IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

Image Scrambling Toward Efficient Encrypted Image Retrieval in Cloud Computing

Ms. Payal Ramteke[1], Ms. Akshata Nawale[2], MS. Priti Kashyap[3], Ms. Pornima Petkar[4]
Students, Computer Science and Engineering[1-4]
Shri Sai College of Engineering and Technology, India

Abstract: *A previously proposed image encryption method, which applied dual scrambling at both the pixel position and bit levels, was subjected to cryptanalysis. The original algorithm rearranged pixel locations using a chaotic sequence and further scrambled individual pixel bits (0s and 1s) through a second chaotic sequence derived from a user-provided key. While the designers claimed that the method could withstand chosen-plaintext attacks, detailed analysis revealed that its security primarily relied on three components: the pixel position scrambling sequence (T), the bit-level scrambling sequence (WT), and the diffusion sequence (S). Among these, only the generation of sequence T was influenced by the original image's pixel values, whereas WT and S remained independent of the image content. This structural weakness allowed attackers to successfully perform chosen-plaintext attacks and recover these equivalent key streams, effectively decrypting the image. The feasibility of this attack was confirmed through both theoretical evaluation and experimental validation. To address this vulnerability, the authors introduced an improved encryption algorithm designed to resist chosen-plaintext attacks and mimic the behaviour of a one-time pad system.*

Keywords: cryptanalysis; chosen plaintext attack; image encryption; chaotic system

I. INTRODUCTION

With the increasing use of digital images for data transmission and storage, ensuring their security has become essential due to the sensitive information they may contain. Among various protection methods like data hiding and watermarking, image encryption stands out as a direct and effective approach, often involving pixel scrambling and diffusion. Chaotic systems are frequently used in these algorithms because of their pseudo-randomness and high sensitivity to initial conditions.

Over time, researchers have developed various chaos-based encryption methods, including bit-level scrambling, DNA coding, and hyperchaotic systems. These algorithms aim to resist attacks such as chosen-plaintext attacks by incorporating dynamic feedback and complex transformations.

However, many of these methods have shown vulnerabilities when their keystreams do not depend on the image itself. Cryptanalysis has revealed that such independence allows attackers to retrieve encryption keys using a small number of specially crafted plaintexts.

In one such case, Deng et al. proposed a dual scrambling algorithm using Kent maps, which was later shown to be insecure against chosen-plaintext attacks. This paper reviews their approach, identifies its weaknesses, demonstrates an attack, and finally introduces an improved algorithm that strengthens security and enhances resistance to such cryptanalytic methods.

II. LITERATURE REVIEW

With the rise of digital image sharing, securing visual data has become essential. Among various protection methods, image encryption is widely used due to its direct ability to transform original images into unintelligible forms. Most modern techniques use pixel scrambling and diffusion, often powered by chaotic systems known for their randomness and sensitivity to initial conditions. Fridrich pioneered chaos-based image encryption, leading to numerous improvements. Yang et al. [used fractional-order chaotic systems, while Zhu et al. combined SHA-256 and dynamic

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 8, June 2025 Impact Factor: 7.67

ciphertext feedback to counter chosen-plaintext attacks. Xu et al. proposed block scrambling with dynamic index diffusion, and others explored hyperchaotic systems, dual S-boxes, and avalanche effects.DNA-coding methods have also gained traction. Rehman et al and others incorporated DNA encoding and chaotic diffusion to enhance security and plaintext sensitivity.Despite these innovations, many schemes have been broken due to weak links between the keystream and plaintext. Researchers demonstrated that such independence allows chosen-plaintext attacks to reconstruct the encryption key. Deng et al. introduced a dual chaotic scrambling method using Kent maps, but it too was found vulnerable under cryptanalysis. These studies highlight the need for encryption systems where the keystream tightly depends on the image content to resist modern cryptanalytic attacks.

III. METHODOLOGY

The improved encryption algorithm enhances the original chaotic image encryption scheme by strengthening key dependency and adding bit-level security. It consists of the following three main phases:

Pixel-Level Global Scrambling

Convert the image matrix *A* of size *m x n* into a 1D sequence *P*.

Compute the sum of pixel values to derive the control parameter *a* and iteration count*K* for the Kent chaotic map:

$a=\frac{sum}{108}$, K= 1000+mod(sum,1000)

Generate a chaotic sequence using the Kent map, sort it, and obtain a scrambling index sequence TTT. Then scramble the image as:

p′(i)=p(t(i)),i=1, 2…,mn

Bit-Level Scrambling

Recalculate a control parameter a_2 and generate a new chaotic sequence D.

For each element *d(i)* in *D,* extract 8 decimal digits to construct a permutation *WT*for bit reordering.

Convert each pixel value to binary, apply bit scrambling using *WT,* and convert the scrambled bits back to decimal to get the intermediate ciphertext sequence *C′*

Diffusion Process

The final diffusion adds confusion and chaining across pixel values using the following formulas:

Construct sequence *VP* :

$$vp(1) = j = 2\sum mnc'(j), vp(i) = vp(i-1) - c'(i) for\ i = 2,3,\dots,mn$$

Generate sequence *SP* .:

$$sp(i) = mod(\lfloor \frac{vp(i).d(i)}{2565\ X\ 10} \rfloor, 256)$$

Compute reference index kt(i):

$$kt(i) = \lfloor \frac{c'(i+1)\cdot(i-1)}{256} \rfloor + 1 for\ i = 2,\dots,mn-1$$

Generate the final ciphertext *C* :

$$\begin{cases} c(1) = mod(sp(1) + c'(1), 256) \\ c(i) = mod(sp(i) + c'(i), 256) \oplus c\big(kt(i)\big), i = 2,\dots,mn-1 \\ c(mn) = mod\big(sp(mn)\big) + c(mn, 256) \end{cases}$$

DOI: 10.48175/IJARSCT-28197

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

3.1 Decryption methodology

The decryption process is the inverse of the encryption pipeline and is divided into three main phases:
The first step involves undoing the pixel value diffusion to retrieve the intermediate scrambled pixel values C′.

Recalculate VP, SP, and Kt

Using the same chaotic sequence DDD, recompute the sequences:

$$VP = \{vp(1), vp(2), \dots, vp(mn)\}$$
$$SP = \{sp(1), sp(2), \dots, sp(mn)\}$$
$$Kt = \{kt(2), kt(3), \dots, kt(mn-1)\}$$

Compute Intermediate Ciphertext C′C'C′

Use the inverse of the encryption formula:

$$\begin{cases} c'(1) = mod(c(1) - sp(1), 256) \\ c'(i) = mod\left(\left(c(i) \oplus c(kt(i))\right) - sp(i), 256\right), i = 2, \dots, mn-1 \\ c'(mn) = mod(c(mn) - sp(mn), 256) \end{cases}$$

This step restores the **bit-scrambled pixel values**.

Reverse Bit-Level Scrambling

In this phase, the scrambled binary values are reordered back to their original form:
Recalculate the Permutation *WT*
From the same chaotic sequence*D*, regenerate the bit permutation pattern *WT*.
Binary Conversion and Unscrambling
For each pixel value in *C′,* convert it to an 8-bit binary string.
Apply the **inverse permutation** WT^{-1} to reorder the bits back to their original sequence.
Convert the unscrambled bits to decimal to get the **pixel-scrambled sequence** P′.

Reverse Pixel Position Scrambling

Finally, the original spatial arrangement of the pixels is restored:
Regenerate the Position Scrambling Sequence TTT
Using the sum of the original pixel values (which must be known or transmitted securely), recalculate:
a=sum/108
K=1000+mod(sum, 1000)
Generate the same chaotic sequence and derive the position index vector TTT.

Inverse Permutation of Pixels

Initialize an array of length *mn* to hold the final pixel values.
For each index iii, place the pixel value at position *T(i)* back to its original location iii:
P(t(i)) = P'(i)
Reshape the 1D array into the original *m*×*n* image matrix A

DOI: 10.48175/IJARSCT-28197

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

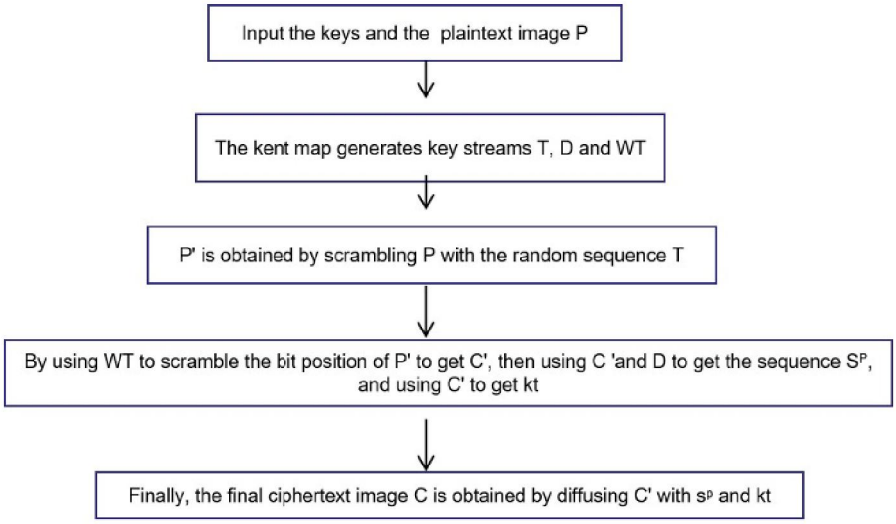

Figure 1. The flow chart of the improved encryption process.

IV. EXPERIMENTAL SIMULATION

To validate the effectiveness of the improved image encryption algorithm, a set of experiments were conducted using MATLAB R2015a. The following grayscale test images were selected:
Cameraman (256 × 256 pixels)
Peppers (384 × 512 pixels)

4.1. Simulation Setup

The encryption parameters were initialized as follows:
Initial value of Kent map: x0=0.3987623x_0 = 0.3987623x0=0.3987623
Control parameter: a2=0.8739a_2 = 0.8739a2=0.8739
Number of iterations: k2=3000k_2 = 3000k2=3000
The encryption and decryption operations were applied to both test images using the improved algorithm.

4.2. Visual Results

The encryption and decryption results are illustrated in **Figure 2** of the original paper:
Figure 2(a): Encrypted "Cameraman" image (256×256)
Figure 2(b): Decrypted result of (a) — matches original exactly
Figure 2(c): Encrypted "Peppers" image (384×512)
Figure 2(d): Decrypted result of (c) — matches original exactly
These results confirm that the algorithm achieves lossless encryption and decryption.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

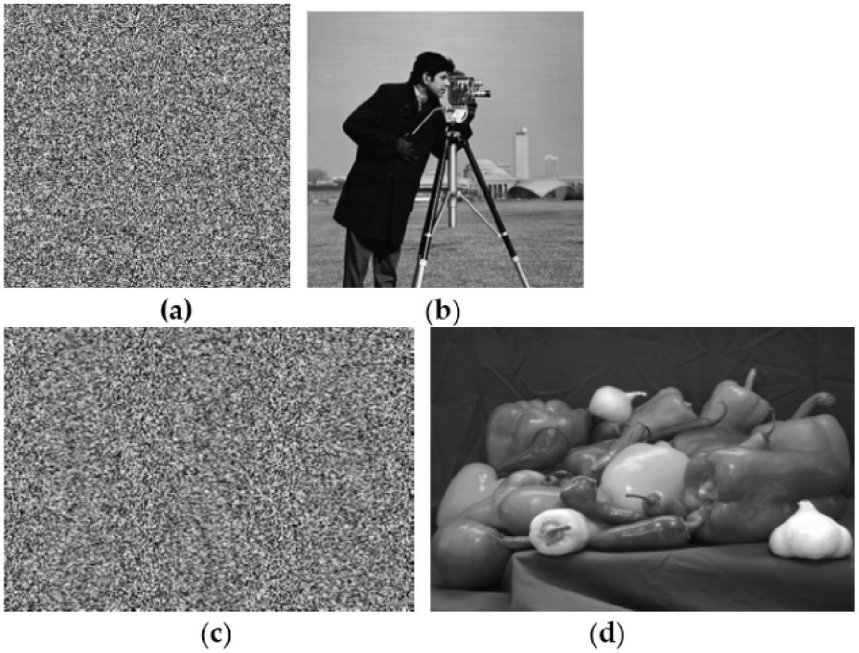

Figure 2. The encryption and decryption effect. (a) The 256 × 256 encrypted image. (b) The decrypt Image of (a). (c) The 384 × 512 encrypted image. (d) The decrypted image of (c).

4.3 Time and Cost Analysis

The execution time is a key indicator for assessing the practicality of an image encryption algorithm, especially in real-time or resource-constrained applications. Table 5 summarizes the encryption and decryption times for various standard test images:

image	Size (pixels)	Encryption Time (s)	Encryption Time (s)
Rice	256 × 256	0.0349	0.0495
Autumn	206 x 345	0.0950	0.1295
Peppers	384 x 512	0.1110	0.1307
Cameraman	256 x 256	0.0346	0.0515

The encryption time comprises the generation of chaotic sequences, global pixel scrambling, bit-level scrambling, and the diffusion process. Similarly, the decryption time includes chaotic sequence regeneration, inverse spatial scrambling, inverse bit scrambling, and reverse diffusion.

These results demonstrate that the improved algorithm performs efficiently, with encryption and decryption operations completing in fractions of a second. This makes the scheme well-suited for applications requiring fast and lightweight image protection.

V. CONCLUSION

This study analysed an image encryption algorithm and revealed its vulnerability to chosen-plaintext attacks, where equivalent key components could be derived using only a few specific image pairs. To resolve this issue, an enhanced algorithm was proposed that incorporates dynamic key generation based on the characteristics of the input image. The improved method strengthens resistance against cryptanalytic attacks while maintaining computational efficiency. Experimental evaluations demonstrated its high information entropy, strong key sensitivity, and robustness against differential analysis. These qualities make the proposed algorithm a reliable and secure solution for protecting digital images in various applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

REFERENCES

[1]. Lowlesh Yadav and Asha Ambhaikar, "IOHT based Tele-Healthcare Support System for Feasibility and perfor-mance analysis," Journal of Electrical Systems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.

[2]. L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.

[3]. L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.

[4]. Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879.

[5]. Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

[6]. Sandhya.S. Bachar, Neehal.B.Jiwane, Ashish.B. Deharkar "Sentiment analysis of social media" DOI: 10.17148/IJARCCE.2022.111234 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 12, December 2022.

[7]. Akshay A. Zade, ,Lowlesh N. Yadav, Neehal B. Jiwane. "A Review on Voice Browser" DOI: 10.17148/IJARCCE.2022.111238 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 12, December 2022.

[8]. Omkar K. Khadke, Lowlesh N. Yadav, Neehal B. Jiwane. "Review On Challenges and Issues in Data Mining" DOI: 10.17148/IJARCCE.2022.111149 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 11, November 2022

[9]. Miss. Vaishali Vaidya, Mr. Vijay Rakhade, Mr. Neehal B. Jiwane. "VOICE CONTROLLED ROBOTIC CAR BY USING ARDUINO KIT" DOI: 10.17148/IJARCCE.2022.111232 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 12, December 2022.

[10]. Atharv Arun Yenurkar , Asst Prof. Neehal B. Jiwane , Asst. Prof. Ashish B. Deharkar. "Effective Validation for Pervasive Computing and Mobile Computing Using MAC Algorithm". International Journal of Research Publication and Reviews, Vol 3, no 12, pp 470-473 December 2022.

[11]. Pooja Raju Katore, Asst. Prof. Ashish B. Deharkar , Asst. Prof. Neehal B. Jiwane. "Cloud Computing and Cloud Computing Technologies: A-Review". International Journal of Research Publication and Reviews, Vol 3, no 12, pp 538-540 December 2022

[12]. Combining Vedic & Traditional Mathematic Practices for Enhancing Computational Speed in Day-To-Day Scenarios, Speed in Day-To-Day Scenarios, Conference: Industrial Engineering Journal ISSN: 0970-2555 Website: www.ivyscientific.org, At: Industrial Engineering Journal ISSN: 0970-2555 , Website: www.ivyscientific.org. (UGC JOURNAL)

[13]. python.net, December 2022, DOI:10.17148/IJARCCE.2022.111237 , Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[14]. A Survey for Credit Card Fraud Detection Using Machine Learning ,December 2022, DOI:10.17148/IJARCCE.2022.111221 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

[15]. GRB 210217A: a short or a long GRB? ,December2022 ,DOI: 10.1007/s12036-022-09822, Journal of Astrophysics and Astronomy , Published by Online ISSN: 0973-7758, Print ISSN: 0250-6335.

[16]. Pronunciation Problems of English Language Learners in India, November 2022 ,DOI: 10.17148/IJARCCE.2022.111151 , Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[17]. Photometric and spectroscopic analysis of the Type II SN 2020jfo with a short plateau, November 2022 , DOI:10.48550/arXiv.2211.02823 ,License CC BY 4.0.

[18]. Artificial Neural Network, May 2022 , DOI: 10.17148/IJARCCE.2022.115196 , Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[19]. Cloud Storage Security Based on Dynamic key Generation Technique ,May 2022 DOI: 10.17148/IJARCCE.2022.115189 , Conference: International Journal of Advanced Research in Computer and Communication Engineering

[20]. Research on Techniques for Resolving Big Data Issues ,May2022,DOI: 10.17148/IJARCCE.2022.115192 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering

[21]. STUDY on INTERNET of THINGS BASED APPLICATION ,May2022 , DOI: 10.17148/IJARCCE.2022.115179 , Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[22]. Research on Data Mining, May 2022 , DOI: 10.17148/IJARCCE.2022.115176, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[23]. Security Solution of The Atm and Banking System, May 2022 ,DOI: 10.17148/IJARCCE.2022.115165 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[24]. Study on Positive and Negative Effects of Social Media on Society , May 2022 , DOI: 10.17148/IJARCCE.2022.115161 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[25]. Research on Association Rule Mining Algorithms , May 2022 , DOI: 10.17148/IJARCCE.2022.115152 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[26]. Block chain Technology , May 2022 ,DOI: 10.17148/IJARCCE.2022.115154 Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[27]. INTERNET of THINGS RESEARCH CHALLANGES and FUTURE SCOPE , May 2022 DOI: 10.17148/IJARCCE.2022.115150 , Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[28]. .Data Collection and Analysis in a Smart Home Automation System , May 2022 DOI: 10.17148/IJARCCE.2022.115148 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[29]. Using Encryption Algorithms in Cloud Computing for Data Security and Privacy , May 2022 , DOI:10.17148/IJARCCE.2022.115149 , Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[30]. An Efficient Way to Detect the Duplicate Data in Cloud by using TRE Mechanism , May 2022 ,DOI:10.17148/IJARCCE.2022.115139 ,Conference: International Journal of Advanced Research in Computer and Communication Engineering , Volume: 11.