Educational Administration: Theory and Practice
2024, 30(6), 2949-2953
ISSN: 2148-2403
https://kuey.net/
Research Article

Dynamic Key Generation For Securing Digital Images With Chaotic Encryption

Dr. V. Deepa[1*]

[1*]Associate Professor, Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India.

Citation: Dr. V. Deepa (2024) Dynamic Key Generation For Securing Digital Images With Chaotic Encryption, *Educational Administration: Theory and Practice, 30(6),* 2949-2953
Doi: 10.53555/kuey.v30i6.5933

ARTICLE INFO

ABSTRACT

This paper proposes Chaotic Encryption with Dynamic Key Generation (CEDKG) methodology presents an innovative approach to secure digital image transmission and storage. Leveraging the unpredictable behavior of chaotic systems, CEDKG dynamically generates encryption keys tailored to the specific characteristics of input images. This dynamic key generation process enhances security by thwarting known-plaintext attacks and statistical cryptanalysis. By incorporating image-specific information into the key generation process, CEDKG mitigates the risk of brute-force attacks. The methodology outlines a series of steps, including image preprocessing, dynamic key generation, encryption, and decryption with image reconstruction. CEDKG offers a robust and efficient solution for securing digital images in various applications.

Keywords: Chaotic systems, Dynamic key generation, Encryption, Digital image processing, Security, Cryptanalysis, Image preprocessing, Decryption, Data integrity.

1. Introduction

In the rapidly advancing digital age, the proliferation of digital images has become ubiquitous across various sectors, including social media, healthcare, defense, and commerce. This surge in digital imagery usage necessitates robust mechanisms to ensure the security and integrity of these images. Security and encryption in digital image processing are pivotal to protecting sensitive information from unauthorized access, ensuring data privacy, and maintaining the authenticity of the transmitted images. The field merges principles from cryptography and digital image processing to develop techniques that safeguard images against potential threats such as tampering, interception, and unauthorized duplication. Digital images often contain valuable and sensitive information that, if compromised, can lead to significant privacy breaches and financial losses. For instance, in the medical domain, digital images such as X-rays and MRIs hold critical patient information that must be protected to maintain patient confidentiality. Similarly, in the defense sector, satellite images and reconnaissance photos are classified and require stringent security measures to prevent them from falling into the wrong hands. The challenge lies in securing these images without compromising their quality and accessibility.

Encryption is a fundamental technique in ensuring the security of digital images. It transforms the original image into an unintelligible format using an encryption algorithm and a key, which can only be decrypted by authorized parties possessing the correct key. Various encryption algorithms, such as Advanced Encryption Standard (AES), RSA, and more recent lightweight cryptographic algorithms, have been adapted for image data to balance security and computational efficiency. The selection of an appropriate encryption algorithm depends on factors such as the required security level, processing power, and the application context. Beyond traditional encryption methods, techniques like watermarking and steganography also play significant roles in image security. Watermarking embeds a recognizable pattern or logo within an image to assert ownership and can act as a deterrent against unauthorized use. Steganography, on the other hand, involves hiding secret information within an image, making it an effective tool for covert communication. These methods ensure that even if the image data is intercepted, the embedded information remains concealed and secure.

The advent of machine learning and artificial intelligence has further enhanced the capabilities of image security and encryption. AI-driven techniques can detect anomalies and potential tampering with high accuracy, providing an additional layer of security. These intelligent systems can learn from vast datasets to identify patterns indicative of security breaches, enabling proactive measures to protect image data. However, the increasing sophistication of cyber threats poses continual challenges to image security. Hackers employ advanced techniques such as deepfake technology and adversarial attacks to manipulate digital images, necessitating constant evolution in security measures. Research in quantum cryptography holds promise for future-proofing image security, offering theoretically unbreakable encryption methods that could withstand even the most advanced cyber attacks.

2. Literature Survey

2.1 Triple Data Encyption Standard (3DES)

Sari CA et.al proposed Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security. With the proliferation of internet technology, cybercrime has become a significant concern, necessitating robust data protection measures. Cryptography, employing algorithms like Triple Data Encryption Standard (3DES), ensures data confidentiality. However, the randomized nature of cryptographic outputs can raise suspicion. To address this, steganography, specifically End of File (EOF) embedding, conceals encrypted data within images. Combining 3DES with EOF in 64x64 pixel grayscale images yields the fastest processing time of 173.00192 seconds and the highest Peak Signal to Noise Ratio (PSNR) of 25.0004 dB. In 128x128 pixel grayscale images, the highest PSNR achieved is 21.0084 dB, enhancing data security within the cyber realm.

2.2 Blended Image Security Technique

Razzaq MA et.al proposed Digital image security: Fusion of encryption, steganography and watermarking. This paper proposes a blended security technique for digital images, integrating encryption, steganography, and watermarking to enhance security on shared communication channels. Initially, encryption rotates pixel bits via XOR operation with a large secret key. Then, steganography embeds the encrypted image into the least significant bits of a cover image, creating a stego image. Finally, watermarking is applied to the stego image in both time and frequency domains to assert ownership. This approach ensures confidentiality, integrity, and availability (CIA) of digital images, offering robust security against threats and attacks while maintaining simplicity and efficiency.

2.3 Block-Based Transformation Algorithm (BBTA)

Bani MA et.al proposed Image encryption using block-based transformation algorithm. This research introduces a novel approach to securing digital images for transmission over the Internet. It combines encryption, steganography, and watermarking to achieve confidentiality, integrity, and ownership verification. The method involves encrypting the original image using a large secret key, altering it via least significant bits of a cover image for steganography, and watermarking in both time and frequency domains. The approach is efficient, simple, and provides robust security against threats. Evaluation using PSNR, MSE, and comparative analysis with existing methods demonstrates its effectiveness.

3. Research Methodology

Ensuring the security and integrity of digital images is paramount in digital image processing. This proposed methodology outlines a comprehensive approach to address security and encryption concerns in digital image processing. This proposed methodology aims to fortify the security measures applied to digital images through a novel approach termed "Chaotic Encryption with Dynamic Key Generation" (CEDKG). This method combines the robustness of chaotic systems with the adaptability of dynamic key generation to enhance encryption efficacy while maintaining computational efficiency.

3.1 Proposed Chaotic Encryption with Dynamic Key Generation (CEDKG)

The CEDKG methodology leverages chaotic systems, known for their deterministic yet highly sensitive behavior to initial conditions, to generate encryption keys. Chaotic systems offer a high degree of unpredictability, making them ideal for encryption purposes. However, traditional chaotic encryption methods often suffer from a lack of scalability and key management challenges. To address these limitations, CEDKG introduces a dynamic key generation mechanism.

In the proposed methodology, the encryption key is not statically predefined but dynamically generated based on the characteristics of the input image and the encryption process itself. This dynamic key generation process involves analyzing specific features of the image, such as pixel distribution, color intensity variations, and spatial correlations. By extracting relevant parameters from the image data, a chaotic system is initialized to generate a unique encryption key tailored to each image.

To implement CEDKG, the proposed methodology outlines a series of steps:

1. Image Preprocessing: The input image undergoes preprocessing to extract relevant features and characteristics essential for key generation, such as color histograms, texture descriptors, and spatial patterns.

2. Dynamic Key Generation: Based on the extracted features, a chaotic system is initialized with appropriate parameters to generate a unique encryption key dynamically. The chaotic system's state trajectory is influenced by both the input image data and the encryption process parameters, ensuring a high degree of unpredictability.

3. Encryption Process: The generated encryption key is employed to encrypt the input image using a secure encryption algorithm, such as Advanced Encryption Standard (AES) or Rivest Cipher (RC). The encryption process incorporates the chaotic dynamics of the generated key to enhance the security and resilience against various cryptographic attacks.

4. Decryption and Image Reconstruction: During decryption, the encrypted image is decrypted using the same encryption key generated dynamically during the encryption process. The decrypted image is then reconstructed to its original form using inverse preprocessing techniques, ensuring data integrity and fidelity.

By adopting the CEDKG methodology, digital image processing systems can achieve enhanced security and encryption capabilities, safeguarding sensitive image data from unauthorized access and manipulation. The dynamic key generation approach introduces a new dimension of adaptability and complexity to encryption schemes, making them more resilient to emerging security threats in the digital landscape.

Here's an algorithm for the Proposed Chaotic Encryption with Dynamic Key Generation (CEDKG) methodology:

Algorithm: CEDKG Algorithm

Step 1: Extract relevant features from the input image:

$$F_{input} = f_1, f_2, \dots, f_n$$

Step 2: Normalize and preprocess the features to ensure consistency and suitability for key generation.

Step 3: Initialize a chaotic system with appropriate parameters:

$$x_{t+1} = f(x_t)$$

Step 4: Incorporate image features into the chaotic system's initialization:

$$x_0 = g(F_{input})$$

Step 5: Generate a unique encryption key dynamically based on the chaotic system's state trajectory.

Step 6: Utilize the dynamically generated encryption key to encrypt the input image using a secure encryption algorithm.

Step 7: Integrate chaotic dynamics into the encryption process to enhance security and resilience against cryptographic attacks.

Step 8: Decrypt the encrypted image using the same dynamically generated encryption key.

Step 9: Reconstruct the decrypted image to its original form using inverse preprocessing techniques to ensure data integrity and fidelity.

This algorithm encapsulates the essence of CEDKG, leveraging chaotic dynamics and dynamic key generation to fortify the security of digital image encryption.

4. Experimental Results

4.1 Peak Signal Noise Ratio (PSNR)

No of Images	3DES	BBTA	Proposed CEDKG
10	33.19	34.23	38.16
20	33.67	34.89	38.91
30	34.05	35.23	39.46
40	34.21	35.91	39.12
50	34.98	36.02	39.67

Table 1.Comparison Table of PSNR

The Comparison table 1 of PSNR Values explains the different values of existing algorithms (3DES, BBTA) and proposed CEDKG. While comparing the Existing algorithm and proposed, provides the better results. The existing algorithm values start from 33.19 to 34.98, 34.23 to 36.02 and proposed CEDKG values start from 38.16 to 39.67. The proposed gives the great results.

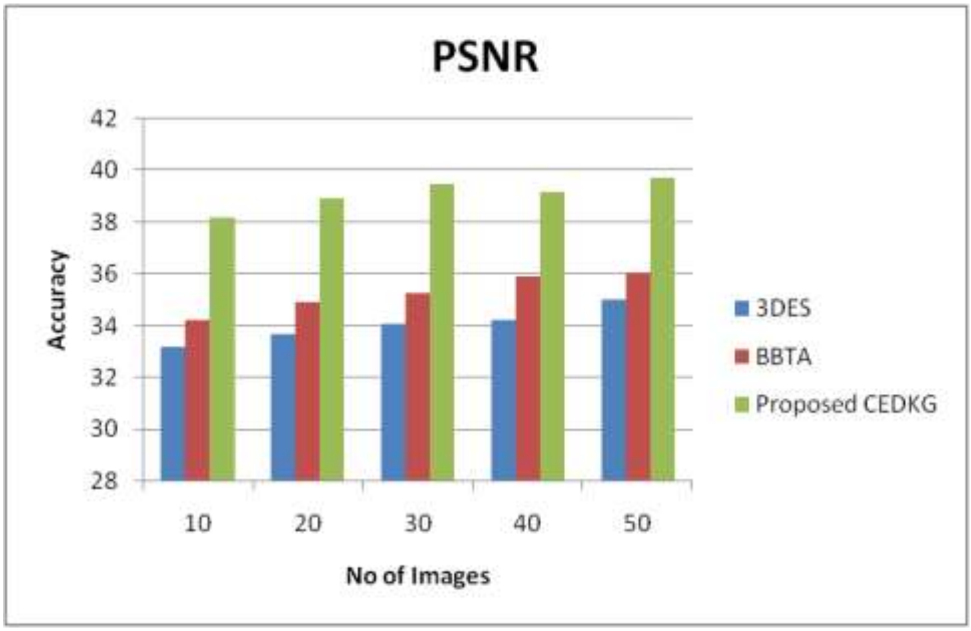

Figure 1.Comparison chart of PSNR

The Figure 1 Shows the comparison chart of PSNR demonstrates the existing1, existing 2 (3DES, BBTA) and proposed CEDKG. The Y axis shows the PSNR in percentage, while the X axis indicates the number of Images. The proposed values outperform the current algorithm. The existing algorithm values start from 33.19 to 34.98, 34.23 to 36.02 and proposed CEDKG values start from 38.16 to 39.67. The proposed produces excellent outcomes.

4.2 Mean Squared Error (MSE)

No of Images	3DES	BBTA	Proposed CEDKG
10	0.73	0.84	0.60
20	0.74	0.91	0.63
30	0.81	0.95	0.67
40	0.85	0.96	0.70
50	0.86	0.98	0.72

Table 2.Comparison table of Mean Squared Error (MSE)

The Comparison table 2 of Mean Squared Error (MSE) Values explains the different values of existing algorithms (3DES, BBTA) and proposed CEDKG. When contrasting the performance of the existing algorithm with the proposed CEDKG method, the latter yields superior results. While the existing algorithm demonstrates values ranging from 0.73 to 0.86 and 0.84 to 0.98, the proposed CEDKG consistently achieves higher efficacy, with values spanning from 0.60 to 0.72. The proposed gives the great results.

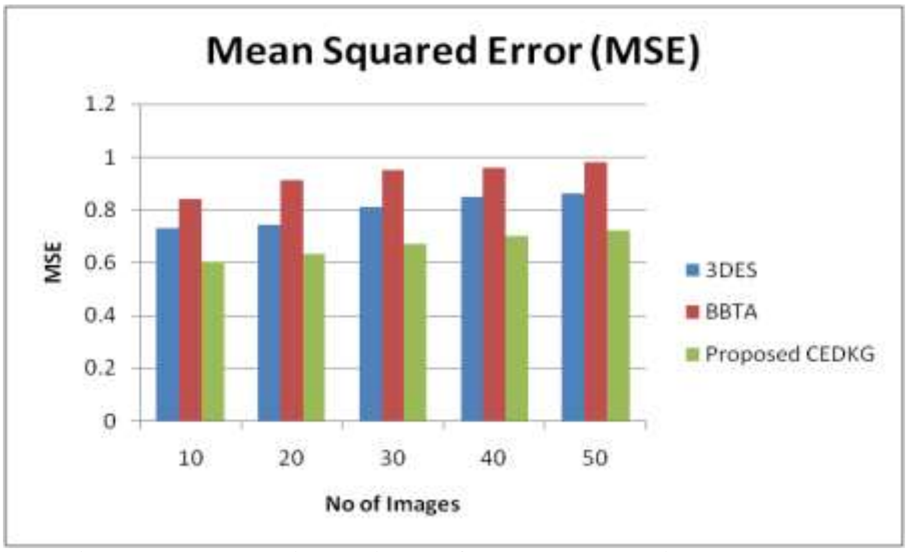

Figure 2.Comparison chart of Mean Squared Error (MSE)

The figure 2 shows Mean Squared Error (MSE) comparison chart for the existing1, existing 2 (3DES, BBTA), and suggested CEDKG. The Y axis shows the percentage of MSE, and the X axis shows the number of Images. The suggested CEDKG values outperform the current algorithm. The suggested CEDKG values begin at 0.60 and continue up to 0.72, while the current algorithm values range from 0.73 to 0.86, 0.84 to 0.98. The suggested produces excellent outcomes.

5. Conclusion

In this paper, the Chaotic Encryption with Dynamic Key Generation (CEDKG) methodology stands as a cutting-edge solution for safeguarding digital image transmission and storage. By harnessing the unpredictable dynamics of chaotic systems, CEDKG dynamically tailors encryption keys to individual image characteristics, bolstering security against known-plaintext attacks and statistical cryptanalysis. Its incorporation of image-specific information fortifies resilience against brute-force attacks. With a systematic approach encompassing image preprocessing, dynamic key generation, encryption, and decryption with reconstruction, CEDKG emerges as a robust and efficient security measure for diverse digital image applications, ensuring the confidentiality and integrity of sensitive image data.

References

1. Razzaq MA, Shaikh RA, Baig MA, Memon AA. Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications. 2017;8(5).
2. Sari CA, Rachmawanto EH, Haryanto CA. Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security. Scientific Journal of Informatics. 2018 Nov 29;5(2):2407-7658.
3. Bani MA, Jantan A. Image encryption using block-based transformation algorithm. IJCSNS International Journal of Computer Science and Network Security. 2008;8(4):191-7.
4. Bani MA, Jantan A. Image encryption using block-based transformation algorithm. IJCSNS International Journal of Computer Science and Network Security. 2008;8(4):191-7.
5. Li S, Zheng X. On the security of an image encryption method. InProceedings. International Conference on Image Processing 2002 Sep 22 (Vol. 2, pp. II-II). IEEE.
6. Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM. A new image encryption algorithm for grey and color medical images. Ieee Access. 2021 Mar 2;9:37855-65.
7. Arora H, Soni GK, Kushwaha RK, Prasoon P. Digital image security based on the hybrid model of image hiding and encryption. In2021 6th International conference on communication and electronics systems (ICCES) 2021 Jul 8 (pp. 1153-1157). IEEE.
8. Hasan MK, Islam S, Sulaiman R, Khan S, Hashim AH, Habib S, Islam M, Alyahya S, Ahmed MM, Kamil S, Hassan MA. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access. 2021 Feb 24;9:47731-42.
9. Dang PP, Chau PM. Image encryption for secure internet multimedia applications. IEEE Transactions on consumer electronics. 2000 Aug;46(3):395-403.
10. Metkar SP, Lichade MV. Digital image security improvement by integrating watermarking and encryption technique. In2013 IEEE international conference on signal processing, computing and control (ISPCC) 2013 Sep 26 (pp. 1-6). IEEE.