–13280 (2017).

[10] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors*, vol. 20, no. 18, pp. 5162 (2020).

[11] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser Technol.*, vol. 57, pp. 327–342 (2014).

[12] R. Padate and A. Patel, "Image encryption and decryption using AES algorithm," *Int. J. Electron. Commun. Eng. Technol.*, pp. 23–29 (2015).

[13] P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," *Global J. Comput. Sci. Technol.*, vol. 13, no. 15, pp. 15–22 (2013).

Received May, 2025