ISSN (Paper) 1994-697X

Online 2706 -722X

A Secure Search for Outsourced Image Collection Based Content-Based Image Retrieval

Israa Kadhem Abady Hamady
B.Sc., Computer Science, Basrah University

Abstract:

Various research fields have shown significant interest in the real-world applications of image retrieval in recent years. Content-Based Image Retrieval (CBIR) has become a prevalent technique that is gradually being integrated into retrieval systems. However, images require more storage than text documents, and cloud computing is often used to outsource them. For sensitive images, like those used in medicine, they must be encrypted before being sent to a third party.This study proposes a novel classification and retrieval technique to search for related objects in encrypted images. The proposed framework relies on Convolutional Neural Networks (CNN) and LSTM networks, which unlock the potential of secure, content-based image retrieval and mass encoding. In this technique, the original images are first processed using a CNN neural network, and their features are extracted. Next, the features of the encoded images are extracted by training a new CNN neural network using the weights and activation functions of the previous neural network. The feature set is then divided into two groups for training and testing, with the feature training portion used to train the LSTM neural network. The proposed method outperforms the original article in all of the evaluated parameters, according to simulation findings using MATLAB software and the results was viwed in excel based on the generated numbers. This research offers a promising approach to secure content-based image retrieval and mass encoding, which could have significant implications for sensitive fields like medicine.

Keywords: Content-Based Image Retrieval (CBIR), Secure Search, Outsourced Image Collection, CNN, LSTM.

1. Introduction

Due to the quick growth of digital technology, a lot of images are produced and shared every day. Rich information can be discovered from this image data, which has been investigated in various fields such as feature extraction, information hiding, and image retrieval. Today, there is growing interested in finding the desired image in a large dataset, and many sophisticated retrieval techniques are presented. More quality images in the database can be used in different research fields, leading to more accurate and optimal diagnoses. However, significant storage and computing resources are required to support this capacity. Therefore, cloud services can meet user storage and other computing needs (sharing, retrieval, and analysis).

Because it takes a lot of storage space and sophisticated computing power to find a specific image among a large number of images, which is nearly impossible for users of light devices (like smartphones), outsourcing image data to cloud storage providers is one of the most practical solutions because they offer enormous storage space and strong computing power. However, outsourcing image data containing sensitive information to a server often creates significant problems concerning data control and privacy (such as financial status, personal identity, and health records). Researchers have devoted much effort to this field to manage and utilize image resources efficiently and developed some useful retrieval schemes. Before outsourcing, the proprietor of the data can typically encrypt sensitive information to guard against hackers or unauthorized access to cloud services. Despite the fact that such a measure can help secure the privacy of primary data, implementing such a system can be expensive and challenging.

To increase the efficiency of retrieving comparable images and make the best use of image information, researchers put forth a number of image retrieval schemes. Examples of current methods for retrieving images in the plaintext realm include text-based image retrieval (TBIR) and content-based image retrieval (CBIR). Due to many images, storing and finding images is challenging for image owners. As a result, CBIR services often require a lot of computation and storage.

The image owner's primary worry, in addition to the many advantages of CBIR outsourcing, is image privacy. Additionally, attacks on cloud servers are frequent because hackers are frequently interested in the data kept on these platforms. However, a cloud service may correctly follow some protocol requirements. Still, it may be sensitive due to the desire to extrapolate or analyze data from the image to discover information. The cloud server may scan sensitive data in images and expose personal information.

To avoid unauthorized access, the majority of image owners typically encrypt their image data before sending it to the computer. The encrypted picture, however, might not be appropriate for image recovery in this manner [2]. Searching on encoded tag-based indices can be helpful for secure picture searching because any real-world image can be annotated with multiple tags [3] [4].

ISSN (Paper)-1994-697X (Online)-2706-722X

Many content-based, privacy-preserving, and picture retrieval techniques have been put forth. Still, according to research on the subject, they are generally not applicable to some images, such as medical imaging. This research investigates the potential of creating a safe method for automatically searching images using CNN. The proposed method combines CNN and LSTM neural networks to search and retrieve encrypted images. The rest of the article is organized as follows: In the second part, a background of the work done in the field of image recovery will be stated. The third part contains the details of the proposed method. The fourth part will also show the results of the simulation and evaluations. In the final part, express the general conclusion in the field of research.

2. Related Work

In recent years, due to the growth and importance of multimedia information, as well as the existence of very large databases of image and video data, the effort to find suitable tools for retrieving various images from these data centers have always increased. The goal of content-based image retrieval (CBIR), a frequently and widely used field of study in digital image processing, is to locate digital images from a significant database. To retrieve images from huge databases, a method called content-based image retrieval uses the visual content of the images. Therefore, efficient and useful image retrieval and retrieval is very important.

A secure recovery technique for images encoded in the YUV color space was introduced by Xia et al. [1]. The search result reveals that in the YUV color space, the combination of AC coefficients and color histograms offers higher retrieval accuracy than either of them alone. In this paper, the researchers combine color histograms and AC coefficients to recover the image in the encrypted domain.

An effective and practical computational outsourcing strategy for the local binary pattern (LBP) feature on huge encrypted images was put forth by Xia et al. in their paper published in [5]. In this approach, a picture is split into non-overlapping blocks for encryption purposes, and the blocks are then mixed to safeguard the image data. The non-centered images are then distributed at random within each block. The original picture data is then randomly divided to encode the pixels. Cloud servers can use secure multiparty computation to determine LBP features after getting such an encrypted image. The three algorithms in the suggested plan are carried out by three different parties: the image owner for the GenKey and EncImg algorithms, and cloud servers for LBP feature extraction. Then, using LBP features, other algorithms are run, like image recovery or facial recognition.

Cheng et al. [6] suggested a brand-new unsupervised approach for image retrieval in the encrypted domain without training sets. Using this technique, images are completely encrypted while maintaining the file structure and size. The server can first extract the local data of intra-block AC coefficients from an encrypted query image without having to decode it. As a result, the user gets encrypted images that can be decoded and displayed because they contain plain text data that is similar to the requested image.

In the novel image retrieval scheme, Wang et al. [2] combined the bag-of-words model with random mapping features to develop a cipher text image retrieval approach. The cloud server

ISSN (Paper)-1994-697X (Online)-2706-722X

generates random patterns, encrypts the image using an advanced encryption standard, and then extracts local features. Forough and Mumtazi [7] suggested a privacy-preserving image retrieval scheme in which images are encrypted but images that match a query can be successfully retrieved from encrypted images. This research suggested a user-privacy-protecting Secure Local Binary Pattern (LBP) and Bag-of-Words (BOW) model-based image retrieval scheme.
Bush et al[8]. Introduction of SOFIR, a tool for securely outsourcing forensic image recognition that enables companies and law enforcement to jointly identify illegal network traffic at its source, made it possible to quickly adopt measures. SOFIR employs cryptography to keep the participating companies from seeing the hash database. In addition to regulatory protecting the company's legitimate network traffic, SOFIR transmits an encrypted report comprising just the number of illegal images found during predetermined intervals to the appropriate law enforcement agency.

A technique for enabling CBIR on encrypted images without revealing personal information to the cloud service is presented by Xia et al. in [9]. Related images are first represented by the feature vectors that are extracted first. Then, to improve search speed, prefilter tables are built using locale-sensitive hashing. Then, the secure k-nearest neighbor (kNN) algorithm is used to defend the feature vectors.

Nayak et al. [10] suggest a brand-new public-key searchable encryption scheme (SEPS) that makes use of an inverse index data structure. They demonstrate that SEPS beats earlier initiatives (both theoretically and empirically). Using the Diffie-Hellman bilinear assumption, they show that the suggested scheme is secure. SEPS protects against keyword guessing attacks and has port anonymity.

Cao et al. [11] proposed a framework for an encrypted image and privacy preservation in painting for outsourced images. Unlike traditional image painting in plain text, this framework has two entities: the content owner and the image retriever. The image recovery, which may be a cloud server with powerful computing capabilities, receives the encrypted and damaged image from the content owner after it has been first encrypted for privacy protection. Image recovery applies in painting to an encrypted domain and sends the in-painting and encrypted image to the content owner or other authenticated recipient.

Li et al. [12] propose a new privacy-preserving content-based image retrieval that defends against attacks by the data owner, cloud server, and users with a key privacy scheme combining HE and ASPE perspectives. This image recovery method protects anonymity and is developed using a powerful threat model that resembles the real world. This system simultaneously protects the query information's privacy and the key's confidentiality.

With a key switching technique, Song et al. [13] suggest an efficient image retrieval and privacy-preserving scheme (PPIRS). PPIRS makes use of inner product encryption to calculate Euclidean distances between picture feature vectors and query vectors while maintaining anonymity. PPIRS achieves the lowest communication cost and minimizes the search area for image retrieval by using the key switching technique (KST) to reduce the dimensions of the encoded image feature vectors.

Wang and Yu [14] proposed a secure, searchable image retrieval scheme with an appropriate retrieval identity to address user privacy concerns. They implement entity identification in this method using elliptic curve cryptography. Locale-sensitive hash functions can create prefilter tables

ISSN (Paper)-1994-697X (Online)-2706-722X

that increase retrieval effectiveness.The findings of the experiments demonstrate that it is possible to accurately identify the system and to safeguard the statistical data contained in the image data.

Anju and Shreelekshmi's prototype for faster and more secure content-based image retrieval (FSeCBIR) [15] guarantees secure search and retrieval in sizable encrypted image databases. The anti-copy module in this prototype aids in the detection of data breaches brought on by suspect query users.

In next section, described the system model and present the proposed method and its details.

3. Proposed method

A set of technologies called Query by Image Content (QBIC), also known as Content-Based Image Retrieval (CBIR), makes organizing digital images according to their visual characteristics possible. Their main concept is to use computer vision methods to solve the problem of image retrieval in large databases. CBIR involves searching through an image database for images that resemble a query image. In this case, image retrieval is based on features that can be extracted directly from the visual data instead of using keywords or annotations. Therefore, in this study, the database's end output is retrieved by extracting features from the images used as query input. This research uses the optimization feature selection technique based on CNN to select the best features by combining color and texture data. During the training process, the vector dataset maintains these ideal properties. Finally, training images are taken from the dataset and classified using the LSTM network in order to extract pertinent images.

The proposed approach combines CNN and LSTM neural networks to search and retrieve encrypted images. The original images are first processed using the CNN neural network in the proposed method, and their features are extracted. In the next step, the weight of the neurons, bias, and activation functions used in the trained neural network is sent to the server along with the coded images. Next, a new CNN neural network is trained with the neural network's weights and activation functions and extracts features from the coded images. In this step, the features of encrypted images are extracted. In the next step, this set of facilities is divided into two categories, training, and testing. An LSTM neural network then uses the properties of the feature training section. The next step consists of testing the proposed system using the properties of the features. The steps of the proposed method are shown in Figure (1):

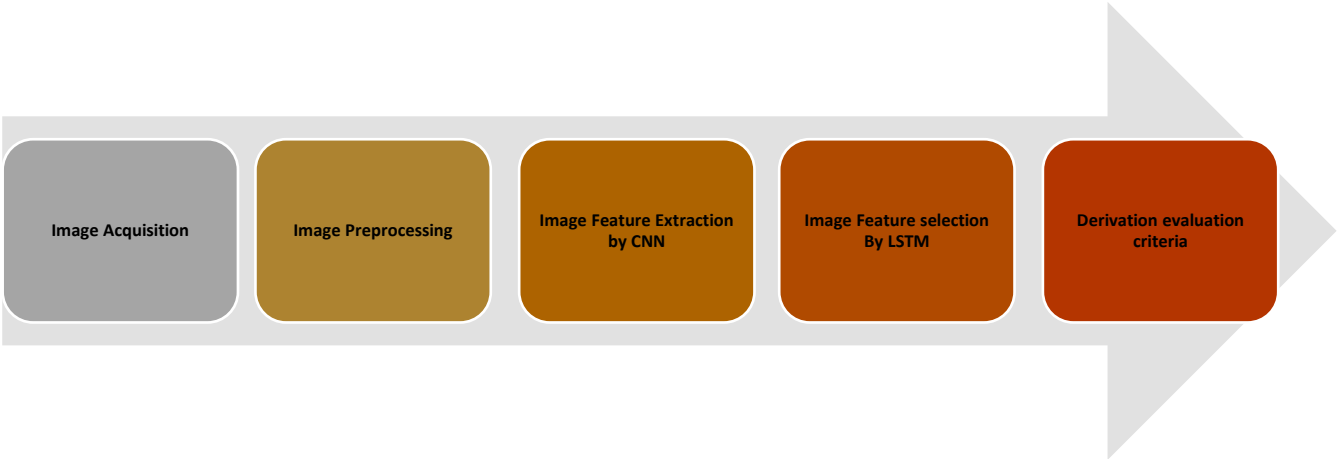

Figure (1) Steps of the proposed method

Steps of proposed method:

1. Pre-processing: increasing the quality of received images by removing unwanted waves such as noise, poor contrast, and unwanted background.
2. Feature extraction with CNN: Low-level features are important and are used to extract features from the neural network method. The input layer of the proposed CNN model uses images with a size of 224×224. Convolutional, Bulk Normalization, and Maxpooling layers are placed after the input layer.
3. Feature selection with LSTM: When classifying images, the selection of input features has a great impact on classification accuracy, training set requirements, and classification accuracy.

1.1 Feature Extraction using CNN

Three characteristics of CNN-based techniques have made them well-liked in image processing: local receptive fields, joint weights, and spatial or temporal subsampling. These characteristics make it possible to recognize the characteristics of a picture regardless of scale, distortion, or level of change. It is more practical to use CNNs because they can narrow the gap between training and testing errors. The complexity layer, hybrid layer, and fully connected layer are the three major layers of a CNN. Post-propagation and feed-forward are the two training phases that each convolutional neural network goes through. In the first stage, the input image is presented to the network. After dot multiplication between the input parameters and each neuron, the convolution operation is applied to each layer. Then the output of the network is determined. The output product is also used to perform network training, which is changing network parameters by calculating the amount of error in the network.

The amount of error is determined by comparing the network output with an appropriate response and error function. The next step, post-propagation, is based on the calculated error rate. The gradient of each parameter is calculated using the chain rule at this point, and the value of each parameter is adjusted according to how it affects the network error. After the parameters are updated, the next feed-forward process starts. When many of these steps are repeated, the network is trained.

1.2 Feature reduction using LSTM

Short-term memory is a special kind of recurrent neural network that can form long-term memories. In LSTM networks, the feedback unit has a memory cell vector to preserve long-term connections. To control when and how data is read or written from a memory cell, LSTM also incorporates a gating mechanism. A gate in LSTM typically uses a sigmoid function $\sigma(z) = 1 / (1 + e - z)$ and controls the data using a point multiplication operation. In particular, the gate prevents any information from passing when the sigmoid function ends at 0, but permits all information to pass when the output of the sigmoid function is 1. The LSTM unit "remembers" the data using the status of the memory cell and the gate mechanism until the forget gate deletes it. The proposed approach uses a CNN feature extraction system for original and encoded images. Instead of using a clustering approach (like the paper [14]) to identify the query image, it uses LSTM neural network. Using the

www.misan-jas.com ISSN (Paper)-1994-697X (Online)-2706-722X

LSTM neural network makes it possible to train a powerful neural network to extract query images using features extracted from original and encoded images. For this purpose, the extracted features are divided into training and testing. The training part is used to learn the LSTM neural network, but the test part is used to query the proposed system. Using the LSTM neural network for querying has a higher ability than the clustering method. Figure (2) displays the suggested method's flowchart.

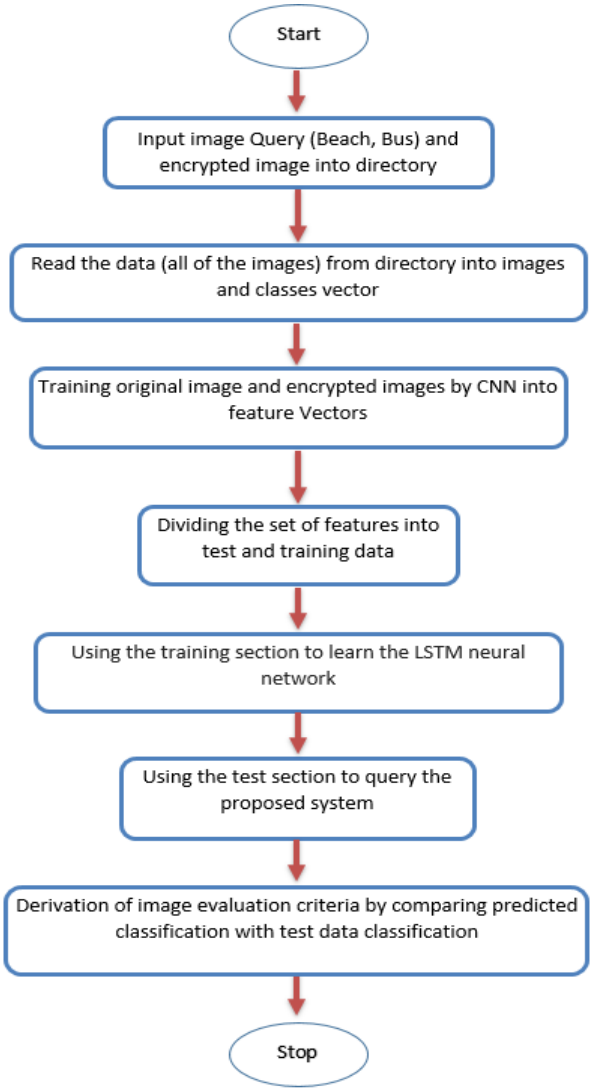

Figure (2) Flowchart of the proposed method

2. Evaluate the proposed method

This article uses MATLAB software to compare the performance and prove the proposed method's effectiveness. Also, in addition to the proposed strategy, one of the latest articles presented in the field of image retrieval has been implemented. In this paper, used the Corel dataset [16][17], which contains many real-world Images of nature and humans, to evaluate the results. This dataset contains 1000 images organized into ten distinct categories. All images are in JPEG format with dimensions of 384 x 256 pixels and are tagged with RGB color space

ISSN (Paper)-1994-697X (Online)-2706-722X

.Classification and retrieval of images using features extracted from images are investigated. In image classification, the output of the system is images that are placed in different categories and considering that the correct class of each idea is already determined, there are four possible states for the classification performed by the proposed system, Evaluation criteria such as accuracy, precision, recall, and F-measure have been used to check the results and performance of the proposed method.

On the other hand, two different scenarios have been used according to the effect of the number of parameters in evaluating the results. In the first scenario, examined the effect of the number of queries on the data set. Here, varied the number of queries between 30% and 70% of the total data sample size and then analyzed the evaluation findings. In the following, the evaluation results of this scenario are presented.

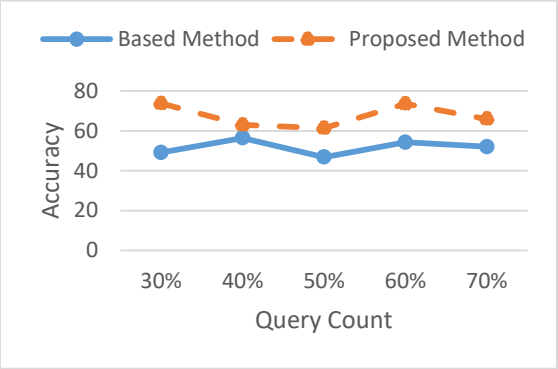

Figure (3) Checking the Accuracy parameter with changes in the number of queries

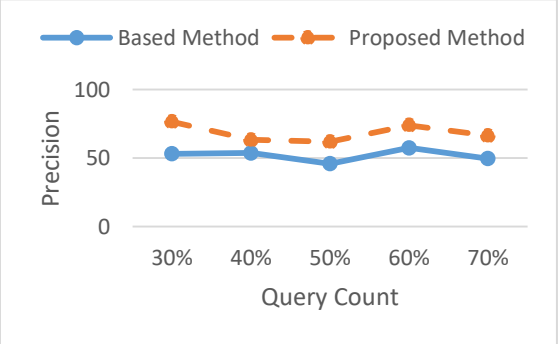

Figure (4) Checking the Precision parameter with changes in the number of queries

ISSN (Paper)-1994-697X (Online)-2706-722X

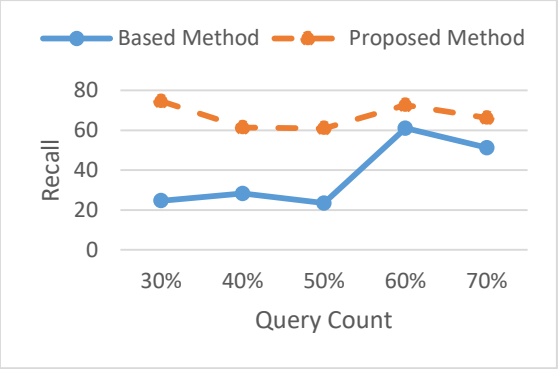

Figure (5) Checking the Recall parameter with changes in the number of queries

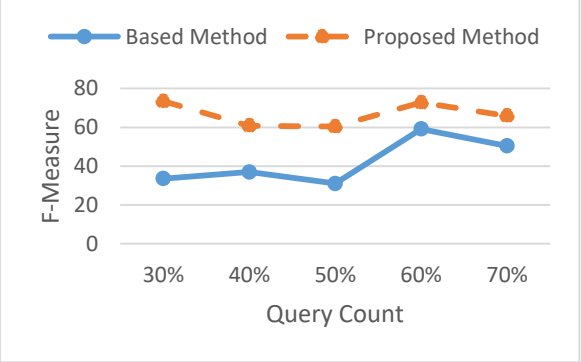

Figure (6) Checking the F-Measure parameter with changes in the number of queries

According to the results presented in figures (3) to (6), it can be seen that in all criteria, the absolute superiority of the proposed method is such that in all the measured distances, has been able to achieve far better results.

In the second scenario, the effect of the change in the data set size parameter have examined. The number of images used in a strategy can significantly affect its performance. The following results for each evaluation criterion can be seen in figures (7) to (10).

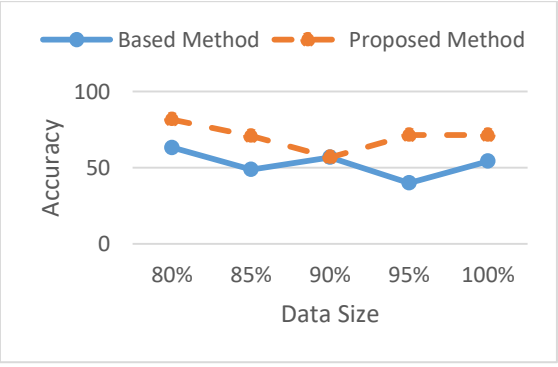

Figure (7) checks the Accuracy parameter for changing the size of the data set

ISSN (Paper)-1994-697X (Online)-2706-722X

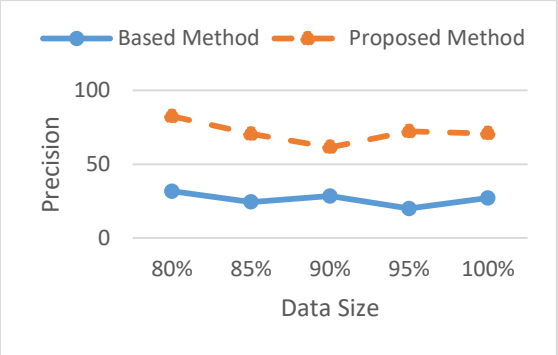

Figure (8) checks the Precision parameter for changing the size of the data set

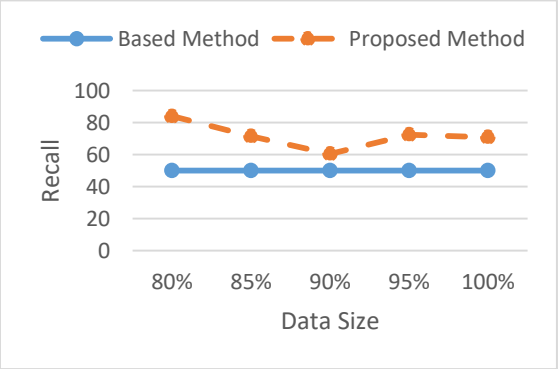

Figure (5) checking the Recall parameter for changing the size of the data set

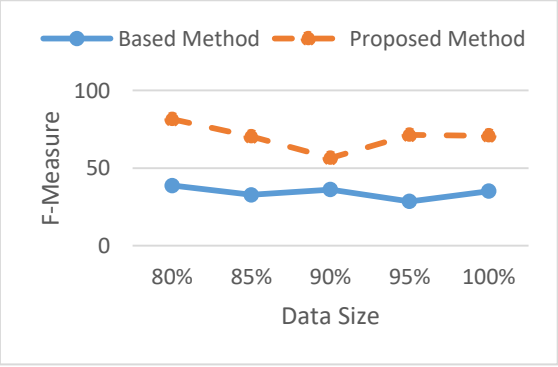

Figure (5) checking the F-Measure parameter for changing the size of the data set

The above graphs show that compared to the base method in the second scenario, and the proposed method has provided significant results. The proposed approach has maintained superiority over the comparison method in all evaluation criteria.

ISSN (Paper)-1994-697X (Online)-2706-722X

5. Conclusion

Image retrieval is one of the newest research areas in machine vision. The diverse applications of this research area have attracted much attention among academic researchers and industrialists. Due to the diverse applications, numerous investments in this research field, and significant developments, this research field is still considered nascent.

The proposed method combines CNN and LSTM neural networks to search and retrieve encrypted images. The original images are first processed using the CNN neural network in the proposed method, and their features are extracted. In the next step, the weights of the neurons, the bias, and the activation functions used in the trained neural network are sent to the server along with the encoded images. Next, a new neural network CNN with weights and neural network activation functions is trained and extracts features from encoded images. In this step, the features of encrypted images are extracted. In the next step, this set of features is divided into two groups, training, and testing. Then an LSTM neural network uses the features of the training part. The next step consists of testing the proposed system using the properties of the features.

To evaluate the proposed method, the Corel dataset has been used in the field of research. In addition, there are two different scenarios to evaluate. The first scenario examines the impact of the number of queries. However, the purpose of the second scenario is to examine the impact of the amount of data collected. The results demonstrate that the proposed method outperforms the base paper in both situations and for all evaluated parameters, according to evaluation criteria like accuracy, precision, recall, and F-measure.

Researchers who are interested in image processing studies are advised to look at dataset feature selection using different algorithms, especially meta-heuristic algorithms. To increase the effectiveness of image search and retrieval, a variety of classifiers, including neural networks, can be used in addition to effective feature extraction techniques with evolutionary approaches.

References:

[1] Xia, Z. H., Lu, L. H., Qin, T., Shim, H. J., Chen, X. Y., & Jeon, B. (2019). Privacy-preserving image retrieval based on AC coefficients and color histograms in a cloud environment. CMC-COMPUTERS MATERIALS & CONTINUA, 58(1), 27-43. https://doi.org/10.32604/cmc.2019.02688

[2] Wang, H., Xia, Z., Fei, J., & Xiao, F. (2020). An AES- based secure image retrieval scheme using random mapping and BOW in cloud computing. IEEE Access, 8, 61138-61147. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9046783

[3] Alasadi, A. H. H., & Wahid, S. A. (2016). Effect of Reducing Colors Number on the Performance of CBIR System. International Journal of Image, Graphics and Signal Processing, 8(9), 10. http://dx.doi.org/10.5815/ijigsp.2016.09.02

[4] J. Wang, Y. Yang, J. Mao, Z. Huang, C. Huang, W. Xu, ―CNN-RNN: A unified framework for multi-label image classification‖, in Proceeding of 2016 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR'16, Las Vegas, NV, USA, 2016, pp. 2285-2294. https://doi.org/10.48550/arXiv.1604.04573

[5] Xia, Z., Ma, X., Shen, Z., Sun, X., Xiong, N. N., & Jeon, B. (2018). Secure image LBP feature extraction in cloud-based smart campus. IEEE Access, 6, 30392-30401. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8375960

[6] Cheng, H., Zhang, X., Yu, J., & Zhang, Y. (2016). Encrypted JPEG image retrieval using block-wise feature comparison. Journal of Visual Communication and Image Representation, 40, 111-11. http://dx.doi.org/10.1016/j.jvcir.2016.06.016

[7] Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 99, 106883. https://doi.org/10.1016/j.asoc.2020.106883

[8] Bösch, C., Peter, A., Hartel, P., & Jonker, W. (2014, May). SOFIR: Securely outsourced Forensic image recognition. In 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2694-2698). IEEE. http://dx.doi.org/10.1109/ICASSP.2014.6854089

[9] Xia, Z., Xiong, N. N., Vasilakos, A. V., & Sun, X. (2017). EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Information Sciences, 387, 195-204. https://doi.org/10.1016/j.eswa.2022.117508

[10] Nayak, S. K., & Tripathy, S. (2021). SEPS: Efficient public-key-based secure search over outsourced data. Journal of Information Security and Applications, 61, 102932. https://doi.org/10.1016/j.jisa.2021.102932

[11] Cao, F., Sun, J., Luo, X., Qin, C., & Chang, C. C. (2021). Privacy-preserving inpainting for outsourced image. International Journal of Distributed Sensor Networks, 17(11), 15501477211059092. https://doi.org/10.1177/15501477211059092

[12] Li, J. S., Liu, I. H., Tsai, C. J., Su, Z. Y., Li, C. F., & Liu, C. G. (2020). Secure content-based image retrieval in the cloud with key confidentiality. IEEE Access, 8, 114940-114952. http://dx.doi.org/10.1109/ACCESS.2020.3003928

[13] Song, F., Qin, Z., Zhang, J., Liu, D., Liang, J., & Shen, X. S. (2020, December). Efficient and privacy-preserving outsourced image retrieval in public clouds. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). IEEE. http://dx.doi.org/10.1109/GLOBECOM42002.2020.9322134

[14] Wang, L., & Yu, H. (2021, June). A Secure Searchable Image Retrieval Scheme with Correct Retrieval Identity. In ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 8183-8187). IEEE. https://doi.org/10.1109/ICASSP39728.2021

[15] Anju, J., & Shreelekshmi, R. (2022). FSeCBIR: A Faster Secure Content-Based Image Retrieval for Cloud. Software Impacts, 11, 100224. https://doi.org/10.1016/j.simpa.2022.100224

[16] J. Z. Wang, J. Li, and G. Wiederhold, "SIMPLIcity: Semantics-Sensitive Integrated Matching for Picture Libraries," IEEE Transactions on Pattern Analysis and Machine Intelligence (**TPAMI**), vol. 23, no. 9, pp. 947-963, September 2001. https://doi.org/10.1016/j.simpa.2022.100224

[17] Abdulsada, A. I., & Ridha, H. S., & Younis, H. A. : Enabling a Secure Match over Private Image Collections
, Journal of Kufa for Mathematics and Com p u t e r, Vol.3, No.2, pp 25-36, Dec , 2016.
http://wang.ist.psu.edu/_jwang/test1.tar.