International Scientific Journal of Engineering and Management
Volume: 03 Issue: 04 | April – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

DETECTING THE SECURITY LEVEL OF VARIOUS CRYPTOSYSTEMS USING MACHINE LEARNING MODELS

Dr. N.Saranya[1], Abinaya C[2], Hemaa Mathiyarasu[3], and Shrijaa A[4]

[1]Assistant Professor (Sl.G), Department of Artificial Intelligence and Data Science, KPRInstitute of Engineering and Technology, e-mail: saranya.n@kpriet.ac.in

[2]Department of Artificial Intelligence and Data Science, KPR Institute of Engineering andTechnology, e-mail: abiiabi2003@gmail.com

[3] Department of Artificial Intelligence and Data Science, KPR Institute of Engineering andTechnology, e-mail: hemaamathiyarasu@gmail.com

[4]Department of Artificial Intelligence and Data Science, KPR Institute of Engineering andTechnology, e-mail: a.shrijaa@gmail.com

ABSTRACT

In contemporary data management, cloud storage is widely adopted, yet it remains susceptible to security vulnerabilities. Utilizing cryptography techniques is essential for enhancing data security in such environments. One promising approach is hybrid cryptography, which combines multiple algorithms to bolster protection. Our proposed solution integrates RDH with DES algorithms, leveraging their respective strengths to fortify data security before it's stored in the cloud. Extensive testing has validated the efficacy of this approach. Specifically, we introduce an RDH with DES block-based transformation algorithm tailored for image content protection. Notably, our framework enables direct image retrieval and convolution on the content-protected images, enhancing usability alongside security.

Keywords: deployment models, Infrastructure as a service, cryptosystems, machine learning

1. INTRODUCTION

The term "cloud computing" has gained prominence in the IT field, offering a glimpse into the future of computing from both technical and societal perspectives. While the term itself is relatively recent, the concept of centralizing compute and storage in remote data centres managed by external entities dates back to the 1990s, alongside other distributed computing models like grid computing. Cloud computing operates on a utility computing paradigm, providing IT services to customers on-demand with increased flexibility, availability, dependability, and scalability.

1.1 Deployment Models

Cloud deployment models encompass Public, Private, Hybrid, and Community types of access. Public shadows offer fluently accessible systems and services but may pose security pitfalls due to their openness. Private shadows, accessible only within a company, give enhanced security. Community shadows enable groups of associations to pierce participated systems and services. mongrel shadows combine public and private shadows, with unnecessary tasks handled by the public pall and critical tasks managed through the private cloud.

1.2 Infrastructure As A Service (Iaas)

INFRASTRUCTURE AS A SERVICE(IaaS) structure as a Service (IaaS) offers access to essential coffers similar as physical and virtual machines, as well as virtual storehouse, through a cloud calculating model. In this setup, a third-party provider hosts tackle, software, waiters, and storehouse factors on behalf of guests.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

This relieves associations of the burden of managing their own structure and allows them to concentrate on their operations and services. Providers of IaaS handle tasks similar as system keep, backup, and adaptability planning, thereby icing the trust ability and vacuity of the structure. also, they offer largely scalable coffers that can be acclimated grounded on demand, making IaaS suitable for workloads that are ad hoc, experimental, or subject to unforeseen changes in resource conditions. crucial features of IaaS include dynamic scaling, which enables coffers to be provisioned order-provisioned automatically in response to changes in demand. This scalability ensures optimal resource application and cost effectiveness. also, IaaS platforms support desktop virtualization, allowing druggies to pierce virtual desktop surroundings from anywhere with an internet connection. robotization of executive conditioning is another benefit of IaaS, streamlining repetitious tasks and perfecting functional effectiveness. also, IaaS providers offer policy- grounded services, enabling associations to define and apply rules for resource allocation, security, and access control. Overall, IaaS provides associations with the inflexibility, scalability, and cost- effectiveness demanded to efficiently manage their IT structure. It's a precious result for businesses seeking to acclimatize to changing conditions and influence the benefits of cloud computing.

1.3 Cryptosystems

Modern information security heavily relies on cryptosystems, pivotal for securing data transmission and storage. A cryptosystem encompasses cryptographic protocols and algorithms designed to authenticate, maintain confidentiality, and decrypt sensitive data during communication. These systems find application in diverse domains including government communication, military operations, data storage, and online transactions. Cryptosystems utilize complex mathematical formulas to convert plaintext into ciphertext, thwarting unauthorized decryption attempts. The strength and effectiveness of a cryptosystem are influenced by factors such as security procedures, key lengths, and encryption algorithms employed. Research and analysis in cybersecurity focus significantly on cryptosystems and their security levels, crucial for adapting to evolving digital landscapes and sophisticated security threats.

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 a wide range of 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.

2. LITERATURE REVIEW

The rapid growth of urban populations globally presents 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 develop intelligent services across various sectors such as agriculture, healthcare, and surveillance. A wealth of data is gathered by IoT devices and sensors, and this data can be analyzed to reveal insightful information. An area of artificial intelligence called deep learning (DL) has showed promise in improving the performance and IoT big data analytics efficiency. This evaluation defines IoT, outlines the characteristics of big data produced by IoT, and covers various computing infrastructures in addition to reviewing the literature on the combination of IoT and DL for the development of smart cities. Cloud, fog, and edge computing are used in IoT big data analytics. To generate intelligent applications and services for smart urban environments, it also examines current research combining IoT and DL, as well as popular DL models.

The proliferation of social networks has led to a surge in unverified rumours, posing significant threats. Recent research focuses on using deep learning techniques to automatically address online rumours by mining textual data from open networks. This literature review examines 108 studies, highlighting trends in employing deep learning for rumour detection. It discusses challenges faced by researchers and suggests future research directions, serving as a valuable resource for researchers. It is difficult to evaluate the virtual reality 360-degree video's

ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

Quality of Experience (QoE) (VR) because there are many variables that can affect QoE. An AI-based QoE prediction model that takes cyber illness and perceptual quality into account is presented in this research., along with the user's VR experience and interest in 360-degree media are new aspects that impact QoE. In order to propose a new Linear Regression (LR) based model for QoE prediction related perceptual quality and compare it with supervised AI algorithms, emotional trials on 96 video samples and data from 29 users are gathered.

Hanze University implements a health promotion program using activity trackers to monitor daily step counts among employees. This study explores automating aspects of coaching by providing personalized, real-time feedback on participants' progress towards daily step goals. Data from step counts is used to train eight machine learning algorithms, with the Random Forest algorithm emerging as the most effective.

Finally, this work investigates the encryption and decryption of color images using polarization dynamics in vertical-cavity surface-emitting lasers (VCSELs), which have hyperchaotic behavior and highly synchronized emission features.

3. EXISTING SYSTEM

Recent advancements in multimedia technologies have heightened concerns about digital data security, leading researchers to investigate changing current security procedures. However, it has come to light that many of the encryption algorithms created in the last few decades are insecure, seriously endangering sensitive data. Selecting the right encryption technique is essential for protecting data, but weighing each one separately might take time. We provide a support vector machine (SVM)-based security level detection method for picture encryption techniques to address this. We also present a dataset of standard encryption security parameters collected from different cipher pictures, such as energy, correlation, peak signal-to-noise ratio, mean square error, contrast, entropy, and homogeneity. The dataset is divided into three security levels: strong, acceptable, and poor, and these parameters act as features.

4. PROPOSED SYSTEM

Reversible Data Hiding is incorporated into the proposed Content-Based Image Retrieval (CBIR) system (RDH) with the DES algorithm to represent and index visual image attributes such as colour, shape, texture, and spatial arrangement. Current CBIR research emphasizes refining methodologies for image database analysis, interpretation, cataloguing, and indexing, along with evaluating retrieval system performance. This project introduces a novel steganography approach through reversible texture synthesis. Small texture images, whether artistically crafted or photographically captured, are resampled to generate new textures of varying sizes. This process utilizes 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, feature vectors are extracted from input images and stored within the dataset alongside their corresponding images. Moving to the second module, the query module, an image is inputted, and its feature vector is extracted. Finally, in the retrieval process, the feature vector of the query image is compared with those stored in the dataset. These feature vectors typically encompass essential aspects such as texture, colour, local shape, and spatial information. The increasing need for efficiently searching image datasets of expanding sizes has driven the widespread adoption 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

International Scientific Journal of Engineering and Management
Volume: 03 Issue: 04 | April – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

to geometric variations, partial resistance to lighting changes, and resilience to geometric deformations, enhances their utility in addressing these intricate challenges in shape analysis.

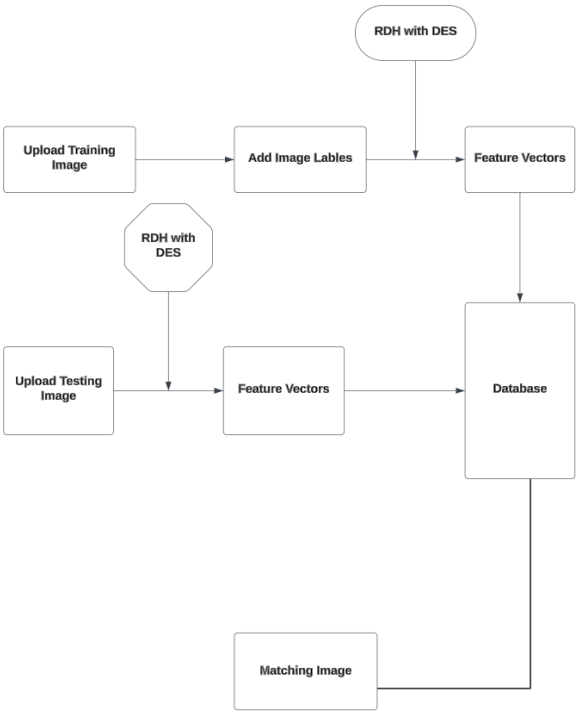

Fig. 1 Block Daigram

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 in relation to the current working location.

4.4 DES

In the realm of cryptography, DES, short for Data Encryption Algorithm (TDEA or 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, 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. ALGORITHM DETAILS

A. Reversible Data Hiding

ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

Essential data can be embedded into a variety of media, including music, video, and graphics, using a technique called reversible data hiding. This system employs a method of reserving space before encryption to hide data within the image or video, thereby increasing the amount of hidden data while ensuring lossless recovery after extraction. This system presents a new technique called Reserving Room Before Encryption (RRBE), which is different from earlier approaches where room for data hiding was allotted after encrypting the image, potentially generating mistakes during data extraction and image recovery. RRBE utilizes visual cryptography to reserve space in images and videos before encryption, ensuring error-free extraction and recovery. This technique can also serve as a watermarking method to authenticate images and videos by embedding additional data.

B. Data encryption standard algorithm (des)

One type of symmetric block encryption is the DES algorithm that uses XOR, substitution, and permutation operations in an iterated fashion. These operations are repeated for 16 internal rounds, following the Feistel Cipher structure. XOR, expansion/permutation, and substitution operations are used with the round function F. The 64- bit ciphertext is created by combining the two 32-bit halves of the plaintext, L0 (left) and R0 (right), after they have been processed through 16 rounds.

Each round takes inputs Li-1 and Ri-1 from the previous round. Additionally, a key generation procedure is used for each round to generate a distinct 48-bit sub-key Ki from the 64-bit input key K.

6. RESULT ANALYSIS

A bitmapped (bmp) image with 256 colors and 300 by 300-pixel size was used in the assessment procedure to gauge the effectiveness of the method.

Three distinct scenarios were explored to assess how the number and sizes of blocks affected correlation and entropy. Table I illustrates the number and sizes of blocks for each scenario. The results of each scenario were as follows: (a) a ciphered image created with the Blowfish algorithm; (b) a modified picture created with the proposed algorithm; and (c) an image that has been encrypted using the suggested technique and the Blowfish algorithm. During the investigation, A, B, C, and D represented, in that order, the original image, the altered image, the Blowfish ciphered image, and the combined ciphered image. The highest accuracy was achieved when using SVM with the corresponding algorithm employing RDH and 3DES. Conversely, applying the suggested algorithm on different block sizes of the original image led to varying correlations and entropies, which were compared using the matching method. The experiment's outcomes demonstrated a straightforward and robust approach to picture security by integrating block-based image processing with encryption methods. Specifically, applying the suggested technique before the Blowfish approach resulted in reduced correlation.

ALGORITHM	ACCURACY
RDH with DES	97
SVM	78
ANN	66

Table.1 Various Examples to Evaluate the Effect of Block Count on Entropy and Correlation

ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

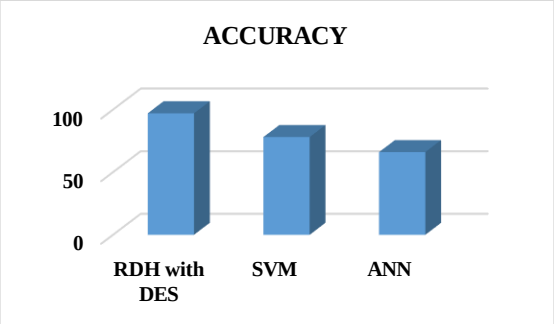

Figure 1.Comparison graph

7. CONCLUSION

In summary, the paper introduces an innovative image encryption algorithm that combines reversible data hiding (RDH) with a 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.

8. FUTURE WORK

To ensure the robustness and applicability of the proposed algorithm, it is imperative to conduct a comprehensive evaluation on 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.

9. REFERENCES

1. 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 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 with respect 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, "SubjectiveQoE 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. 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. P. R. Krishna, C. V. M. S. Teja, S. R. Devi, and V. Thanikaiselvan, "A chaos-based image encryption employing Tinkerbell map functions," in Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA), Mar. 2018,
pp. 578-582.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01475

7. R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo. "A novel chaos-based symmetric image encryption using bit-pair level process." IEEE Access, vol. 7, pp. 99470-99480, 2019.

8. Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel- and bit-level permutation," Opt. Lasers Eng., vol. 90, pp. 238-246, Mar. 2017.

9. Mohamed, ElKamchouchi, and Moussa, "A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences," Entropy, vol. 22, no. 2, p. 158, Jan. 2020.

10. Shafique, A. 'A novel algorithm for the creation of replacement box by employing chaotic map," Eur. Phys. J. Plus, vol. 135, no. 2, pp. 1-13, February 2020.