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, Erode Sengunthar Engineering College (Autonomous) Thudupathi, Erode, Tamilnadu, India.

[2, 3, 4] Final Year, Department of Computer Science and Engineering, 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. This paper is a survey of Detecting the Strength of Security in Cryptosystems using RDH and CBIR.

Keywords: deployment models, infrastructure as a service, cryptosystems, machine learning.

1. Introduction

In the field of information technology, the phrase "cloud computing" has recently become popular. A true picture of the future of computing, both from a technical and societal perspective, may be found behind this flowery word. Even though the phrase "Cloud Computing" is relatively new, consolidating computing and storage in dispersed data centers run by outside corporations is not. It was first introduced in the 1990s along with other distributed computing techniques like grid computing. With a utility computing paradigm, cloud computing aims to deliver IT as a service to cloud customers on demand with more flexibility, availability, dependability, and scalability.

1.1 Deployment Models

The four different types of access to the cloud deployment models are defined as Private, Public, Hybrid, and Community. The public can readily access systems and services thanks to the public cloud. Due to its openness, such as email, public clouds can be less secure.

Access to systems and services within a company is made possible via the private cloud. Because of its private nature, it provides a higher level of security. Groups of organizations can access the system and services thanks to the community cloud. Public and private clouds are combined to create the hybrid cloud. However, the non-essential tasks are completed using the public cloud while the critical tasks are completed utilizing the private cloud.

1.2 Infrastructure As A Service

Access to basic resources like virtual machines, physical machines, virtual storage, etc. is made available through IaaS. A third-party supplier such as hosts hardware, software, servers, storage, and other infrastructure parts on behalf of its customers in the IaaS model. IaaS providers take care of things like system upkeep, backup, and resilience planning in addition to hosting users' apps. Platforms for IaaS provide highly scalable resources that can be changed as needed. IaaS is thus well suited for workloads that are ad hoc, experimental, or subject to sudden change. IaaS setups also provide dynamic scaling, desktop virtualization, automation of administrative activities, and policy-based services.

1.3 Cryptosystems

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 used. A crucial area of research and analysis in the realm of cyber security is the study of cryptosystems and their security levels, as the digital landscape changes and security threats become more sophisticated.

1.4 Machine Learning

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 a variety of 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 3 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.

1.5 Integration of RDH and Triple DES

Encryption with Triple DES: Initially, the sensitive data is encrypted using Triple DES to ensure confidentiality. Triple DES applies multiple rounds of encryption using a symmetric key.

Embedding Data with RDH: After encryption, the encrypted data can undergo reversible data hiding using RDH techniques. RDH methods embed additional data (such as a watermark or additional information) into the encrypted data in such a way that the original encrypted data can be accurately recovered after extraction of the embedded data.

Transmission or Storage: The data, now with embedded additional information, can be transmitted or stored securely. This additional information can serve various purposes such as authentication, integrity verification, or copyright protection, depending on the application.

Data Extraction and Decryption: Upon receiving or retrieving the data, the embedded additional information is extracted using RDH techniques. Then, the Triple DES decryption process is applied to recover the original sensitive data.

1.6 Objective

- Develop a robust CBIR system using RDH with Triple DES, integrating advanced visual content analysis for accurate image representation.
- Optimize and evaluate the CBIR system's performance, focusing on efficiency and scalability in handling large image databases.
- Introduce a novel steganography approach through reversible texture synthesis, ensuring secure information hiding with visually imperceptible changes.
- Implement and refine a texture synthesis process to create new textures with arbitrary sizes while maintaining local appearance similarities for effective steganography concealment.

2. Related Study

The rapid urban population [1] growth worldwide poses numerous challenges, such as environmental pollution, public safety, and

traffic congestion. To address these issues, smart cities are leveraging emerging technologies like the Internet of Things (IoT) to innovate intelligent services across various sectors, including healthcare, surveillance, and agriculture. IoT devices and sensors collect vast amounts of data, which can be harnessed for valuable insights. Deep Learning (DL), a subset of Artificial Intelligence (AI), has shown promise in enhancing IoT big data analytics efficiency and performance. This survey offers a comprehensive review of the literature on the integration of IoT and DL in the development of smart cities. It begins by defining IoT and outlining the characteristics of IoT-generated big data. The survey also covers different computing infrastructures, including cloud, fog, and edge computing, utilized for IoT big data analytics. Furthermore, it explores popular DL models and recent research that combines IoT and DL to create intelligent applications and services for smart urban environments. Finally, the survey highlights the current challenges and issues encountered in the advancement of smart city services.

The surge in the social network's [2] popularity has led to an alarming increase in the dissemination of unverified rumors, posing significant threats. Recent research efforts have delved into leveraging deep learning techniques to automatically tackle online rumors by mining vast textual data from the open network. In this comprehensive literature review, we meticulously sourced and examined 108 studies from prominent databases such as IEEE Explore, Springer Link, Science Direct, ACM Digital Library, and Google Scholar. Our review rigorously addresses seven key research questions, shedding light on prevailing trends in employing deep learning methodologies for rumor detection. Furthermore, we expound on the challenges encountered by researchers in this domain and propose promising avenues for future investigations. This review serves as a valuable resource for researchers, offering a comprehensive repository of performance metrics, dataset characteristics, and deep learning models employed in each study. It also facilitates the identification of annotated datasets suitable for benchmarking new approaches against state-of-the-art works, aiding researchers in advancing this field.

The 360-degree video gives [3] a vivid encounter to end-clients through Augmented Simulation (VR) Head-Mounted-Presentations (HMDs). Be that as it may, it isn't trifling to grasp the Nature of Involvement (QoE) of 360-degree video since client experience is impacted by different variables that influence QoE when watching the 360-degree video in VR. This composition presents the AI-based QoE expectation of 360-degree video in VR, taking into account the two key QoE angles: perceptual quality and cybersickness. Likewise, we proposed two new QoE-influencing factors: the client's knowledge of VR and the client's

advantage in 360-degree video for the QoE assessment. To point out this, we first led an emotional trial on 96 video Tests and gathered datasets from 29 clients for perceptual quality and cybersickness. The forecast exactness of the proposed model is looked at against notable regulated AI calculations for example, k-Closest Neighbor's (kNN), Backing Vector Machine (SVM), and Choice Tree (DT) with deference to exactness rate, review, f1-score, accuracy, and mean outright mistake (MAE). LR performs well with 86% exactness, which is in close concurrence with emotional assessment. The proposed model performs well against the best-in-class QoE expectation strategies regarding cybersickness.

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).

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 5 VCSELs. These VCSELs demonstrate hyper-chaotic behavior and exhibit a high degree of synchronization in their emission characteristics. The coupled VCSELs are then used as a transmitter and a receiver for the communication of images or data. Furthermore, it proposes a modified chaos-based image encryption algorithm using bit-level permutations and pixel-level which provides faster, robust, and simpler encryption or decryption compared to other chaos-based cryptosystems.

3. 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, it proposed a security-level detection approach for the image encryption algorithms using a support vector machine (SVM). Additionally, it has created a dataset incorporating standard encryption security parameters, such as contrast, homogeneity, entropy, peak signal-to-noise ratio, energy, mean square error, and correlation, extracted from the different cipher images. These parameters serve as features, and the dataset is categorized into three security levels: strong, acceptable, and weak.

3.1 Disadvantage

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 accurately predict the security level of new algorithms. 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.

4. Proposed System

The proposed system for Content-Based Image Retrieval (CBIR) integrates Reversible Data Hiding (RDH) using the Triple DES algorithm to represent and index visual image content attributes such as color, shape, texture, and spatial arrangement. 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.

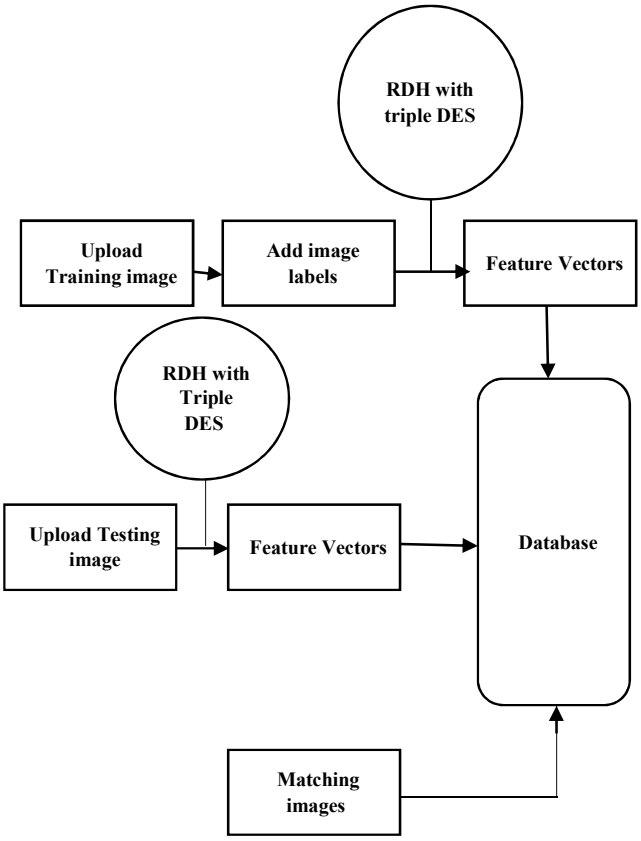

Figure. 1. Block diagram

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.

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).

5. Discussion

Using true random number keys from environmental noise ensures a high level of unpredictability, enhancing security by making it challenging for attackers to decipher encrypted images. Integrating chaotic systems into the encryption process adds another layer of complexity, making decryption even more difficult. This approach is well-suited for safeguarding sensitive color image data, like medical images or confidential documents, and ensuring data privacy and confidentiality in secure communications. Overall, it combines randomness and complexity to create robust encryption suitable for protecting valuable information.

6. 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.

7. 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] 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 0 20 40 60 80 100 RDH with triple DES SVM ANN ACCURACY 9 headings," Comput. Sci. Fire up., vol. 38, Nov. 2020, Workmanship. no. 100303.

[2] M. Al-Sarem, W. Boulila, M. Al-Harby, J. Qadir, and A. Alsaeedi, "Profound learning-put together gossip recognition to 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] 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.

[5] 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.