Detecting the Strength of Security In Cryptosystem Using RDH and CBIR

M. Shankar[1], S. V. Raga Keerthini[2], S. Sowmiya[3], P. Yashika Sri[4]
[1] Assistant Professor, Department of Computer Science and Engineering
[2, 3, 4] Final Year, Department of Computer Science and Engineering
[1, 2, 3, 4]Erode Sengunthar Engineering College (Autonomous) Thudupathi, Erode, Tamilnadu, India.

Abstract- *These days, many people use cloud storage to keep their files, but there are serious worries about how safe this data is. One way to make it safer is by using cryptography, which involves encoding data so that only authorized people can access it. To address these security concerns, experts recommend a mix of two encryption methods: RDH and triple DES. This combination adds extra layers of protection to data before it goes onto the cloud. Studies have shown that this approach significantly improves data security. Specifically for protecting images, we propose using a combination of RDH and triple DES in a block-based transformation method. What's great about this system is that even after the images are encrypted, you can still do things like find specific images or make changes to them directly, without compromising their security.*

Keywords- deployment models, 1infrastructure as a service, cryptosystems, machine learning

I. INTRODUCTION

The term "cloud computing" has gained widespread popularity in the realm of IT, offering a glimpse into the future of computing both technically and societally. While the term itself is relatively recent, the idea of centralizing computing and storage in geographically dispersed data centers operated by external entities is not new. This concept emerged in the 1990s, alongside other distributed computing methodologies such as grid computing. Cloud computing, operating under a utility computing model, strives to provide IT services to customers via the cloud, offering increased flexibility, availability, reliability, and scalability on demand.
There are four primary access types to cloud deployment models: Public, Private, Hybrid, and Community. The public cloud allows easy accessibility to systems and services for the general population. However, its openness may pose security concerns, akin to those faced with email services. Conversely, the private cloud enables access to systems and services exclusively within an organization, offering a heightened level of security due to its restricted nature. Community cloud facilitates access to systems and services for groups of organizations. A hybrid cloud integrates both public and private clouds, leveraging the public cloud for non-essential tasks and the private cloud for critical operations. Infrastructure as a Service (IaaS) offers access to fundamental resources such as physical machines, virtual machines, and virtual storage. In this model, a third-party provider hosts hardware, software, servers, storage, and other infrastructure components on behalf of customers. IaaS providers handle tasks such as system maintenance, backup, and resilience planning, while also hosting users' applications. IaaS platforms offer highly scalable resources that can be adjusted according to requirements. This flexibility makes IaaS ideal for workloads that are ad hoc, experimental, or prone to sudden changes. Additionally, IaaS setups provide features like dynamic scaling, desktop virtualization, automation of administrative tasks, and policy-based services.

Modern information security is based on cryptosystems, which are the cornerstone of safe data transmission and storage. A cryptosystem is a systematic configuration of cryptographic protocols and algorithms intended to authenticate, maintain confidentiality, and decode sensitive data in communication. These systems are used in many different contexts, such as government and military communications, data storage, and safe online transactions. Cryptosystems, at their foundation, use intricate mathematical formulas to convert plaintext into cipher text, which prevents unauthorized parties from deciphering the data. A cryptosystem's strength and efficacy are determined by several variables, including the security procedures, key lengths, and encryption algorithms.

Within the larger subject of artificial intelligence, machine learning is a revolutionary discipline that has completely changed how computers can learn from and adapt to data. It covers many methods and algorithms that let robots see trends, anticipate outcomes, and get better at what they do over time. Fundamentally, machine learning is based on the notion that computers may be taught to learn from data instead of explicit programming instructions. Machine learning models can interpret intricate linkages and reveal hidden insights in various disciplines, from picture and

speech recognition to financial predictions and healthcare diagnostics, by utilizing large datasets and strong computational resources. Machine learning is central to automating tasks, improving decision-making processes, and propelling innovations in domains as diverse as autonomous vehicles, natural language processing, and personalized recommendations, as the volume of data generated in today's digital age continues to grow. It's a vital and active field for research and development because of its many uses, which are always changing.

II. LITERATURE REVIEW

This project[1] develops an image encryption algorithm utilizing a hyper-chaotic system to enhance security. It shuffles pixel arrangement and rearranges individual bits, utilizing cryptographic keys generated by the hyper-chaotic system for decryption. This ensures that only authorized parties can access the original image, providing robust protection against unauthorized access. Additionally, the rise of social networks has led to increased unverified rumors, prompting research into deep learning for automatic rumor detection. This literature review[2] scrutinizes 108 studies from prominent databases, addressing seven key research questions. It highlights prevailing trends in utilizing deep learning for rumor detection and outlines challenges in this area. The review proposes future research directions and serves as a valuable resource for researchers, offering insights into performance metrics, dataset characteristics, and deep learning models used. It aids in identifying annotated datasets for benchmarking new approaches and advancing the field of rumor detection.

This composition [3] introduces an AI-based method to predict Quality of Experience (QoE) for 360-degree videos in Virtual Reality (VR), focusing on perceptual quality and cybersickness. It considers user familiarity and interest in 360-degree videos. The study includes a trial with 96 video tests and data collection from 29 users. A Linear Regression (LR) model achieves an 86% accuracy rate for perceptual quality, matching emotional assessment closely. LR is compared with k-nearest Neighbors (kNN), Support Vector Machine (SVM), and Decision Tree (DT) algorithms. Additionally, a Brain Network-based model predicts cybersickness competitively. This project[4] merges compressive sensing and Fourier Transform for efficient image compression and security. Compressive sensing captures signals in a compressed form exploiting signal sparsity, while Fourier Transform reduces redundancy by converting image data into frequency domain information. After transformation, compressive sensing further reduces data while maintaining essential information. Encryption techniques are then applied to secure the compressed image data, ensuring access only for authorized users. This integration provides a comprehensive solution, reducing storage space and preventing unauthorized access effectively. In this study, [5] we investigate the encryption and decryption processes of color images through the synchronization of polarization dynamics in free-running vertical-cavity surface-emitting lasers (VCSELs), specifically employing a bidirectional master-slave configuration or two-way coupling with two VCSELs. These VCSELs demonstrate hyper-chaotic behavior and exhibit a high degree of synchronization in their emission characteristics. This study[6] proposes a method to encrypt images rapidly and effectively using chaotic systems. In simple terms, chaotic systems are used to generate random-like sequences of numbers that are highly sensitive to initial conditions. These sequences are then utilized to shuffle the pixels of an image (permutation) and alter their values (diffusion) simultaneously, making it extremely difficult for unauthorized users to decipher the original image without the correct decryption key. This approach offers a balance between security and efficiency, providing a fast encryption process while maintaining a high level of protection for the image data. By leveraging chaotic systems, the encryption scheme ensures unpredictability and randomness, key factors in secure encryption methods.

This project[7] introduces a new method for encrypting images using chaos theory. In simple terms, chaos theory involves systems that are highly sensitive to initial conditions, producing seemingly random behavior. In this project, chaotic systems are employed to generate encryption keys. The key idea is to manipulate the image data at the level of pairs of bits, rather than individual bits. This process involves combining bits in pairs and applying chaotic operations to them, which enhances the security of the encryption process. By utilizing chaos theory and operating at the bit-pair level, the encryption scheme aims to provide robust protection for image data while maintaining efficiency in the encryption and decryption processes. This approach offers a balance between security and computational complexity, making it suitable for practical applications where both speed and security are essential. This project [8] employs Elliptic Curve ElGamal Encryption, utilizing complex mathematical operations based on elliptic curves to scramble image data securely, akin to locking it in a box accessible only with the right key. Additionally, Chaotic Systems, generating unpredictable patterns, are integrated into the encryption process, making decryption challenging for unauthorized users. By combining these approaches, the method ensures robust protection for sensitive image data, rendering it extremely difficult for unauthorized access. Thus,

it effectively safeguards image privacy from potential threats, enhancing security measures significantly.

This project[9] integrates chaos theory into image encryption, utilizing confusion, diffusion, dynamic substitution, and chaotic sequences to establish a robust encryption approach. Rapid urban population growth brings challenges like pollution and traffic congestion, prompting smart cities to utilize IoT for solutions in healthcare and agriculture. IoT devices collect vast data, analyzed through DL for valuable insights. This survey[10] examines IoT-DL integration for smart city development, starting with IoT and its big data characteristics. It discusses computing infrastructures like cloud, fog, and edge computing supporting IoT analytics. Additionally, it explores popular DL models and recent research combining IoT-DL for urban applications. The survey concludes by addressing current challenges in smart city service advancement.

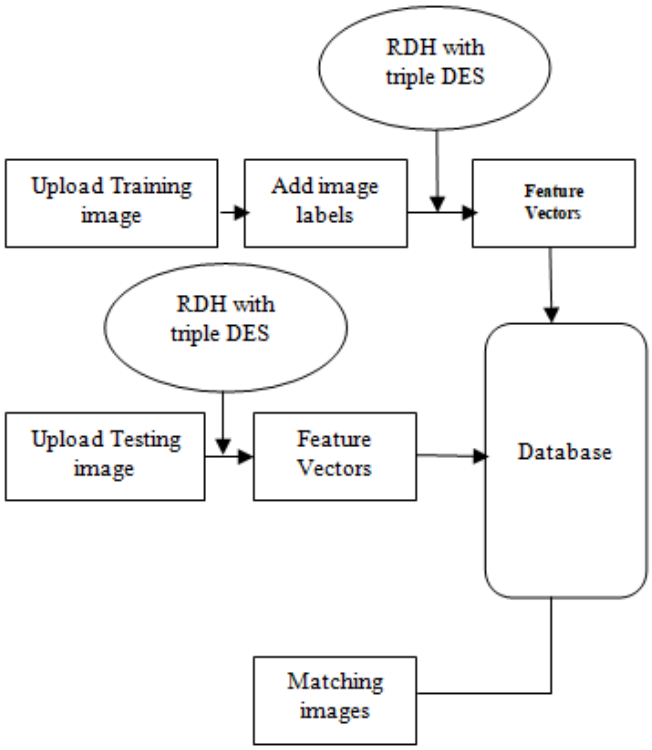
This project[11] merges compressive sensing and Fourier Transform for efficient image compression and security. Compressive sensing captures signals in a compressed form exploiting signal sparsity, while Fourier Transform reduces redundancy by converting image data into frequency domain information. After transformation, compressive sensing further reduces data while maintaining essential information. Encryption techniques are then applied to secure the compressed image data, ensuring access only for authorized users. This integration provides a comprehensive solution, reducing storage space and preventing unauthorized access effectively. Hanze University initiated [4] a health promotion program aimed at reducing sedentary lifestyles among employees. An integral part of this program involved using activity trackers to monitor daily step counts, which then informed fortnightly coaching sessions. This study explores the potential for automating aspects of the coaching process by delivering personalized, real-time feedback on participants' progress toward achieving their daily step goals. To achieve this, the data collected from step counts was used to train eight distinct machine learning algorithms to predict the likelihood of meeting individualized daily step thresholds on an hourly basis. Among these algorithms, the Random Forest algorithm emerged as the most effective in 80% of cases, boasting a mean accuracy of 0.93 (with a range between 0.88 and 0.99) and a mean F1-score of 0.90 (with a range between 0.87 and 0.94).

III. EXISTING SYSTEM

Recent advancements in multimedia technologies have heightened concerns about the security of digital data, prompting researchers to explore modifications to existing security protocols. However, numerous encryption algorithms proposed over the last few decades have proven to be insecure, posing significant threats to critical data. The choice of an appropriate encryption algorithm is crucial for safeguarding data, but selecting the right one can be time-consuming when evaluated individually. To address this, we propose a security-level detection approach for image encryption algorithms using a support vector machine (SVM). Additionally, we have created a dataset incorporating standard encryption security parameters, such as entropy, contrast, homogeneity, peak signal-to-noise ratio, mean square error, energy, and correlation, extracted from different cipher images. These parameters serve as features, and the dataset is categorized into three security levels: strong, acceptable, and weak. The dataset used to train the SVM should be comprehensive and representative of the range of image encryption algorithms that are available. If the dataset is not representative, the SVM may not be able to predict the security level of new algorithms accurately. The security parameters used to characterize the security level of the encryption algorithms should be carefully selected. If the security parameters are not well chosen, the SVM may not be able to learn the relationship between security parameters and security level accurately.

IV. PROPOSED SYSTEM

The envisioned Content-Based Image Retrieval (CBIR) system incorporates Reversible Data Hiding (RDH) with the Triple DES algorithm to encode and categorize visual image characteristics such as color, shape, texture, and spatial arrangement for efficient indexing. Ongoing CBIR research focuses on refining methodologies for image database analysis, interpretation, cataloging, and indexing, alongside efforts to assess retrieval system performance. This project introduces a novel steganography approach through reversible texture synthesis, where small texture images, whether artistically crafted or photographically captured, are resampled to generate new textures of varying sizes while employing a patch-based technique to embed secret messages, ensuring reversibility for source texture recovery during message extraction.



4.1 IMAGE PREPROCESSING AND FEATURE EXTRACTION

In the initial input module, the feature vectors are extracted from input images, and these images are subsequently stored within the dataset alongside their respective feature vectors. Moving on to the second module, known as the query module, an image is inputted, and its feature vector is also extracted. Finally, in the third module, which involves the retrieval process, a comparison is made by matching the feature vector of the query image with those stored in the dataset. These feature vectors typically encompass various essential aspects like texture, color, local shape, and spatial information. The growing demand for efficiently searching image datasets of ever-expanding sizes has fueled the widespread popularity of Content-Based Image Retrieval (CBIR) techniques.

4.2 RDH FEATURE EXTRACTION FOR REFERENCE AND TEST IMAGES

The process of transforming image data into scale-invariant coordinates, generating a multitude of features that comprehensively cover the image across various scales and locations, poses a significant challenge in shape representation and description. This challenge arises from the inherent loss of one dimension when projecting a 3-D real-world object onto a 2-D image plane, resulting in a shape representation that only captures a partial aspect of the object. Moreover, shape data in images is often compromised by noise, defects, arbitrary distortion, and occlusion, making it even more complex to extract meaningful information. Additionally, the determination of which aspects of shape are crucial remains uncertain. Nonetheless, the extracted feature vectors exhibit invariance to geometric variations, partial resistance to lighting changes, and resilience to geometric deformations, enhancing their utility in addressing these intricate challenges in shape analysis.

4.3 DATA EMBEDDING AND EXTRACTION

This module employs message-oriented texture synthesis to embed a secret message, resulting in the creation of the stego synthetic texture. To accomplish this, it calculates the ranks of all potential patches. The chosen patch for message embedding corresponds to a rank that matches the decimal value of a specific n-bit secret message segment. This selected patch is then placed into the designated working location, effectively concealing a portion of the n-bit secret message within it. The subsequent message extraction and authentication module consists of three key sub-steps. The initial sub-step involves generating a candidate list by considering the overlapping region concerning the current working location.

4.4 TRIPLE DES

In the realm of cryptography, Triple DES, short for Triple Data Encryption Algorithm (TDEA or Triple DEA), employs the Data Encryption Standard (DES) cipher algorithm thrice on each data block. Originally, the 56-bit key size of the DES cipher sufficed, but with advancing computational power, brute-force attacks became viable. To counter this, Triple DES offers a straightforward approach to augmenting DES's key size for enhanced security, obviating the need for an entirely new block cipher design. It utilizes a "key bundle" consisting of three 56-bit DES keys, denoted as K1, K2, and K3 (excluding parity bits).

V. RESULT ANALYSIS

A description of the process used to assess the current method is given. A bit-mapped (bmp) image with 256 colors and a dimension of 300 pixels by 300 pixels was used to test the technique. Three distinct scenarios were explored to assess how the number of blocks affected the correlation and entropy. Table I displays the number of blocks and the sizes of the blocks for each example. The results of each example are as follows: (a) a ciphered image created with the Blowfish algorithm; (b) a modified picture created with the proposed algorithm; and (c) a ciphered image created with

the proposed algorithm and the Blowfish algorithm combined. The original image, the ciphered image using the Blowfish algorithm, the converted image, and the ciphered image using the proposed algorithm followed by the Blowfish algorithm are all denoted by the images A, B, C, and D throughout the rest of this study. Together with SVM, the corresponding algorithm using RDH and 3DES offers the highest accuracy leading to poor accuracy. The outcome of using the suggested algorithm on the original image's various block sizes. Each one's correlation and entropy were compared using just the matching method. The experiment's outcomes are displayed. A straightforward and robust approach to picture security has been put forth that combines block-based image processing with encryption methods. The cases demonstrated that applying the suggested technique before the Blowfish approach reduced the correlation. The suggested technique's experimental results demonstrated a direct relationship between entropy and the number of blocks and an inverse relationship between the number of blocks and correlation. The suggested approach performed the best when compared to other well-used algorithms, yielding the lowest correlation and the highest entropy.

ALGORITHM ACCURACY

ALGORITHM	ACCURACY
DH with Triple DES	97
SVM	78
ANN	66

Table.1 Different Cases to Test the Impact of the Number of Blocks on the Correlation and Entropy

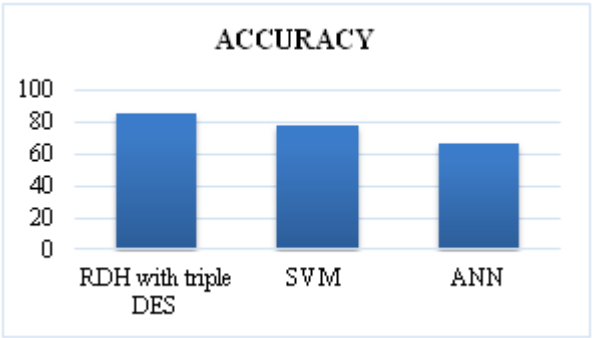


Figure 1. Comparison graph

VI. CONCLUSION

In summary, the paper introduces an innovative image encryption algorithm that combines reversible data hiding (RDH) with a triple DES block-based transformation. This novel approach ensures the protection of image content while still enabling seamless content-based image retrieval (CBIR) and direct image convolution. This algorithm caters to applications where both security and image processing are paramount. While the algorithm is relatively new and awaits comprehensive real-world testing, the initial findings presented in the paper are promising. Furthermore, its compatibility with CBIR and image convolution sets it apart from other encryption methods that often compromise image quality and hinder image processing capabilities.

VII. FUTURE WORK

To ensure the robustness and applicability of the proposed algorithm, it is imperative to conduct a comprehensive evaluation of a larger and more diverse dataset of images. While the algorithm has undergone testing on various image types in the paper, extending its assessment to encompass a broader spectrum of images will validate its versatility and effectiveness across different characteristics. Furthermore, the practical utility of this algorithm extends to real-world applications, including safeguarding sensitive medical and satellite imagery, as well as enhancing the security of consumer photographs. Therefore, implementing and rigorously evaluating the algorithm within these real-world contexts is essential to gauge its performance and usability, thereby validating its potential impact and relevance.

REFERENCES

[1] Chen, H. Li, Y., and Wang, C. (2017) ‘A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation’, Opt. Lasers Eng., vol. 90, pp. 238–246.

[2] M. Al-Sarem, W. Boulila, M. Al-Harby, J. Qadir, and A. Alsaeedi, "Profound learning-put together gossip recognition concerning microblogging stages: A precise survey," IEEE Access, vol. 7, pp. 152788-152812, 2019.

[3] M. S. Anwar, J. Wang, W. Khan, A. Ullah, S. Ahmad, and Z. Fei, "Subjective QoE of 360-degree augmented reality recordings and AI expectations," IEEE Access, vol. 8, pp. 148084-148099, 2020.

[4] Liu, B. Liu, J. Liu, J. Ma, J. Tong, X. J. Wang, Z. Zhang, M. (2020) ‘Image compression and encryption scheme based on compressive sensing and Fourier transform’, IEEE Access, vol. 8, pp. 40838–40849.

[5] A. Roy, A. P. Misra, and S. Banerjee, "Turmoil-based picture encryption utilizing vertical-hole surface-producing lasers," Optik, vol. 176, pp. 119-131, Jan. 2019.

[6] Lei, Y. Liu, L. and Wang, D. (2020) ‘A fast chaotic image encryption scheme with simultaneous

permutation-diffusion operation', IEEE Access, vol. 8, pp. 27361–27374.

[7] Chen, Y. Coatrieux, G. Ge, R. Luo, L. and Wu, J. (2019) 'A novel chaos-based symmetric image encryption using the bit-pair level process', IEEE Access, vol. 7, pp. 99470–99480.

[8] vchen cao, junxiu liu, xue ouyang, and Yuling luo, (2019) 'An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems', IEEE Access, Digital Object Identifier 10.1109/ACCESS.2019.2906052.

[9] 9. Ahmad, J. Arshad, Boulila, W. Buchanan, W. J. Khan, F. Masood, F. Rubaiee, S. and Qayyum, A. (2020) 'Chaos-based confusion and diffusion of image pixels using dynamic substitution', IEEE Access, vol. 8, pp. 140876–140895.

[10] S. B. Atitallah, M. Driss, W. Boulila, and H. B. Ghézala, "Utilizing profound learning and IoT huge information examination to help the savvy urban areas advancement: Survey and future headings," Comput. Sci. Fire up., vol. 38, Nov. 2020, Workmanship. no. 100303.

[11] T. B. Dijkhuis, F. J. Blaauw, M. W. van Ittersum, H. Velthuijsen, and M. Aiello, "Customized actual work instructing: An AI approach," Sensors, vol. 18, no. 2, p. 623, Feb. 2018.

[12] Hua, Z. Huang, H. and Zhou, Y. (2019) 'Cosine-transform-based chaotic system for image encryption', Inf. Sci., vol. 480, pp. 403–419.