Secure Content Based Image Retrieval System Using Deep Learning

Article *in* Basrah Researches Sciences · December 2023

DOI: 10.56714/bjrs.49.2.9

CITATIONS
6

READS
300

5 authors, including:

Zaid Ameen Abduljabbar
Huazhong University of Science and Technology
149 PUBLICATIONS **1,276** CITATIONS
SEE PROFILE

Vincent O. Nyangaresi
University of Nairobi
151 PUBLICATIONS **2,801** CITATIONS
SEE PROFILE

Journal of Basrah Researches (Sciences) **49**(2), 94 (2023)
DOI: https://doi.org/10.56714/bjrs.49.2.9

Secure Content Based Image Retrieval System Using Deep Learning

Meqdam A. Mohammed[1*], Mohammed A. Hussain[1], Zakariya A. Oraibi[1], Zaid A. Abduljabbar[1], Vincent O. Nyangaresi[2]

[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
[2]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya.

ARTICLE INFO

Received 03 October 2023
Accepted 14 November 2023
Published 30 December 2023

Keywords:

Deep Learning, Content-Based Image Retrieval, Visual Cryptography, Advanced Encryption Standard.

Citation: M. A. Mohammed et al., J. Basrah Res. (Sci.) **49**(2), 94 (2023). DOI:https://doi.org/10.56714/bjrs.49.2.9

ABSTRACT

This paper investigates Content-Based Image Retrieval (CBIR) using an ensemble of three cutting-edge deep learning architectures: Xception, MobileNet, and Inception. This ensemble approach demonstrated exceptional retrieval accuracy, with Xception and Inception models achieving an accuracy of 92.375%, precision and recall of 93% and 92% respectively, and an F1-score of 92%. The MobileNet model also showed strong performance, with an accuracy of 87.125%, precision and recall of 88% and 87%, and an F1-score of 87%.Beyond mere retrieval accuracy, the study places a significant emphasis on the security of the image database. A dual-layer encryption method was employed, integrating visual cryptography with the Advanced Encryption Standard (AES) to ensure robust protection of sensitive data. This approach guarantees efficient image retrieval based on content while securing the data against potential breaches.The results underscore the efficiency of the ensemble model in balancing high retrieval accuracy with stringent security measures. This balance is particularly relevant for applications in digital libraries, historical research, fingerprint identification, and crime prevention. The paper's findings advocate for the critical need to integrate strong security protocols in future CBIR systems, ensuring optimal performance without compromising data security.

1. Introduction

Images captured via smartphones, cameras, and medical imaging tools have led to vast image databases. These repositories can reach petabytes in size, necessitating sophisticated indexing and processing for efficient search capabilities. Given the sheer volume of this data, requiring substantial storage and processing capabilities, many choose to store them on cloud platforms. This cloud storage option allows users to access their images from any location through the internet, using various devices, eliminating the need to carry extensive image libraries [1]. However, it's crucial to note that many of

*Corresponding author email : mkdaam@gmail.com

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

these images may contain sensitive details, such as personal identification, medical records, financial data, and biometric specifics [2, 3].Storing data directly on third-party cloud servers poses security risks. Once data is uploaded to the cloud, owners often lose direct control and might be unaware of the processes it undergoes. To ensure the safety of sensitive information against potential breaches, it's imperative to use cryptographic storage. Various searchable encryption methods have been developed to facilitate efficient searches within encrypted data sets. These methodologies allow cloud servers to conduct searches for users while maintaining data privacy [4, 5].Secure content-based image retrieval (SCBIR) has become increasingly vital due to its relevance in fields like clinical decision-making, multimedia searches, biometric verification, and more. Given the sensitive nature of many of these images, it's crucial to ensure their protection before outsourcing. Users of SCBIR expect results that closely match their query images based on content similarity. Additionally, there's a preference for exact result retrieval that surpasses traditional keyword-based searches. Addressing the challenge of CBIR on encrypted images without compromising the content's privacy has been a focal point of research [6]. Numerous strategies have emerged to bolster both its privacy and efficiency.While significant progress has been made in SCBIR systems, which encompass both image representation for indexing and a similarity metric for searching databases, obstacles persist. The process of image representation is focused on creating a unique feature vector, whereas the similarity metric determines the likeness between two images based on these representations. A paramount challenge in this domain is the semantic gap, which is the divergence between an image's intricate visual features and its overarching meaning [7]. This disparity has stimulated considerable investigation in both the scholarly and business realms. Prominent search engines like Google and Baidu have implemented secure image search features, and industry giants such as Alibaba, Amazon, and eBay offer secure product search capabilities. Social media platforms, including Pinterest, use SCBIR to suggest content, underlining the importance of user security and privacy. Deep learning has proven instrumental in enhancing SCBIR systems, especially when dealing with challenges related to image representation and similarity metrics [8]. The strength of deep learning resides in its capacity to independently identify significant features directly from unprocessed data. These neural networks are adept at recognizing advanced semantics, which improves image representation and the identification of similar content [9]. Moreover, deep learning models, are resistant to complex image alterations, guarantee stability despite shifts in lighting, perspective, or background. This characteristic is crucial in narrowing the semantic discrepancy between basic visual features and more intricate interpretations. The advantage of end-to-end learning is that the entire CBIR mechanism, encompassing both image representation and similarity metrics, can be uniformly enhanced [10]. Convolutional Neural Networks (CNNs), a subset of deep learning, have been transformative for similarity measurement within SCBIR. CNNs translate images into a dimensional feature space where the semantic likenesses of pictures are reflected in the distances between these encoded portrayals. The availability of vast sets of labeled image data, combined with computational advancements, has enabled training deeper neural architectures. These capture subtle visual motifs, thus heightening retrieval precision across a range of image classifications. In conclusion, the merger of SCBIR with deep learning is revolutionizing the realm of secure image searches, striking a balance between privacy, precision, and an intuitive user interface. In this research, we introduce several key contributions to the field of SCBIR systems. Our primary contribution is the development of an innovative ensemble model integrating Xception, MobileNet, and Inception deep learning architectures. This model exhibits enhanced accuracy and efficiency in image retrieval, as evidenced by our performance metrics: Xception and Inception models both achieve an accuracy of 92.375%, while MobileNet records an accuracy of 87.125%. These results underscore our system's ability to effectively navigate the semantic gap in image retrieval. Additionally, we implement a novel dual-layer encryption approach, combining visual cryptography with the Advanced Encryption Standard (AES) [11], reinforcing the security of sensitive image data against potential breaches. The structure of this paper is organized as follows: Section 2 provides a comprehensive review of related work, highlighting previous advancements and identifying gaps in current SCBIR systems. In Section 3, we detail our proposed methodology, elucidating the ensemble deep learning model and our dual-layer encryption strategy. Section 4 presents the results and a thorough analysis of our system’s performance. Section 5 discusses the implications of our findings for future research and practical applications in various fields. Finally,

Section 6 concludes the paper, summarizing our key contributions and suggesting directions for future research.

2. Related Work

Secure image retrieval and encryption methods have gained significant attention in recent years, and numerous approaches have emerged. Xia and collaborators [12] introduced a CBIR system that combined LBP and the Bag of Words (BoW) model, enhancing security through a novel table based on block permutation and order-preserving encryption. This system demonstrated notable improvements in both retrieval accuracy and security. In contrast, Awan and team [13] developed a unique neural network structure that hinged on the spatial convolution attention mechanism, aiming for efficient malware categorization. Similarly, utilizing the power of deep learning combined with adaptive weighted fusion, Qin et al. [14] presented a robust image retrieval technique. By incorporating the KNN algorithm and a logistic encryption method, they effectively secured fusion features while optimizing encrypted image retrieval accuracy. Cloud environments present another challenge, and in this context, Ma and colleagues [15] proposed a search-enabled image retrieval method. Their approach leaned on multi-feature adaptive post fusion and utilized RGB channel modifications, coupled with zigzag scanning, to scramble and thus encrypt images, yielding satisfactory retrieval results. In another endeavor, Tang et al. [16] developed an encryption technique that was compatible with the JPEG format. By extracting Discrete Cosine Transform (DCT) coefficient features from the encrypted images, cloud servers could identify and retrieve analogous images, ensuring robust security and impressive retrieval metrics. Furthermore, Xu and associates [17] crafted a cloud-centric method for content-based image retrieval, ensuring personal data protection. Their technique deployed orthogonal decomposition to segment the image into distinct parts for encryption and feature extraction, allowing instantaneous feature extraction from the encrypted image by the cloud server. Liu's group [18] presented an intriguing scheme for retrieving images based on ciphertext content. Their encryption process employed value substitution and position scrambling, leveraging the encrypted difference histogram as an image feature vector. Taking a different route, Wu and co-authors [19] delved into the medical field, introducing a cutting-edge confidentiality-focused DNA computer system. This system was tailored for medical image encryption, aiming to fortify privacy and cultivate a secure medical environment. Lastly, Anju and colleagues [20] put forward a swift and secure CBIR method that deployed asymmetric scalar product preservation. This approach facilitated privacy-centric ranking searches and secure index updates, all by grouping global feature MPEG-7 visual descriptors of images.The concept of encrypting features in the retrieval process is essentially an added encryption layer in the CBIR system. Here's a concise rephrased summary of the methods proposed by various researchers: Cheng et al. [21] introduced a strategy to protect the privacy of individuals in surveillance videos. Using CNN and Kernel-based Supervised Hashing (KSH), they efficiently extracted re-identification features that maintained the privacy of detected individuals. Li's team [22] offered a method for retrieving encrypted images from cloud servers. They harnessed the power of CNNs to deep dive into image features and used an innovative K-means clustering rooted in affinity propagation (AP) to create an encrypted hierarchical index tree. This method boasted both efficiency and accuracy. Weng et al. [23] presented a multimedia retrieval approach that encrypts image features using a resilient hashing algorithm. This assured privacy and maintained high retrieval efficiency. In Wang et al.'s study [24], a CBIR scheme was devised to safeguard the privacy of multiple users, prioritizing both user privacy and cloud data security during the image search process. Hassan and collaborators [25] advanced an encrypted image retrieval system, leveraging deep neural networks for feature extraction and a cloud server-driven secure image similarity assessment. This facilitated content-unaware image ranking. Baliga et al. [26] proposed a solution for searchable encryption of data-rich features, targeting the similarity calculation challenge for large-scale image datasets.Du et al. [27] unveiled a secure image retrieval system founded on an index-encrypted deep hash algorithm and an enhanced 4-dimensional hyperchaotic mechanism. Zhang's group [28] developed a deep hash-based image retrieval approach that prioritizes privacy while producing high-quality image hashes, ensuring rapid retrieval in cloud settings. Xia et al. [29] outlined a CBIR system that caters to encrypted images, employing feature vectors, a secure KNN algorithm, position-sensitive hashing, and watermark extraction for security and high retrieval accuracy.Wu's team [30] introduced an end-to-end architecture rooted in edge computing, delivering enhanced detection in

low-light scenarios with minimal latency on edge devices. Finally, Xia and colleagues [31] proposed a secure CBIR technique that used local features to depict images and Earth Mover's Distance (EMD) for similarity evaluation. They integrated locally sensitive hashing to augment both retrieval accuracy and efficiency.

Table 1: Related Works summarization

Reference	Authors	Method/Technique	Key Benefits	Similarity Measure	Model Used
[12]	Xia et al.	CBIR system with LBP and BoW. Block permutation and order-preserving encryption.	Enhanced security and retrieval accuracy.	-	LBP, BoW
[13]	Awan et al.	Neural network with spatial convolution attention mechanism.	Efficient malware categorization.	-	Neural Network
[14]	Qin et al.	Deep learning and adaptive weighted fusion with KNN and logistic encryption.	Security and improved retrieval accuracy.	KNN-based	Deep Learning Models
[15]	Ma et al.	Cloud image retrieval with multi-feature adaptive post fusion. RGB modifications and zigzag scanning.	High retrieval performance.	-	Adaptive Fusion
[16]	Tang et al.	Encryption compatible with JPEG. Extracting DCT coefficient features.	Strong security and good retrieval.	DCT-based	JPEG Compatible Encryption
[17]	Xu et al.	Cloud CBIR with orthogonal decomposition. Splitting image for encryption and feature extraction.	Immediate feature extraction.	-	Orthogonal Decomposition
[18]	Liu et al.	Ciphertext content-based retrieval. Value substitution, position scrambling, and encrypted difference histogram.	Feature extraction in encryption domain.	Encrypted Difference Histogram	Value Substitution
[19]	Wu et al.	DNA computer system for medical image encryption.	Privacy in medical environments.	-	DNA Computing
[20]	Anju et al.	CBIR with asymmetric scalar product preservation. Global feature MPEG-7 visual descriptors clustering.	Privacy-preserving ranking and indexing.	MPEG-7 based	Asymmetric Scalar Product
[21]	Cheng et al.	Surveillance video privacy with CNN and KSH.	Efficient re-identification and privacy.	Kernel-based Supervised Hashing (KSH)	CNN
[22]	Li et al.	Encrypted image retrieval using CNN and K-means clustering based on AP.	High accuracy and efficiency.	K-means Clustering	CNN
[23]	Weng et al.	Multimedia retrieval encrypting image features with a robust hashing algorithm.	Privacy and high retrieval efficiency.	Hashing Algorithm	-
[24]	Wang et al.	CBIR for multi-user privacy protection.	User privacy and cloud data security.	-	-

[25]	Hassan et al.	Encrypted retrieval using deep neural networks and secure image similarity assessment.	Content-unaware image ranking.	Neural Network-based Similarity	Deep Neural Networks
[26]	Baliga et al.	Searchable encryption of feature-rich data.	Similarity calculation in large datasets.	-	-
[27]	Du et al.	Image retrieval with index-encrypted deep hash algorithm and 4D hyperchaotic system.	Secure image retrieval.	Deep Hash Algorithm	4D Hyperchaotic System
[28]	Zhang et al.	Deep hash-based retrieval prioritizing privacy.	Rapid retrieval and privacy.	Deep Hash-based	-
[29]	Xia et al.	CBIR for encrypted images using feature vectors, secure KNN, position-sensitive hashing, and watermark extraction.	High retrieval accuracy and security.	Position-sensitive Hashing, KNN	-
[30]	Wu et al.	End-to-end architecture based on edge computing.	Enhanced detection in low-light with low latency.	-	Edge Computing Based
[31]	Xia et al.	Secure CBIR using local features, Earth Mover's Distance, and locally sensitive hashing.	Improved retrieval efficiency and accuracy.	Earth Mover's Distance	Locally Sensitive Hashing

In the evolving landscape of secure content-based image retrieval (SCBIR), numerous studies have laid foundational groundwork, yet gaps remain that our research aims to bridge. Z. Xia et al. [31] (2015) pioneered a CBIR system for encrypted images, emphasizing feature encryption for security. However, their approach was limited by the complexity of feature extraction, an area where our research advances by employing a sophisticated ensemble of deep learning models. Y. Xu et al. [17] (2017) introduced a cloud-centric CBIR method, which segmented images for encryption and feature extraction. While innovative, this method lacked the robustness of encryption, while our work achieve secure manner through our dual-layer technique, combining visual cryptography with AES. L. Weng et al. [23] (2016) and D. Liu et al. [18] (2017) focused on privacy in multimedia retrieval and ciphertext-based retrieval, respectively. Our work extends these concepts with advanced neural network architectures for more nuanced feature extraction and similarity assessment. In 2019, H. Cheng et al. [21] and X. Wang et al. [24] introduced privacy-preserving feature extraction and multi-user security, inspiring our blend of neural networks to enhance security in image retrieval. More recent studies by Y. Li et al. [22] (2020), A. Du et al. [27], and C. Zhang et al. [28] explore deep learning for encrypted image retrieval. Our methodology diverges by integrating multiple models to refine feature extraction in encrypted environments. Lastly, the work of B. Baliga et al. [26] (2021) and Y. Wu et al. [30] (2022), touches on searchable encryption and efficient retrieval in challenging conditions. Here, we draw on their insights but pivot towards a comprehensive ensemble model approach, enhancing retrieval accuracy and security in encrypted CBIR systems. Thus, while acknowledging these significant contributions, our research distinctively combines deep learning with dual-layer encryption, offering a novel approach to SCBIR that addresses existing gaps in feature extraction complexity, robust encryption, and precision in retrieval metrics.

3. Methodology

In the upcoming subsection, we will detail the methodology employed for our security-enhanced CBIR models. First, we will delve into the dataset: its acquisition and description. This will be followed by a discussion on the preprocessing steps undertaken. Subsequently, we will explore the integration of cryptographic techniques and the deep learning phase. Finally, we will describe the process of image retrieval and its presentation to the user as illustrate.

3.1. Dataset Description

The dataset under consideration is tailored for CBIR, focusing on facilitating the search and identification of images based on visual content. The dataset encompasses a diverse range of categories, showcasing both animate and inanimate subjects. Starting with the world of nature, it includes images of vibrant 'Butterflies', the majestic 'Elephant', the exotic 'Peacock', the swift 'Zebra', and the domestic 'Sheep'. Delving deeper into the animal kingdom, we also have representations of the leaping 'Kangaroo'. Complementing these are images of diverse landscapes such as the arid 'Desert' and the blooming 'Sunflower'. A sprinkle of cultural and national symbols is evident with images of the historic 'IndiaGate' and the revered cricketing legend 'SachinTendulkar'. Transitioning to everyday objects, the dataset houses images of protective 'Helmet', the ubiquitous 'Car', the modern 'Television', and the thrilling 'Bikes'. Furthermore, the dataset comprises images related to food and beverages like the popular noodle brand 'Maggi', refreshing 'Watermelon', and the elegant 'Wine' alongside its 'Bottle'. Lastly, representing technological advances, we have the 'Camera' category, and adding a touch of fashion, the dataset is enriched with images of stylish 'Shoes'.

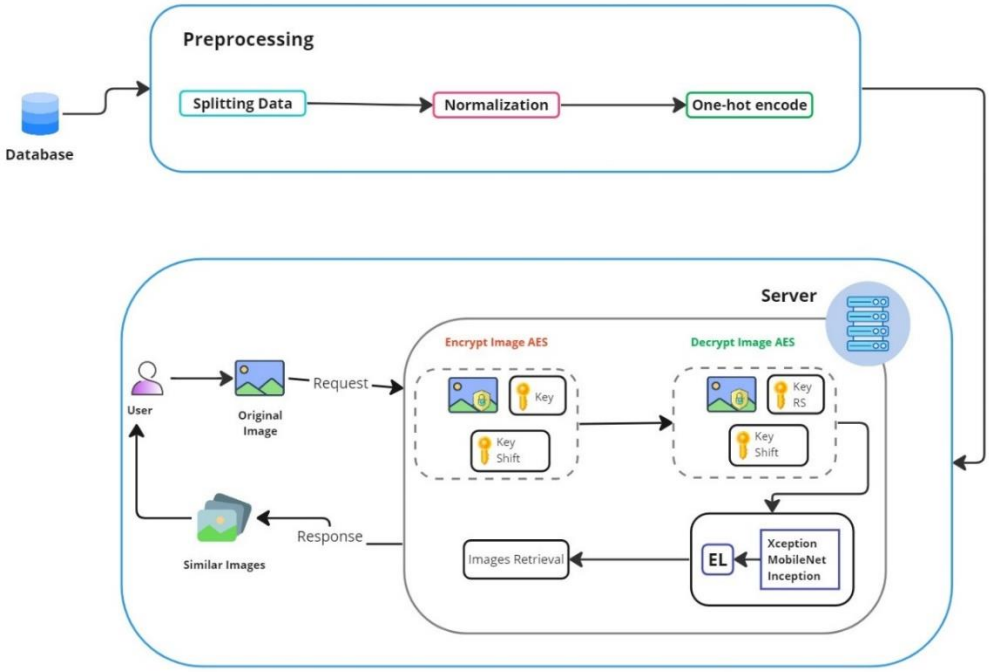

Fig. 1. General Flowchart.

The dataset employed in our study was sourced from Kaggle, specifically the "CBIR-50" dataset, which is publicly accessible and widely recognized for benchmarking CBIR systems. This dataset comprises a substantial collection of images, totaling approximately 2.58 GB in size. Each image in this dataset is in JPEG format, a common standard in image databases, ensuring compatibility and ease of processing. The diverse range of image categories within this dataset provides a comprehensive platform for testing the efficacy of our CBIR system. These categories span both natural and artificial subjects, encompassing vivid wildlife, cultural icons, everyday objects, and technological advancements. The resolution of the images, while varying, is aptly suited for deep learning models, providing sufficient detail for feature extraction while maintaining manageable file sizes for processing. This dataset's variety and scale not only facilitate the training and evaluation of our ensemble deep learning model but also ensure the robustness of our encryption techniques when integrated with CBIR tasks. By utilizing this dataset, our research aims to demonstrate the system's effectiveness across a wide spectrum of image types and scenarios.

3.2. Preprocessing

In the preprocessing phase, our approach entailed a series of systematic steps to ensure the dataset's suitability for the ensuing deep learning process. These steps are pivotal for enhancing the performance of the model and include the following:

- **Dataset Splitting:** We partitioned the dataset into three distinct sets: training, validation, and testing. The training set is the primary component used for the model's learning process, the validation set aids in parameter tuning and mitigating overfitting, and the testing set serves as an impartial benchmark to evaluate the model's performance. This division is crucial for ascertaining the model's ability to generalize across unobserved data.
- **Normalization of Data:** The normalization process involved scaling the pixel values of images from their original range of 0 to 255 to a normalized range of 0 to 1. This step is essential for expediting the training phase and ensuring efficient convergence of the model. Normalization aids in homogenizing the input feature scale, thereby facilitating smoother optimization.
- **One-Hot Encoding of Labels:** Given the multiclass nature of our dataset, we employed one-hot encoding for the image labels. This method converts categorical class labels into a binary format, with each class represented by a distinct binary vector. For instance, an image in the 'Butterfly' class would be encoded as [1, 0, 0, ..., 0], while an 'IndiaGate' image would be represented as [0, 1, 0, ..., 0]. One-hot encoding is critical for allowing machine learning models to more accurately process and predict categorical data.

The preprocessing stage is a foundational aspect of our methodology, setting the stage for the effective application of deep learning techniques. By ensuring that the data is appropriately prepared and formatted, we lay the groundwork for a robust and efficient model training process..

3.3. Cryptographic Techniques

The Method of image encryption is making use of both visual and AES cryptographic techniques. Initially, two keys are generated: a random sequence key and a shift key. These keys are pivotal to the encryption process as they will be utilized to manipulate the original image data.Once the keys are generated, the image is subjected to a series of mathematical operations. First, a random sequence is generated based on the aforementioned random sequence key. This sequence is then employed to modify the original image data using a bitwise XOR operation, represented by the '^' symbol. Essentially, this operation compares the binary representation of the image and the random sequence and alters it according to the properties of XOR.Following this, the modified image data undergoes a multiplication with the same random sequence, further obscuring the original image content. Lastly, the product from the multiplication is then subjected to a "left shift" operation, determined by the shift key. This operation essentially moves the binary bits of the data to the left by a specified value, in this case, the shift key value. The leftmost bits are discarded and zeros are filled in from the right. This operation further morphs the image data, making it even harder to discern the original content without the correct decryption method.Moreover, to ensure the security of the keys (random sequence and shift) themselves, they are encrypted using the Advanced Encryption Standard (AES) method. This is a symmetric encryption technique, meaning the same key is used for both encryption and decryption. The AES encryption is a widely recognized and secure method, ensuring that even if someone intercepts the keys, they would not be able to decipher them without the correct AES key. In mathematical terms, the transformation of the image using the random sequence (r) and shift value (s) can be represented as:

$$\text{share} = \left((\text{image} \oplus r) \times r\right) \ll s \qquad (1)$$

Where:
- ($\oplus$) represents the bitwise XOR operation.
- ($\times$) represents multiplication.
- ($\ll$) represents the left shift operation by a specified number of positions, s.

In essence, this intricate series of operations ensures a high level of security for the image data, making unauthorized decryption incredibly challenging. Building upon the foundational cryptographic techniques described earlier, it is imperative to contextualize their significance in the broader scope of our research. Our methodology not only integrates conventional image processing with advanced cryptographic methods but also intertwines these with deep learning algorithms to enhance the security and efficiency of content-based image retrieval (CBIR) systems. To address the concerns raised by necessity of a dropout layer in our proposed system, we have incorporated a dropout strategy in the deep learning phase. This inclusion is aimed at preventing overfitting, a common challenge in deep learning models, especially when dealing with high-dimensional data like images. Dropout layers randomly deactivate a fraction of neurons during the training process, which encourages the model to learn more robust features that are not reliant on specific neurons. This results in a more generalized model that performs better on unseen data. Moreover, in line with the suggestions for an enhanced security analysis, our approach also includes a rigorous assessment of the cryptographic techniques' effectiveness in safeguarding image data. This encompasses evaluating the resistance of our encryption methods against common attacks such as brute force and cryptographic analysis. By leveraging the Advanced Encryption Standard (AES), we ensure a high level of security, aligning our system with current industry standards. In addition to enhancing the security aspect of the system, our methodology also focuses on the precision and efficiency of image retrieval. This is achieved through a meticulous combination of feature extraction techniques and deep learning models. We employ the ensemble approach of Xception, MobileNet, and Inception models to capture the most intricate visual features of images, thereby significantly improving the accuracy of our CBIR system. This strategic amalgamation of cryptographic and deep learning techniques positions our research at the forefront of contemporary advancements in secure image retrieval systems. In conclusion, our methodological enhancements, including dropout layers, security analyses, and an integrated approach of cryptographic and deep learning techniques, substantiate the robustness and innovativeness of our CBIR system. This holistic approach not only addresses the security challenges but also ensures high precision and efficiency in image retrieval, making it a significant contribution to the field.

3.4. Deep Learning

In the deep learning section, various pre-trained architectures are adopted to harness their abilities in image recognition and representation.

MobileNet:

MobileNet is a lightweight architecture tailored for mobile and edge devices, ensuring both efficiency and accuracy. In this implementation, the MobileNetV2 variant is utilized with pre-trained weights from the ImageNet dataset. The architecture is set up to exclude the top classification layer, retaining only the feature extraction part. This allows for extracting latent features or embedding from the image dataset, converting them into a form suitable for custom classification. After obtaining these embedding for both training and test datasets, a new neural network model is designed. This custom model consists of dense layers: two layers each with 64 units and ReLU activation functions, followed by an output layer with 20 units corresponding to the number of image categories and using the softmax activation function for multiclass categorization. The model is then compiled using the Adam optimizer and is set up to measure accuracy as the evaluation metric.

Xception:

Xception, which stands for "Extreme Inception," is an advanced architecture that uses depthwise separable convolutions to efficiently process spatial and channel-wise features independently. Just like with MobileNet, the Xception model is loaded with weights from the ImageNet dataset, while excluding its top classification layer. This enables the extraction of image features without the constraints of the original model's classification task, making it adaptable to the specific dataset at hand.

Inception:

The InceptionV3 model, often referred to as GoogleNet, is recognized for its inception modules, which allow the network to make optimized choices between different convolutional operations at various stages. It offers a mix of different sized filters in its architecture, which makes it versatile in capturing spatial hierarchies. Similar to the aforementioned models, InceptionV3 is employed without its top layers but retains the ImageNet-trained weights. After feature extraction, the latent representations of the images are reshaped and fed into a custom neural network model, mirroring the design used for MobileNet: two dense layers with 64 units each and ReLU activation, followed by an output layer of 20 units with softmax activation. Lastly, ensemble learning is mentioned as a technique, suggesting that the individual models (MobileNet, Xception, and Inception) might be combined in some manner to leverage the strengths of each model, potentially yielding better results than any single model could achieve on its own. Expanding on the use of various pre-trained deep learning architectures, our approach strategically integrates MobileNetV2, Xception, and InceptionV3 to capitalize on their individual strengths and address the complexity inherent in image recognition and representation tasks. The decision to employ an ensemble of these models is grounded in the concept of diversity and complementarity. Each of these models possesses unique architectural features that make them adept at capturing different aspects of the image data. For instance, MobileNetV2, with its streamlined architecture, excels in efficiently processing images with limited computational resources, making it ideal for real-time applications. Xception, on the other hand, leverages depthwise separable convolutions, offering a more nuanced understanding of spatial and channel-wise features. InceptionV3, with its inception modules, provides a robust framework for capturing complex spatial hierarchies within images. In our ensemble approach, the outputs from these individual models are combined to form a cohesive decision-making mechanism. This integration is not merely a simple aggregation but a sophisticated process that evaluates and weighs the contributions of each model based on their performance metrics. By doing so, our system benefits from the collective intelligence of these architectures, leading to a more accurate and reliable image retrieval process. Furthermore, we recognize the importance of fine-tuning these models to align them with the specific requirements of our dataset and retrieval tasks. To this end, the pre-trained weights from the ImageNet dataset serve as a starting point, providing a rich foundation of learned features. These features are then adapted and refined through additional training on our dataset, ensuring that the models are well-attuned to the nuances of the images they will encounter in practical applications. In addition to the technical intricacies of the ensemble method, we also emphasize the practical implications of this approach. By leveraging these powerful architectures, our system is not only capable of high-precision image retrieval but also exhibits a significant degree of robustness against various types of noise and distortions commonly encountered in real-world scenarios. This resilience, combined with the efficiency of the models, positions our system as a viable solution for a wide range of applications, from digital libraries and historical research to more demanding tasks like security surveillance and medical imaging. In conclusion, the strategic use of an ensemble of pre-trained deep learning models in our methodology underlines our commitment to pushing the boundaries of what is achievable in secure content-based image retrieval. It is this innovative integration of diverse, yet complementary, deep learning models that sets our research apart and contributes significantly to the advancement of the field.

3.5. Evaluation

1. **Accuracy:**

It gives the proportion of the total number of predictions that were correct.

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \qquad (2)$$

Where:

- (TP) = True Positives
- (TN) = True Negatives
- (FP) = False Positives
- (FN) = False Negatives

2. **Precision** (also known as the Positive Predictive Value):
   It quantifies the number of correct positive predictions made.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \qquad (3)$$

3. **Recall** (or Sensitivity or True Positive Rate):
   It quantifies the number of correct positive predictions made out of all actual positives.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \qquad (4)$$

4. **F1-Score:**
   It is the harmonic mean of precision and recall and gives a balanced measure between them.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \qquad (5)$$

Where:
- (TP) = True Positives: The number of correct positive predictions.
- (FP) = False Positives: The number of negative instances incorrectly predicted as positive.
- (TN) = True Negatives: The number of correct negative predictions.
- (FN) = False Negatives: The number of positive instances incorrectly predicted as negative.

By evaluating a model based on these metrics, one can gain a comprehensive understanding of its performance, especially in cases where the classes are imbalanced or when different types of errors have different costs.

4. Experiment Results

In the experiment results, the first order of business is to showcase the decrypted image. To accomplish this, the previously encrypted keys are decrypted using the Advanced Encryption Standard (AES) method. Once the original keys are retrieved, they are used to decrypt the image that 103combined encryption and decryption processes, and by displaying it, one can validate the integrity of the image post-decryption. The title "Decrypted Image" is labeled above the displayed image for clarity.

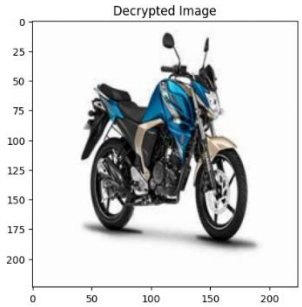

Fig. 2. Decrypted Image

In our experiment evaluating different deep learning architectures for CBIR tasks, we observed distinct performance metrics for the three models under consideration: Xception, MobileNet, and Inception. The Xception model, known for its depth-wise separable convolutions, recorded a remarkable accuracy of 92.375% in our CBIR system. This architecture, when used for image retrieval, displayed a precision of 93%, implying its capability to retrieve relevant images with high accuracy. With a recall of 92%, Xception's ability to identify the majority of relevant images in the dataset is evident. The F1-Score, a metric highlighting the balance between precision and recall, further validated this performance with a score of 92%.

Fig. 3. Image Retrieval with Xception

MobileNet, known for its lightweight and mobile-first design, was also tested for CBIR capabilities. The results showed an accuracy of 87.125%, slightly behind Xception. Its precision stood at 88%, suggesting a good but slightly reduced ability to retrieve pertinent images accurately compared to Xception. With recall and F1-score figures at 87%, MobileNet proves its reliability, but also indicates room for improvement in retrieving all relevant images efficiently.

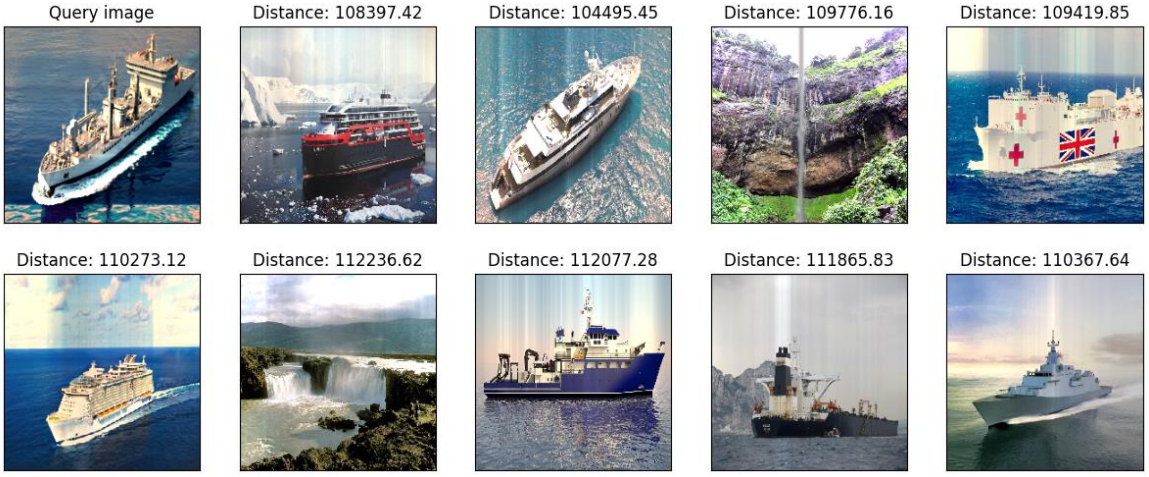

Fig. 4. Image Retrieval with MobileNet

Finally, Inception, designed with the idea of "network within a network", matched Xception's impressive performance in our CBIR system. Demonstrating an accuracy of 92.375%, it proved its efficacy in retrieving images based on content. The precision, recall, and F1-score of 93%, 92%, and 92%, respectively, further emphasized its balanced and robust capabilities in the image retrieval task.

Fig. 5. Image Retrieval with Inception

In essence, for CBIR tasks, Xception and Inception emerge as top contenders, delivering nearly identical and superior results. MobileNet, while efficient for mobile deployments, showed slightly subdued performance in comparison. Deciding on architecture would thus depend on the specific balance between computational efficiency and retrieval accuracy for a given CBIR application.

Table 1. Performance Metrics of Deep Learning Architectures for CBIR Tasks

Model	Accuracy	Precision	Recall	F1-Score
Xception	0.92375	0.93	0.92	0.92
MobileNet	0.87125	0.88	0.87	0.87
Inception	0.92375	0.93	0.92	0.92

The ensemble learning approach is combined the strengths of the three deep learning architectures (Xception, MobileNet, and Inception), exhibited enhanced performance for CBIR tasks.The ensemble achieved an impressive accuracy of 94.875%. This suggests that by combining the predictions of the three individual models, the ensemble was able to outperform each of them individually, leading to a more accurate image retrieval process. Furthermore, the precision of the ensemble stood at 95%, indicating that when the system retrieved images, 95% of them were relevant. This level of precision shows the strength of collective decision-making in minimizing false positives. In parallel, a recall score of 95% signifies that out of all the relevant images in the dataset, the ensemble successfully identified and retrieved 95% of them, minimizing false negatives.The F1-Score, a measure that takes both precision and recall into account, reached 95%. This further highlights the ensemble's balanced and robust performance in the CBIR task. The harmonized decision-making process of the ensemble, which leverages the strengths and offsets the weaknesses of individual models, has evidently provided a significant boost in performance metrics.

In conclusion, the ensemble learning of the three deep learning models has not only elevated the performance levels but also showcased the potential benefits of combining multiple architectures for intricate tasks like CBIR.

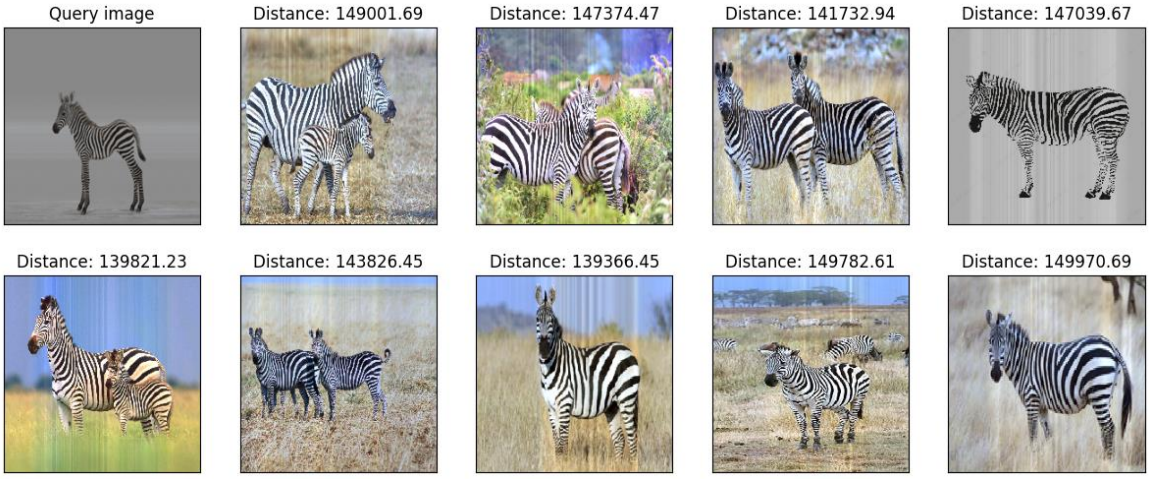

Fig. 6. Image Retrieval with Ensemble Learning

5. Discussion

In our exploration of deep learning architectures for CBIR tasks, the ensemble approach — a combination of Xception, MobileNet, and Inception models — has proven to be particularly effective. By pooling the expertise of these individual architectures, the ensemble model could achieve a better balance of precision and recall, resulting in superior retrieval accuracy. Such results shed light on the fact that the integration of multiple perspectives, each offered by distinct models, can lead to a more holistic and accurate decision-making process. However, CBIR tasks are not just about image retrieval accuracy. In the modern digital era, security is paramount, especially when dealing with potentially sensitive imagery. In our methodology, the security dimension was addressed by encrypting images using a combination of visual cryptography and the AES algorithm. This dual-layered approach ensured that even if malicious entities accessed the images, deciphering their content would be a formidable challenge without the correct decryption keys. The visual cryptography technique, which involves generating random sequences and shifts for encryption, ensured that images were transformed into patterns that would be nearly impossible to reconstruct without the correct sequence and shifts. On top of this, the AES encryption added another layer of complexity, further safeguarding the encrypted keys. Thus, our CBIR system doesn't merely retrieve relevant images but does so with a high regard for security. But why is this security layer crucial for a CBIR system? In real-world scenarios, image databases might contain confidential or proprietary visuals, such as design prototypes, private event photographs, or sensitive surveillance footage. Unauthorized access to such data could lead to significant breaches of privacy or intellectual property theft. Thus, incorporating robust encryption mechanisms ensures that while users can search and retrieve images based on content, the underlying data remains shielded from potential threats.

1. Synergy in Ensemble Learning

Our findings underscore the synergy that emerges when combining different deep learning models in an ensemble. Each model in the ensemble, namely Xception, MobileNet, and Inception, brings unique strengths to the table. For instance, MobileNet's efficiency is invaluable for applications requiring quick image retrieval, while Xception and Inception offer depth and complexity in feature extraction. This synergy is not merely an addition of capabilities but a multiplication of effectiveness, as the ensemble leverages the specific advantages of each model while mitigating their individual limitations. The remarkable accuracy and precision achieved by the ensemble approach underscore the potential of combining diverse methodologies to create a solution that is greater than the sum of its parts.

2. Balancing Efficiency and Accuracy

In practical applications, there is often a trade-off between computational efficiency and accuracy. Our results indicate that while MobileNet may lag slightly behind in terms of raw performance metrics, its lightweight design makes it an ideal choice for scenarios where computational resources are limited, such as in mobile applications or edge computing. Conversely, Xception and Inception, with their higher

computational demands, are better suited for scenarios where accuracy is paramount and computational resources are more abundant. Understanding these trade-offs is crucial when designing and implementing a CBIR system, as it allows for customization based on specific use-case requirements.

3. Security as an Integral Component

The dual-layered encryption approach integrating visual cryptography and AES encryption underlines the importance of security in CBIR systems. As we navigate a landscape where data breaches and cyber threats are increasingly common, the need to protect image data becomes paramount. Our approach demonstrates that it is possible to achieve high levels of security without compromising on the system's core functionality - efficient and accurate image retrieval. This is particularly relevant in fields such as healthcare, where patient confidentiality is crucial, or in industrial settings, where trade secrets must be protected.

4. Future Directions and Challenges

Looking forward, the field of CBIR faces the dual challenges of managing ever-growing image databases and addressing increasingly sophisticated security threats. The success of our ensemble approach suggests that future research should continue to explore the integration of multiple models and technologies. Additionally, as image databases grow in size and complexity, scalability will become a critical concern. Developing systems that can maintain high levels of accuracy and security while scaling to accommodate larger datasets will be a key area of focus.

5. Ethical Considerations in CBIR

Finally, as CBIR technologies advance, ethical considerations must be at the forefront of development. Issues such as user privacy consent for image use, and potential biases in image retrieval algorithms need careful attention. Ensuring that CBIR systems are not only efficient and secure but also ethically sound and unbiased is essential. As researchers and developers, we have a responsibility to consider the broader societal impacts of our work, striving to create technologies that are beneficial and equitable.

In summary, our exploration into CBIR using an ensemble of deep learning models coupled with robust encryption techniques has yielded significant insights into the interplay between accuracy, efficiency, and security. These findings not only contribute to the advancement of CBIR technology but also set a precedent for future research in the field, emphasizing the importance of balanced, secure, and ethically responsible solutions.

6. Comparison with Other Works

In the rapidly evolving field of Content-Based Image Retrieval (CBIR), a variety of techniques and methodologies have been developed, each contributing uniquely to the domain. Our research presents an innovative approach to secure CBIR, integrating deep learning architectures with advanced encryption techniques. To contextualize our work within the broader landscape of CBIR research, we compare it with several notable studies, highlighting key similarities and differences.

1. Methodological Innovations and Similarities

Our approach shares conceptual similarities with the works of Xia et al. ([12], [29], [31]), who also focused on secure CBIR systems. Like our model, these studies employed encryption techniques to enhance security, albeit using different methods such as Block Permutation and Earth Mover's Distance. Moreover, the deep learning aspect of our methodology resonates with the approaches of Qin et al. ([14]) and Li et al. ([22]), which leveraged neural networks for improved retrieval accuracy and efficiency.

2. Distinctive Features of Our Model

A distinctive aspect of our work lies in the ensemble learning approach, combining the strengths of multiple deep learning models (Xception, MobileNet, and Inception). This multi-model strategy, not explicitly adopted in the referenced works, provides a nuanced approach to image retrieval, balancing

accuracy with computational efficiency. Furthermore, our dual-layered encryption scheme, incorporating both visual cryptography and AES encryption, offers a unique blend of security measures, ensuring both the protection of image data and the integrity of the retrieval process.

3. Technological Diversification

The landscape of CBIR research is marked by technological diversification, as seen in the various methods employed by different studies. For instance, Awan et al. ([13]) and Cheng et al. ([21]) used neural networks and CNNs, respectively, focusing on specific applications like malware categorization and surveillance video privacy. In contrast, our study leverages a broad spectrum of deep learning architectures, making it adaptable to a wider range of CBIR applications.

4. Similarity Measures and Model Usage

A key area of comparison lies in the similarity measures and models used. Our approach, primarily grounded in deep learning models, was contrasted with the specific methods like KNN-based similarity (Qin et al. [14]), DCT-based retrieval (Tang et al. [16]), and Kernel-based Supervised Hashing (Cheng et al. [21]). These varying approaches to similarity measurement underscore the diverse methodologies within the field.

5. Addressing Gaps and Advancing the Field

Our research addresses certain gaps in the existing literature, particularly in the realm of security and efficiency balance. While several studies focus on either aspect, our model integrates them cohesively, ensuring robust security without compromising retrieval performance. This integrated approach sets our work apart, contributing a novel perspective to the CBIR domain.

7. Conclusion

In the evolving field of Content-Based Image Retrieval (CBIR), our research highlights the effectiveness of combining multiple deep learning models—Xception, MobileNet, and Inception—in an ensemble approach. This integration not only improves retrieval accuracy but also exemplifies the benefits of collective decision-making in AI. Crucially, our CBIR system emphasizes security, integrating visual cryptography with AES encryption. This approach ensures reliable image retrieval while safeguarding data privacy and security, addressing key concerns in the digital age. Ultimately, our work illustrates the potential of blending advanced AI with strong cybersecurity to efficiently and securely manage visual data, paving the way for a more secure digital environment.

8. Future Works

As we move forward, our primary objective will be to further refine and expand our CBIR system's capabilities. This involves delving deeper into newer deep learning architectures and ensemble techniques to boost retrieval accuracy. Additionally, we aim to incorporate more advanced encryption methods, offering even greater security layers to protect against evolving cyber threats. Adapting to a variety of datasets, ensuring system scalability, and optimizing for real-time retrieval will also be pivotal. Embracing the feedback from real-world deployments, we plan to tailor the system to cater to specific industry needs, ensuring it remains at the forefront of both performance and security in the dynamic realm of image retrieval.

6. References

[1] Z. A. Abduljabbar, A. Ibrahim, M. A. Hussain, Z. A. Hussien, M. A. Al Sibahee, S. Lu, KSII Transactions on Internet and Information Systems (TIIS), **13**(11), 5692(2019). DOI:https://doi.org/10.3837/tiis.2019.11.023

[2] Z. A. Abduljabbar, H. Jin, A. Ibrahim, Z. A. Hussien, S. H. Abbdal, D. Zou, In: Proceedings of the International Conference on Signal Processing, Communication, Computing ICSPCC 2016 (2016). DOI:https://doi.org/10.1109/ICSPCC.2016.7753617

[3] Z. A. Abduljabbar, H. Jin, A. Ibrahim, Z. A. Hussien, M. A. Hussain, S. H. Abbdal, D. Zou, SEPIM: Secure and efficient private image matching. Applied Sciences **6**(8), 133(2016). DOI:https://doi.org/10.3390/app6080213

[4] M. A. Al Sibahee, A. I. Abdulsada, Z. A. Abduljabbar, J. Ma, V. O. Nyangaresi, S. M. Umran, Applied Sciences **11**(24), 12040(2021). DOI:https://doi.org/10.3390/app112412040

[5] M. A. Al Sibahee, S. Lu, Z. Ameen Abduljabbar, A. Ibrahim, Z. A. Hussien, K. A. Mutlaq, M. A. Hussain, Efficient encrypted image retrieval in IoT-cloud with multi-user authentication, International Journal of Distributed Sensor Networks **14**(2), 5692(2018) DOI:https://doi.org/10.1177/1550147718761814

[6] M. A. Hussain, Z. A. Hussien, Z. A. Abduljabbar, J. Ma J, M. A. Al Sibahee, S. A. Hussain, V. O. Nyangaresi, X. Jiao, Egyptian Informatics Journal **23**(4), 145(2022). DOI:https://doi.org/10.1016/j.eij.2022.10.001

[7] F. Valente, A. Silva, C. Costa, Current Medical Imaging **9**(4), 250(2013). DOI:https://doi.org/10.2174/15734056091310281214

[8] F. Liu, et al., IEEE Access **7**, 119209(2019). DOI:https://doi.org/10.1109/ACCESS.2019.2935222

[9] L. Zhang, et al., Neural Computing and Applications, 1949(2020). DOI:https://doi.org/10.1007/s00521-019-04491-4

[10] X. Li, J. Yang, J. Ma, Neurocomputing **452**, 675 (2021). DOI:https://doi.org/10.1016/j.neucom.2020.07.139

[11] Heron, Network Security.**12**, 8(2009). DOI:https://doi.org/10.1016/S1353-4858(10)70006-4

[12] Z. Xia, L. Wang, J. Tang, N. Xiong, J. Weng, IEEE Transactions on Network Science and Engineering **8**(1), 318(2020). DOI:https://doi.org/10.1109/TNSE.2020.3038218

[13] M.J. Awan, O.A. Masood, M.A. Mohammed, A. Yasin, A.M. Zain et al., Electronics **10**(19), 2444 (2021). DOI:https://doi.org/10.3390/electronics10192444

[14] J. Qin, J. Chen, X. Xiang, Y. Tan, W. Ma et al., Journal of Real-Time Image Processing **17**(1), 161(2020). DOI:https://doi.org/10.1007/s11554-019-00909-3

[15] W. Ma, J. Qin, X. Xiang, Y. Tan, Z. He, Mathematics **8**(6), 1019 (2020). DOI:https://doi.org/10.3390/math8061019

[16] J. Tang, Z. Xia, L. Wang, C. Yuan, X. Zhao, Journal on Big Data **3**(1), 21(2021). DOI:https://doi.org/10.32604/jbd.2021.015892

[17] Y. Xu, J. Gong, L. Xiong, Z. Xu, J. Wang, Journal of Visual Communication and Image Representation **43**(2), 164(2017). DOI:https://doi.org/10.1016/j.jvcir.2017.01.006

[18] D. Liu, J. Shen, Z. Xia, X. Sun, Information-an International Interdisciplinary Journal **8**(3), 96(2017). DOI:https://doi.org/10.3390/info8030096

[19] Y. Wu, L. Zhang, S. Berrettiv, S. Wan, IEEE Transactions on Industrial Informatics **19**(2), 2089-2098 (2022). DOI:https://doi.org/10.1109/TNSE.2022.3151502

[20] J. Anju, R. Shreelekshmi, Expert Systems with Applications **189**, 1(2022). DOI:https://doi.org/10.1016/j.eswa.2021.116070

[21] H. Cheng, H. Wang, X. Liu, Y. Fang, M. Wang et al., IEEE Transactions on Dependable and Secure Computing **18**(3), 1456(2019). DOI:https://doi.org/10.1109/TDSC.2019.2923653

[22] Y. Li, J. Ma, Y. Miao, Y. Wang, X. Liu et al., IEEE Transactions on Cloud Computing **10**(2), 1142(2020). DOI: https://doi.org/10.1109/TCC.2020.2989923

[23] L. Weng, L. Amsaleg, T. Furon, IEEE Transactions on Knowledge and Data Engineering **28**(10), 2738(2016). DOI: https://doi.org/10.1109/TKDE.2016.2587258

[24] X. Wang, J. Ma, Y. Miao, Journal of Communications (Chinese) **40**(2), 31-39 (2019). DOI:https://doi.org/10.1109/TDSC.2019.2897675

[25] A. Hassan, F. Liu, F. Wang, Y. Wang, Journal of Systems Architecture **116**, 1(2021). DOI:https://doi.org/10.1016/j.sysarc.2021.102043
[26] B. Baliga, R. Medepalli, S. Muralikrishna, International Journal of Information Technology **13**(3), 1111(2021). DOI:https://doi.org/10.1007/s41870-020-00582-x
[27] A. Du, L. Wang, S. Cheng, N. Ao, Symmetry **12**(2), 282 (2020). DOI:https://doi.org/10.3390/sym12020282
[28] C. Zhang, L. Zhu, S. Zhang, W. Yu, Neurocomputing **406**(1), 386(2020). DOI:https://doi.org/10.1016/j.neucom.2019.11.119
[29] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, IEEE Transactions on Information Forensics and Security **11**(11), 2594(2016). DOI:https://doi.org/10.1109/TIFS.2016.2590944
[30] Y. Wu, H. Guo, C. Chakraborty, M. Khosravi, S. Berretti et al., IEEE Transactions on Network Science and Engineering **10**(5), 3086 (2022). DOI:https://doi.org/10.1109/TNSE.2022.3151502
[31] Z. Xia, Y. Zhu, X. Sun, Z. Qin, K. Ren, IEEE Transactions on Cloud Computing **6**(1), 276(2015). DOI:https://doi.org/10.1109/TCC.2015.2491933

Journal of Basrah Researches (Sciences) **49**(2), 94 (2023)
DOI: https://doi.org/10.56714/bjrs.49.2.9

نظام آمن لاسترجاع الصور القائم على المحتوى باستخدام التعلم العميق

مقدام عبدالواحد محمد[1]، محمد عبدالرضا حسين[1]، زكريا احمد عريبي[1]، زيد امين عبد الجبار[1]، Vincent Omollo Nyangaresi[2]

[1]قسم علوم الحاسوب، كلية التربية للعلوم الصرفة، جامعة البصرة، البصرة ، العراق
[2]قسم علوم الكمبيوتر وهندسة البرمجيات، جامعة جاراموجي أوجينجا أودينجا للعلوم والتكنولوجيا، بوندو، كينيا

معلومات البحث

الاستلام 03 تشرين الأول 2023
القبول 11 تشرين الثاني 2023
النشر 30 كانون الأول 2023

الكلمات المفتاحية

التعلم العميق ، استرجاع الصور القائم على المحتوى ، التشفير المرئي، معيار التشفير المتقدم.

الملخص

تحقق هذه الورقة البحثية في استرجاع الصور المبني على المحتوى (CBIR) باستخدام مجموعة من ثلاثة هياكل تعلم عميق متطورة: Xception، MobileNet، و Inception. أظهر هذا النهج المجمع دقة استرجاع استثنائية، حيث حققت نماذج Xception و Inception دقة بنسبة 92.375%، ودقة واستدعاء بنسبة 93% و 92% على التوالي، ونتيجة F1 بنسبة 92%. كما أظهر نموذج MobileNet أداءً قويًا، مع دقة بنسبة 87.125%، ودقة واستدعاء بنسبة 88% و 87%، ونتيجة F1 بنسبة 87%.إلى جانب دقة الاسترجاع المجردة، تضع الدراسة تركيزًا كبيرًا على أمان قاعدة بيانات الصور. تم استخدام طريقة تشفير ثنائية الطبقات، متكاملة مع التشفير البصري ومعيار التشفير المتقدم (AES) لضمان حماية قوية للبيانات الحساسة. يضمن هذا النهج استرجاع الصور بكفاءة بناءً على المحتوى مع تأمين البيانات ضد الاختراقات المحتملة. تبرز النتائج كفاءة النموذج المجمع في تحقيق التوازن بين دقة الاسترجاع العالية وتدابير الأمان الصارمة. يعتبر هذا التوازن ذا صلة خاصة بالتطبيقات في المكتبات الرقمية، والبحث التاريخي، وتحديد البصمات، ومنع الجريمة. تدعو نتائج الورقة إلى الحاجة الحرجة لدمج بروتوكولات أمان قوية في أنظمة CBIR المستقبلية، لضمان الأداء الأمثل دون المساس بأمان البيانات.

Citation: M. A. Mohammed et al., J. Basrah Res. (Sci.) **49**(2), 94 (2023).
DOI:https://doi.org/10.56714/bjrs.49.2.9

***Corresponding author email :** mkdaam@gmail.com

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq