An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme

A. FRANCIS SAVIOUR DEVARAJ[1], G. MURUGABOOPATHI[1],
MOHAMED ELHOSENY[2], (Senior Member, IEEE), K. SHANKAR[3], (Member, IEEE),
KYUNGBOK MIN[4], HYEONJOON MOON[4], AND GYANENDRA PRASAD JOSHI[4]

[1]Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil 626128, India
[2]Faculty of Computers and Information, Mansoura University, Dakahlia Governorate 35516, Egypt
[3]Department of Computer Applications, Alagappa University, Karaikudi 630002, India
[4]Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea

Corresponding authors: Gyanendra Prasad Joshi (joshi@sejong.ac.kr) and Hyeonjoon Moon (hmoon@sejong.ac.kr)

ABSTRACT Due to the advanced growth in multimedia data and Cloud Computing (CC), Secure Image Archival and Retrieval System (SIARS) on cloud has gained more interest in recent times. Content based image retrieval (CBIR) systems generally retrieve the images relevant to the query image (QI) from massive databases. However, the secure image retrieval process is needed to ensure data confidentiality and secure data transmission between cloud storage and users. Existing secure image retrieval models faces difficulties like minimum retrieval performance, which fails to adapt with the large-scale IR in cloud platform. To resolve this issue, this article presents a SIARS using deep learning (DL) and multiple share creation schemes. The proposed SIARS model involves Adagrad based convolutional neural network (AG-CNN) based feature extractor to extract the useful set of features from the input images. At the same time, secure multiple share creation (SMSC) schemes are executed to generate multiple shares of the input images. The resultant shares and the feature vectors are stored in the cloud database with the respective image identification number. Upon retrieval, the user provides a query image and reconstructs the received shared image to attain the related images from the database. An elaborate experimentation analysis is carried out on benchmark Corel10K dataset and the results are examined in terms of retrieval efficiency and image quality. The attained results ensured the superior performance of the SIARS model on all the applied test images.

INDEX TERMS Image archival, secure image retrieval, deep learning, secret sharing scheme, multiple share creation.

I. INTRODUCTION

Information retrieval and archival becomes highly essential for recent progressive of multimedia data processing which analyzes the real-time information. Here, searching is a well-known process that is carried out via Internet. Image searching, or retrieval, is also very important topic in current industry. Recent IT models depends upon on global and local

The associate editor coordinating the review of this manuscript and approving it for publication was Hossein Rahmani.

features like color, texture, edges, spatial data, key points as well as salient patches. Users apply search engines for exploring images, videos and documents through Internet, under the application of Google, Bing, Yahoo and ASK are well-known search engines. A promising issue involved in search engines are the way of extracting features from wider amount of image data. Feature extraction as well as representation is composed with closer associations along with color point of view and orientation selection models of human visual system.

The traditional and general data retrieving depends upon keyword search that contains limitations like maximum requirement of manpower and dependency on personal point that provides poor simulation outcome. In order to overcome these disadvantages, CBIR method has been utilized [1]. CBIR is composed with models that focus on low level image features, for instance texture values, shape and color signature for retrieving images from image database on the QI that is deployed by [2]. The key factor of CBIR method is to retrieve images relevant to QI from images database [3]. CBIR applies the model of "query by example" that obtains same images by a description regarding the QI provided by a user, the CBIR system is operated by QI feature extraction, then the system explores the extracted features. Besides, feature vector is determined for attained features for QI, CBIR shows image is acquired from database with a vector, once the image is provided to CBIR, it process the feature vector and compares with vectors saved in the database, and images with maximum features similarity to QI would be retrieved.

Using the introduction of CC, protective data retrieval on the cloud has attained maximum concentration recently [4]. As it provides better convergence and financial savings, business and users lead to apply the CC for storage and manage the sensitive data, including photographic albums and personal health details. In order to assure the data confidentiality, the data encryption is carried out before saving in cloud. Hence, the classical encryption makes fundamental data task impossible, for instance, the IR of encrypted data. In cipher text case, how to accomplish effective retrieval of data at the time of securing customers details which is highly complex.

Presently, there are 3 major limitations that restricts the development of IR in the encrypted application. The primary issue is to analyze searching function of encrypted data and accomplish similar precision. Ultimately, a naive model is applied to download the cipher texts, and decrypt them, and explore the plaintext. Hence, it infers higher cost of bandwidth and processing. In order to report these problem, cryptographic models like homomorphic encryption [5] and multiparty processing that encrypts plaintext data and applicable for searching task in ciphertext. Therefore, the pre-defined models are considered with data confidentiality when compared with retrieving efficiency and expensive in real-time domains.

In contrast, some effective models like order-preserving encryption (OPE), randomized hash functions, and asymmetric scalar PE (ASPE) [6], have been applied extensively. Secondly, though it is a plaintext of encrypted data, it is not leaked from predefined models, some statistical data like request frequency of encrypted query is released from privacy of query user. It is a fact that, RAMs [7] is considered to be a solution to save the accessible patterns, however it is insufficient. Thirdly, the issue is that retrieving method of linear efficiency is not applicable as the searching time would enhance as the dataset is developed wider. Obviously,

protective data retrieval is frequently applied for documents saved in a cloud server.

Massive operations are used for accomplishing secured retrieval of encrypted images. Boolean search depends upon the single keyword which has been projected in symmetric key setting as well as public key setting [8]. As similarity search is realistic when compared to Boolean search, multi-keyword ranked search [9] is applied to develop search functions and enhance the resultant accuracy, in which every document is compared with index vector. Every element of a vector represents whether a keyword is present as term frequency (TF) inverse document frequency (IDF). Next, the k-nearest neighbor (kNN) is used by relating the cosine similarity with query vector and every index vector has linear efficiency. For improving the retrieving efficiency, index tree and related operations are developed. For instance, Sun *et al.* [10] provided a tree dependent searching model which develops index vectors of every document as MDB-tree. It reaches sublinear search efficiency by fixing the prediction threshold for index tree levels. Though a better prediction score could accomplish logarithmic searching efficiency, the final accuracy is reached simultaneously.

Additionally, Xia *et al.* [11] developed a KBB-tree from bottom-up method. The components of internal node vector have greatest measure of child node vectors. A "Greedy-Depth-First Search" technique is implemented for identifying k most relevant leaf nodes that is saved in an RList. When the correlation value among query vector as well as internal node vector is minimum than the measures of RList and subtree of internal node cannot be explored. Hence, it is highly applicable for accomplishing sublinear efficiency. Apart from this, few operations are developed for encrypted IR. In [12], a privacy-based face analysis is examined using Paillier homomorphic encryption (HE). The limitation of this method, the application of HE acquires expensive processing and communication.

Practically, Lu *et al.* [13] presented a secure CBIR method on the basis of feature and index randomization or min-Hash. Simultaneously, the working function is to compare HE and distance conserving randomization as deployed in [14]. Because of one-way as well as binary property of hash code, CBIR make use of hash function for feature encryption is effectual in large-scale database. Thus, access pattern has been exhausted in the predefined models. In order to resolve the problems involved, Weng *et al.* [15] remove some specific bits of hash code of QI. Finally, the cloud offers feasible candidates. However, a client is involved in comparing features of candidates and accomplish optimal outcome. Additionally, it is highly complex for generating hash codes which distributes uniformly in the feature space. Furthermore, using a vector space model, hand-based operations is highly applied for productive index structure. For illustration, Xia *et al.* [16] applies local-sensitive hash (LSH) for developing a pre-filter table, however a refinement of candidate tends in linear comparison. Yuan *et al.* [17] use k-means for creating an index tree. As k-means is not

a compete clustering method, it is predictable to produce an index tree of skewed hierarchies. Consequently, as the uneven depth is present in various portions of index tree, the searching efficiency should be sublinear.

On the other hand, the predetermined models are based on encrypted feature; the protective retrieving mechanism depends upon encrypted images. It is developed for extensively applied JPEG image. For sample, Zhang and Cheng [18] first utilizes DC histogram that is conserved in encrypted image as a feature and make use of AC histogram as well as a novel block feature for retrieving task. Hence, the effectiveness of linear comparison cannot be accepted. Thus, the development of secure index tree is highly essential.

In recent days, deep learning models like convolutional neural networks (CNN) become popular due to the following merits. The concept of CNN is inspired from the fact that is has the ability of learning the related features from the image. Besides, the weight sharing of the CNN finds beneficial. Also, the CNN is effective over NN in terms of memory and complexity. At the same time, the CNN outperform the NN on traditional image recognition tasks and many other tasks [29]–[32].

This article introduces a new secure image archival and retrieval system (SIARS) using deep learning and multiple share creation schemes. The proposed model involves Adagrad based convolutional neural network (AG-CNN) based feature extractor to extract the feature vectors of the input images. The AG-CNN includes a VGGNet-16 model and Adagrad optimizer to tune the hyperparameters. Adagrad is found to be an effective hyperparameter tuning technique since it avoids manual tuning of learning rate. Besides, it provides quick convergence and high reliability. It is also not highly sensitivity to the master step size. Then, a secure multiple share creation (SMSC) process takes place to generate multiple shares for every image. Besides, the Manhattan distance measure is utilized in the query matching process. A series of experimental analysis is carried out on Corel10K database and the results are investigated in terms of different evaluation measures.

The remaining section of the article is arranged as follows. Section 2 explains the presented SIARS model and the corresponding experimental analysis takes place in section 3. At last, the conclusions are obtained in section 4.

II. THE PROPOSED MODEL

Fig. 1 defines the detailed function of the SIARS method. The figure states that the SIARS model involves a set of subprocesses namely AG-CNN based image archival and retrieval process, SMSC process and query matching process. Initially, the image in the training set undergoes feature extraction process by the use of AG-CNN model, which incorporates VGG-16 architecture and the hyperparameters of this model is tuned using Adagrad optimizer. At the same time, the SMSC process produces a set of n shares for every RGB color space of the training images. Then, secure multiple share creation scheme [21] to shares are generated.

When a user provides a QI, the SIARS model extracts the feature vectors and undergoes a similarity measurement using Manhattan distance. Then, the secret shares of the adjacent feature vectors of respective images are forwarded to the user. Finally, the user performs the reconstruction process and attains the relevant images in a secured way.

A. AG-CNN BASED IMAGE ARCHIVAL AND RETRIEVAL PROCESS

In this section, the AG-CNN is applied to extract the necessary feature vectors to carry out the retrieval process in an effective way. TO perform this, the AG-CNN model makes use of VGGNet 16 and Adagrad optimizer, which are discussed in the following subsections.

1) CONVOLUTIONAL NEURAL NETWORK (CNN)

CNN model is considered to be supervised learning method which contains maximum benefits and minimum number of parameters [19]. It contains robust training speed than deep ANN. It is pointed that, it is comprised of vital benefits in image segmentation, prediction, as well as classification. The feature map of first layer is attained by convolving the input, and 6 convolution kernels were applied.

Every convolution kernel contains a size of 5×5 and stride as 1. The size of a feature map can is obtained under the application of given expression:

$$n_f = \frac{n_i + 2p - f}{s} \tag{1}$$

where n_f shows the size of a feature map; n_i denotes the input size; p refers the padding value; f signifies the kernel size and s shows the stride value. The fundamental expression of a convolution task is provided in the following:

$$a^l = \delta \left(W^l a^{l-1} + b^l \right) \tag{2}$$

where a^l denotes the output of lth convolution layer; w^l represents convolution kernel of lth convolution layer; a^{l-1} defines the result of $l-1$ th convolution layer; b^l indicates bias of lth convolution layer; δ shows the activation function of lth convolution layer. In case of sub-sampling, pooling operation has been applied. The size of pooling kernel is always 2×2 and stride is 2 for pooling task. Mostly, activation functions such as sigmoid, tanh, and ReLU are frequently applied. The features obtained using convolutional layer and transmit it to the fully connected (FC) layer at the final layer. Besides, a CNN has diverse layers with definite features like convolutional layers, activation layers, pooling layers, FC layers as well as SoftMax layers.

The Convolution layer is composed of a filter that convolves over the width and height of input data. On the other side, the result of a convolutional layer is accomplished under the performance of dot product among the filter weight content as well as unique location of an input image. As a result, it provides 2D activation map that further gives responses of filter at a spatial position. There are different types of parameters like, count of filters, filter size, weight
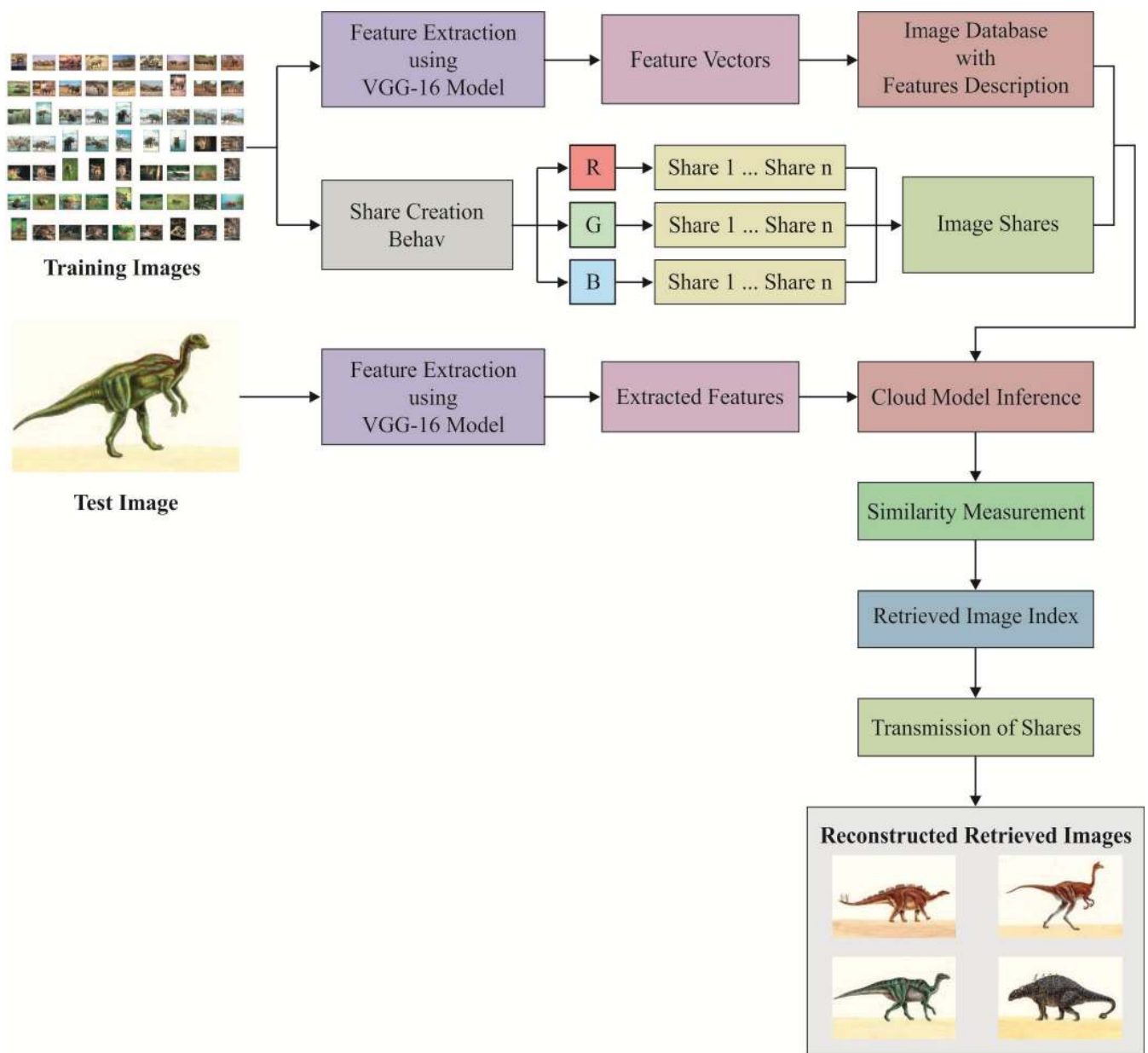
FIGURE 1. The Overall Process of Proposed SIARS Framework.

contents, stride, and padding. Generally, polling layer aims at eliminating over-fitting and using non-linear down-sampling on activation maps it minimizes the dimension as well as the complexity of the process and enhances the computation.

Diverse attributes are employed in this layer namely; filter size and stride, while padding has not been applied in pooling as it is not focused in dimension reduction. Also, it is used for all input channel. Similarly, the count of output and input channels would be symmetric. Additionally, 2 various pooling layers are utilized such as max and average pooling. The fundamental task of pooling layer is same as convolutional layer. The major variation is that, instead of applying a dot product of input and a filter, higher neighboring value can be applied for unique position in the input image. It is accomplished using channel present in

the input. In Average pooling layer, the average values are employed from all the positions of the input image.

The FC layer is also named as hidden layer which is applied in normal NN. In prior to this, input array is transformed into a 1D vector with the help of a flattening layer. As per the name, in a FC layer, every node from the input is linked with each other in the output. This kind of activation function has been used in the output layer of CNN for depicting a categorical distribution among labels which provides the possibilities of all inputs that belong to a label.

2) VGGNET-16 ARCHITECTURE
VGG16 is defined as CNN method which has been developed by K. Simonyan and A. Zisserman from the University of Oxford in "Very Deep Convolutional Networks for

Large-Scale Image Recognition'' [20]. VGGNet is assumed to be a deep CNN (DCNN) is operated on the link over depth and CNN performance. It is effective in building a convolution of 16 to 19 deep layers NN by stacking 3∗3 tiny convolution kernels as well as 2∗2 higher pooling layers in a repeated manner. When compared to existing state of the art network structure, VGGNet acquires an important error rate drop and placed in the second position in ILSVRC 2014 competing category as well as first place in placing project. The 3∗3 convolution kernels as well as 2∗2 pooling cores were used in VGGNet for improving the working function.

As the performance of network is reduced slowly, then the attributes used also decreases the function. Hence, training consumes maximum time as it has processing complexity. VGGNet is composed with 5 sections of convolution, where all sections have 2–3 convolution layers are connected to the end of a maximum pool and results in the image size reduction. Every portion contains similar count of convolution kernels, and contiguous segments are composed of convolution kernels: 64-128-256-512-512. Actually, the structures of convolution layers have various identical 3∗3 convolutions stacked in a combined manner. The impact of two 3∗3 convolution layers is equal to 5∗5 convolution layers, which means that single pixel is related with the adjacent 5∗5 pixels, while the size of receptive field is 5∗5. However previous models have minimum parameters and higher nonlinear transformations when compared with alternate models, thus CNN is applicable to learn the features. The predefined methods can apply a ReLU activation function thrice whereas alternate modules are employed in single iteration. Fig. 2 illustrates the VGGNet network structure for every stage and number of parameters, with better function from 11th layer of a system up to 19th layer of the network. Also, VGGNet16 involves a set of 16 weight layers.

3) HYPERPARAMETER OPTIMIZATION OF CNN USING AG MODEL

Hyper-parameter is a type of parameter which has to be selected manually in prior to train the method. The term 'hyper-' is applied to distinguish hyper-parameter to the parameter which has been altered independently using optimization models at the time of training. The learning rate shows the access of parameter (θ) to be followed from opposite direction of a gradient estimate (g). But, the hyper-parameter would be complex to set, when it is fixed it too small, then parameter update would become slow and it takes maximum duration for achieving reasonable loss while it is fixed it too large, then the parameter would be moved across the function and it does not reach the acceptable loss. However, high-dimensional non-convex nature of NN optimization tends to develop diverse sensitivity for all dimensions. The learning rate might be minimum for some dimension and might be maximum in alternate dimension. Hence, the traditional approach is applied to reflect the problem for DNN which is an AdaGrad algorithm.

Adagrad is defined as gradient-based optimization which applies learning rate to parameters, and process only small updates for parameters related with continuously existing features, whereas larger updates for parameters associated with rare features. For this sake, it is applicable to resolve sparse data. Adagrad is suitable to enhance the efficiency of SGD and utilized for training large-scale NN. Also, Adagrad optimizer is termed as gradient centric optimization method which is highly suitable for sparse gradients. Then, a learning rate has been applied according to the parameters in automated manner.

$$\Theta_{t+1} = \Theta_t - \frac{\alpha}{\sqrt{\varepsilon + \sum g_t^2}} \odot g_t \qquad (3)$$

The fundamental function applied for parameter enhancement is provided in Eq. (3) where θ_t denotes the parameter at time t, α shows the learning rate, g_t implies gradient estimate, and $\odot$ refers element wise multiplication.

B. SECURE MULTIPLE SHARE CREATION (SMSC) PROCESS

The pixel values of an actual image were extracted and the RGB values are defined in the form of matrix (Rm, Gm, Bm) [21]. The matrix size is identical to the size of input image (P∗Q). Hence, actual pixel score of an input image is determined as

$$Pixel = \sum R + G + B \qquad (4)$$

where, *pixel* refers to the sum of the total values of the Rm, Gm and Bm. Every pixel exist in the input image can occurs in the form of *n* transformed ways, known as shares. All the shares comprise a set of sub-pixels of RGB image. The R, G, B shares depends upon the advanced pixel values in the RGB image. A share of RGB is individually represented by Rs, Gs and Bs and it is calculated as,

$$R_s = \int_1^k lim_{k \rightarrow 1ton} R_{ab} \qquad (5)$$

$$G_s = \int_1^k lim_{k \rightarrow 1ton} G_{ab} \qquad (6)$$

$$B_s = \int_1^k lim_{k \rightarrow 1ton} B_{ab} \qquad (7)$$

where, a and b indicates the position of the matrix, $R_s, G_s and B_s$ denotes the shares of RGB, $R_{ab}, G_{ab} and B_{ab}$ are the components of the image pixels. The RGB pixel values are obtained from the actual image and retained as individual matrices. Then, the shares are produced depending upon the partitioning of an image into distinct portions. The SMSC model aims to encrypt the image into a number of meaningless share images. The share does not define any useful information unless all the shares are integrated together [33], [34].

In prior to creating shares, the subsequent operation is carried out on the XR1 and XR2 matrices and the key matrix K_m Generated randomly.

$$XR_1 = 128 - B_{M1}$$
$$XR_2 = B_{M2} \qquad (8)$$

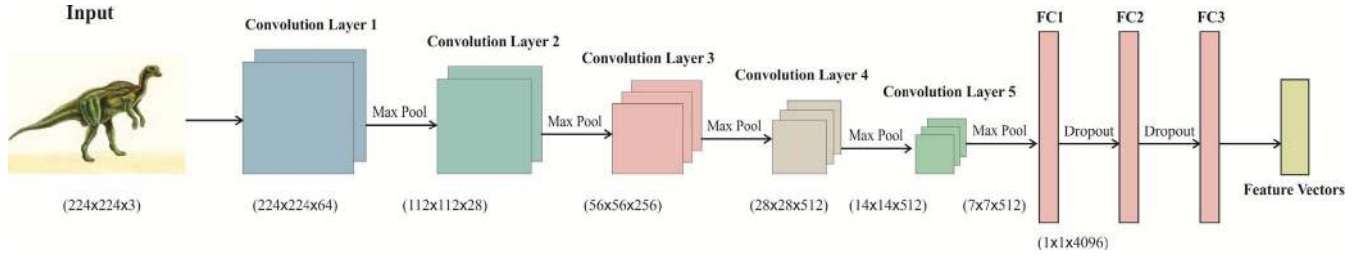**FIGURE 2.** The Layered Architecture of VGG-16 Model.

The red band shares are produced by XORing the basic and key matrices as given below.

$$Rs1 = XR_1 \oplus K_M$$
$$Rs2 = XR_2 \oplus XR_1$$
$$Rs3 = XR_2 \oplus Rs_1$$
$$Rs4 = Rs1 \oplus R \qquad (9)$$

During the reconstruction operation, many shares are integrated for generating the original image which is illustrated as [21],

$$R = Rs1 \oplus Rs2 \oplus Rs3 \oplus Rs4 \oplus Rs4 \oplus K_M$$
$$G = Gs1 \oplus Gs2 \oplus Gs3 \oplus Gs4 \oplus Gs4 \oplus K_M$$
$$B = Bs1 \oplus Bs2 \oplus Bs3 \oplus Bs4 \oplus Bs4 \oplus K_M \qquad (10)$$

The shares are reconstructed, and the encryption and decryption process were employed on color band of reformed share. Every color band image is partitioned into blocks earlier to encryption and decryption processes. From the above processes, many shares are generated, and encryption process is applied on the share and the blocks were segmented as 4∗4 as block size.

C. QUERY MATCHING PROCESS

A feature vector for query image QR is signified as $f_{QR} = (f_{QR1}, f_{QR2}, \ldots \ldots f_{QRLg})$ is achieved behind the feature extraction process [23]. Similarity all images in the database is illustrated with feature vector $f_{DAB_j} = (f_{DAB_{j1}}, f_{DAB_{j2}}, \ldots \ldots f_{DAB_{jLg}}); j = 1, 2, \ldots \ldots, |DAB|$. An aim is to choose n optimal images that resemble the QI. It is contains chosen of n top corresponding images with evaluating the distance among the QI and the image in the database $|DAB|$. For matching the images is utilizing 4 various similarity distance metrics as following

Manhattan distance is a parameter that measures the distance among 2 points is the amount of the accurate variations of Cartesian coordinates. It is a simple method that defines the entire sum of variations among the x as well as y-coordinate points. Assume it has 2 points namely A and B. When it is required to determine the Manhattan distance among them, now it is added with absolute x-axis as well as y-axis variation; it represents that it is needed to determine how these 2 points A and B are altering in X-axis as well as

Y- axis. Mathematically, Manhattan distances among 2 points are evaluated along axes at right angles.

A plane with p1 at (x1, y1) and p2 at (x2, y2).

$$Manhattan \, distance = |x1 - x2| + |y1 - y2| \qquad (11)$$

Manhattan distance metric is also called as Manhattan length, rectilinear distance, L1 distance or L1 norm, city block distance, Minkowski's L1 distance, and city block distance.
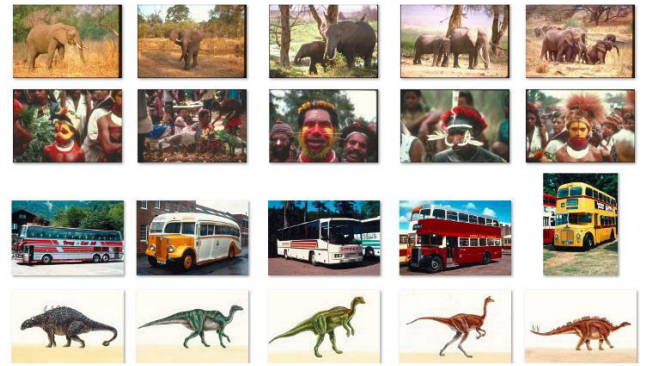
FIGURE 3. The Sample Test Images.

III. PERFORMANCE VALIDATION

The performance of the presented SIARS model has been tested using Corel10K dataset. Fig. 3 shows some sample test images. Corel-10k dataset [24] is composed of 100 classes, and there are 10,000 images from various categories like sunset, beach, flower, building, car, horses, mountains, fish, food, door, and so on. Every class is composed of 100 images under the size 192 × 128 or 128 × 192 in the JPEG format.

A. EVALUATION MEASURES

A set of two measures namely precision and recall were applied to assess the retrieval efficiency of the projected model. To attain maximum retrieval performance, the values of these measures should be high. Besides, correlation coefficient (CC) factor, mean square error (MSE), and peak signal to noise ratio (PSNR) are used [21].

1) CORRELATION COEFFICIENT FACTOR

In order to examine the correlation involving 2 nearby pixels throughout plain-image and ciphered image. At the initial

stage, select 1000 pairs related with 2 adjacent pixels from an image. Followed by, process the correlation coefficient of one set by the consecutive equations,

$$G(p) = \frac{1}{F_p} \sum_{l=1}^{F_p} (p_l - M(p))^2 \tag{12}$$

$$M(p) = \frac{1}{F_p} \sum_{l=1}^{F_p} P_l \tag{13}$$

$$CON(p,q) = \frac{1}{F_p} \sum_{l=1}^{F_p} ((p_l - M(p)) * (q_l - M(q))) \tag{14}$$

$$W(p,q) = \frac{CON(p,q)}{\sqrt{M(p) * M(q)}} \tag{15}$$

where, $W(p,q)$ defines the coefficient, $M(p)$ and $M(q)$ shows the mean value of P_l and q_l and values are $\neq 0.P_l$ and q_l means the 2 adjacent pixel values; F_p denotes the count of pairs (p,q).

2) MEAN SQUARE ERROR (MSE)

The MSE is defined as an average square of an error in specific images that has been formulated as,

$$MSE = \frac{1}{W * L} \left(\sum_{p=1}^{p} \sum_{q=1}^{q} (OI_{pq} - EI_{pq})^2 \right) \tag{16}$$

where, W implies width of actual image, L denotes length of original image, p and q defines the row and column value of a pixel, OI implies actual image pixel and EI means decrypted image pixel value.

3) PEAK SIGNAL TO NOISE RATIO (PSNR)

The PSNR is described as the ratio among the higher possible power of the signal to the power of corrupted noise.

$$PSNR = 20 * log_{10} \left(255/\sqrt{MSE} \right) \tag{17}$$

where, MSE defines the mean square error value of an image.

B. RESULTS ANALYSIS

A sample visualization of the results offered by the SIARS model is shown in Fig. 4. A sample test image "Elephant" is depicted in Fig. 4a and relevant images are demonstrated in Fig. 4b. From the figure, it clearly exhibits that the relevant images are retrieved from the database in an effective manner.

Fig. 5 provides the retrieval results offered by the SIARS model with respect to precision and recall. On the applied sample 'Buses' image, the SIARS model has achieved a maximum precision of 0.98 and recall of 0.79 respectively. Similarly, on the applied 'mountains' image, the SIARS model has attained a higher precision of 0.86 and recall of 0.83. Likewise, on the applied 'Beach' image, the SIARS model has resulted in a maximum precision of 0.93 and recall of 0.84. Simultaneously, on the given sample 'Elephants'
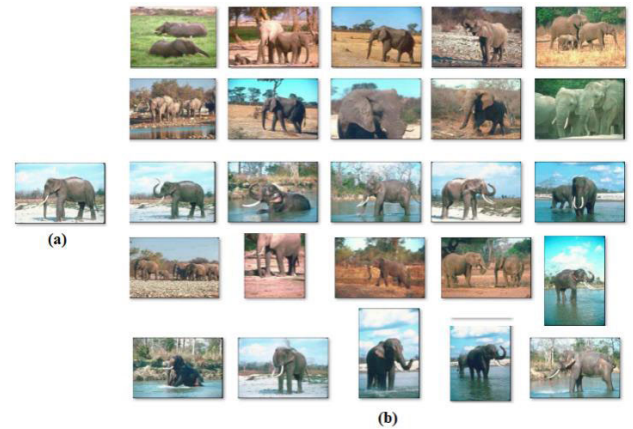
FIGURE 4. (a) Query Image. (b) Retrieved Images.
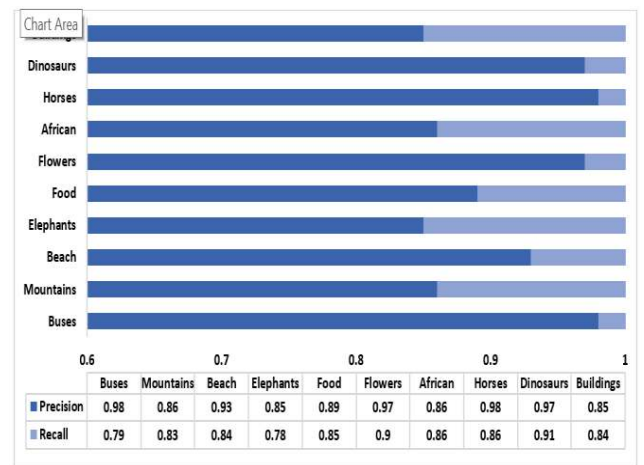
FIGURE 5. The Precision and Recall analysis of SIARS Model.

	Buses	Mountains	Beach	Elephants	Food	Flowers	African	Horses	Dinosaurs	Buildings
Precision	0.98	0.86	0.93	0.85	0.89	0.97	0.86	0.98	0.97	0.85
Recall	0.79	0.83	0.84	0.78	0.85	0.9	0.86	0.86	0.91	0.84

image, the SIARS method has attained higher precision of 0.85 and recall of 0.78 correspondingly. On the other hand, on the applied sample 'Food' image, the SIARS model has accomplished a better precision of 0.89 and recall of 0.85 respectively. At the same time, on the applied sample 'Flowers' image, the SIARS method has reached optimal precision of 0.97 and recall of 0.90 correspondingly. Additionally, on the applied sample 'African' image, the SIARS model has attained a better precision of 0.86 and recall of 0.86 respectively. Thus, on the applied sample 'Horses' image, the SIARS model has accomplished a higher precision of 0.98 and recall of 0.86 correspondingly. Similarly, on the applied sample 'Dinosaurs' image, the SIARS approach has reached a better precision of 0.97 and recall of 0.91 respectively. In line with this, on the applied sample 'Buildings' image, the SIARS model has attained a higher precision of 0.85 and recall of 0.84 correspondingly.

Fig. 6-7 shows the average precision analysis of the SIARS model with the existing methods [25], [26] on the applied dataset. The experimental values indicated that the IR-MCM
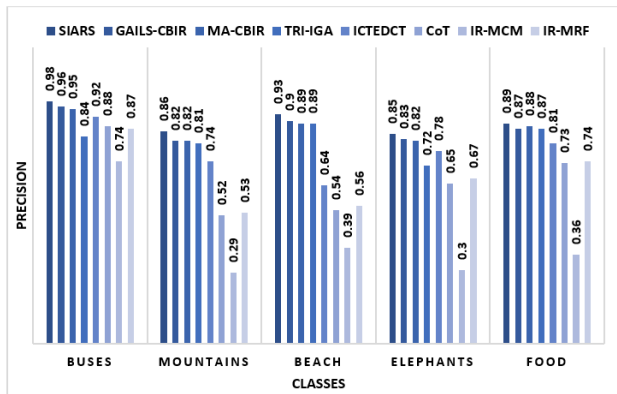
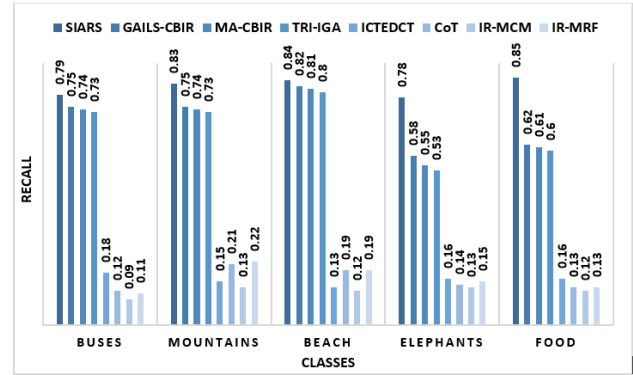**FIGURE 6.** The Precision analysis of SIARS Model-I.

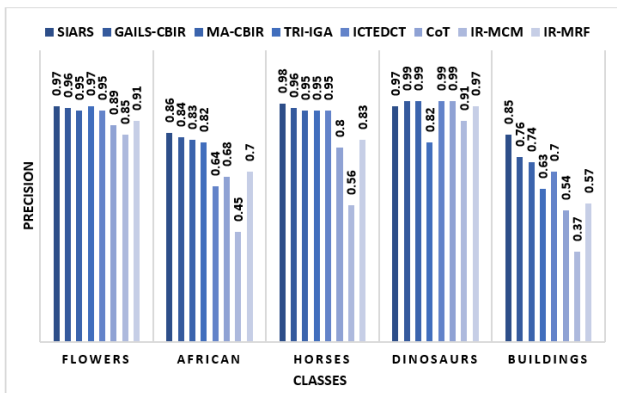**FIGURE 8.** The Recall analysis of SIARS Model-I.

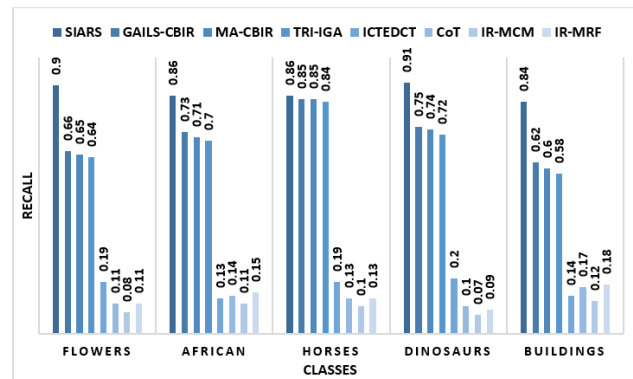**FIGURE 7.** The Precision analysis of SIARS Model-II.

FIGURE 9. The Recall analysis of SIARS Model-II.

method is the ineffective retrieval model which has shown minimum precision value compared to existing models. At the same time, it is noticed that the CoT and IR-MRF models have exhibited near identical and better performance than IR-MCM mode, but failed to outperform other methods. In the same way, the ICTEDCT model has depicted effective performance over CoT, IR-MCM and IR-MRF by offering moderate precision value.

In line with, even better retrieval performance is provided by the TRI-IGA model by exhibiting high precision value over the earlier models. It is also observed that the GAILS-CBIR and MA-CBIR models have showcased superior results over all the earlier models by attaining higher precision value. Though they illustrated better performance over the precious models, it does not outperform the proposed SIARS model. The proposed SIARS model has shown extraordinary results over the compared methods by offering maximum precision value on all the applied images.

Fig. 8-9 implies the average recall analysis of SIARS model with the traditional models on the applied dataset. The experimental values represented that the IR-MCM approach is worst retrieval model that has exhibited lower recall value

than previous models. Meanwhile, it is pointed that the CoT and IR-MRF methodologies have showed closer identical and good performance when compared with IR-MCM model, but failed to perform well than alternate methods. Along with that, the ICTEDCT technology has illustrated efficient performance than CoT, IR-MCM and IR-MRF by providing better recall value. Likewise, moderate retrieval performance is offered by the TRI-IGA methods by representing maximum recall value than earlier models. Also, it is monitored that the GAILS-CBIR and MA-CBIR methodologies have showcased qualified results when compared with previous technologies by accomplishing maximum recall value.

Table 1 provides a visualization study of the results attained by the SMSC model on a set of two sample images. The table shows that the input image is divided into multiple shares and the reconstruction of the generated shares results to the generation of the final image.

Table 2 and Fig. 11 provides the results analysis of the SIARS model in terms of MSE, PSNR and CC with existing methods [27], [28]. The experimental values considered that the SIARS model has indicated effective reconstruction performance over the compared methods. On comparing the results offered by the MSCS with BMOGA and RCP models, the maximum MSE value is offered by the RCP model

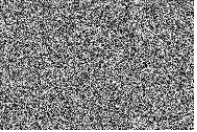**TABLE 1.** The Results Analysis of MSCS in terms MSE, PSNR and CC.
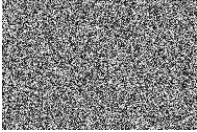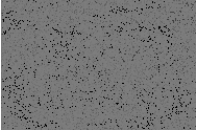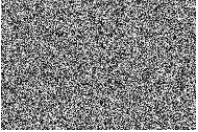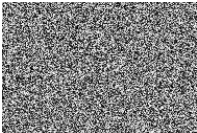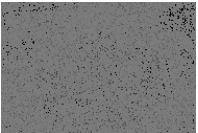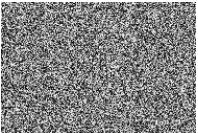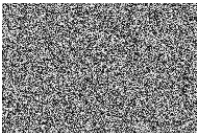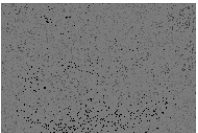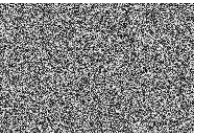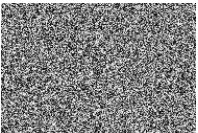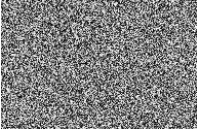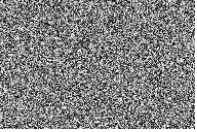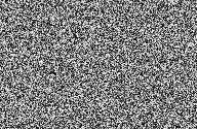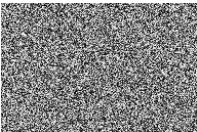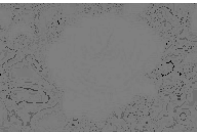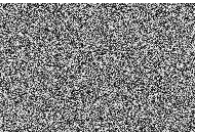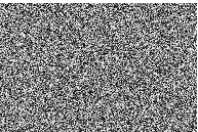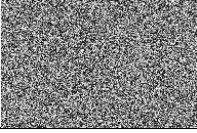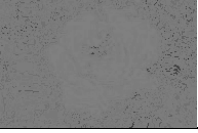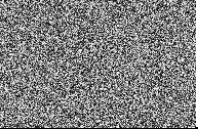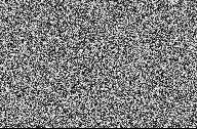
TABLE 2. Result Analysis of SMSC with other Methods.

Input Image	SMSC			BMOGA			RCP		
	MSE	PSNR	CC	MSE	PSNR	CC	MSE	PSNR	CC
	0.0865	58.76	1	0.1243	57.18	0.988	3.1986	43.08	0.967
	0.1083	57.78	1	0.1387	56.71	0.971	2.9854	43.38	0.921

whereas slightly lower MSE is attained by the BMOGA model. However, the proposed MSCS model has attained minimum MSE value on the applied images. Similarly, on assessing the results in terms of PSNR value, the maximum PSNR value is achieved by the proposed model over the compared methods.

Likewise, on comparing the results in terms of CC, the proposed method has exhibited effective performance by attaining maximum CC of 1. At the same time, the existing BMOGA and RCP models have reached to minimum CC values. These above-mentioned experimental values ensured that the SIARS model has attained effective retrieval
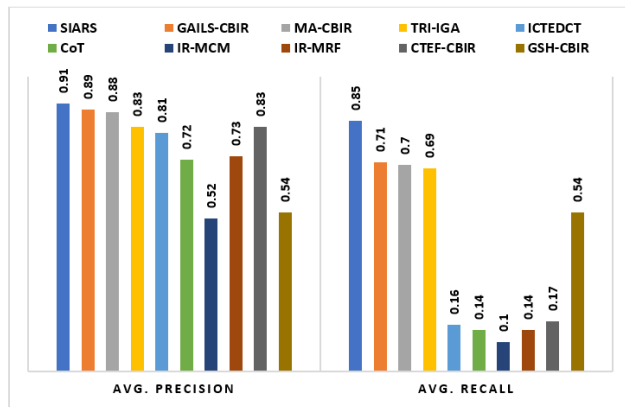
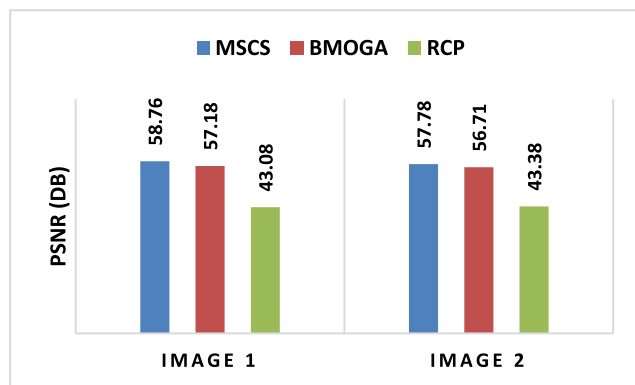**FIGURE 10.** The Average precision and recall analysis of SIARS model.

FIGURE 11. The PSNR analysis of SMSC model with existing methods.

performance with maximum security over the compared methods.

IV. CONCLUSION

This article has introduced a new SIARS model using DL and SMSC concepts. The proposed SIARS model involves a set of subprocesses namely AG-CNN based image archival and retrieval process, SMSC process and query matching process. The AG-CNN includes a VGGNet-16 model and Adagrad optimizer to tune the hyperparameters. Then, a SMSC process takes place to generate multiple shares for every image and ECC. Besides, the Manhattan distance measure is utilized in the query matching process. A series of experimental analysis is carried out on Corel10K database and the experimental values indicated het betterment of the SIARS model. The experimental results ensured the effective performance of the SIARS model by attaining maximum average precision of 0.91 and recall of 0.85. These values proved that the SIARS model is found to be an effective secure image retrieval model. In future, the performance of the SIARS model is improvised by the use of light weight cryptographic techniques.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors.

REFERENCES

[1] V. S. Tseng, J.-H. Su, J.-H. Huang, and C.-J. Chen, "Integrated mining of visual features, speech features, and frequent patterns for semantic video annotation," *IEEE Trans. Multimedia*, vol. 10, no. 2, pp. 260–267, Feb. 2008.

[2] T. Kanimozhi and K. Latha, "A Meta-heuristic optimization approach for content based image retrieval using relevance feedback method," in *Proc. World Congr. Eng.*, London, U.K., 2013, pp. 1–6.

[3] G. Carneiro, A. B. Chan, P. J. Moreno, and N. Vasconcelos, "Supervised learning of semantic classes for image annotation and retrieval," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 3, pp. 394–410, Mar. 2007.

[4] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Comput.*, vol. 16, no. 1, pp. 69–73, Jan. 2012.

[5] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, Bethesda, MD, USA, 2009, pp. 169–178.

[6] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in *Proc. 35th SIGMOD Int. Conf. Manage. Data (SIGMOD)*, Providence, RI, USA, Jul. 2009, pp. 139–152.

[7] P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage," in *Proc. 15th ACM Conf. Comput. Commun. Secur. (CCS)*, vol. 8, Oct. 2008, pp. 139–148.

[8] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer, 2004, pp. 506–522.

[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[10] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 3025–3035, Nov. 2014.

[11] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Feb. 2016.

[12] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Tof, "Privacy-preserving face recognition," in *Privacy Enhancing Technologies* (Lecture Notes in Computer Science), vol. 5672. Berlin, Germany: Springer, 2009, pp. 235–253.

[13] W. Lu, A. L. Varna, A. Swaminathan, and M. Wu, "Secure image retrieval through feature protection," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Taipei, Taiwan, Apr. 2009, pp. 1533–1536.

[14] W. Lu, A. L. Varna, and M. Wu, "Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization," *IEEE Access*, vol. 2, pp. 125–141, 2014.

[15] L. Weng, L. Amsaleg, and T. Furon, "Privacy-preserving outsourced media search," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 10, pp. 2738–2751, Oct. 2016.

[16] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," *Inf. Sci.*, vol. 387, pp. 195–204, May 2017.

[17] J. Yuan, S. Yu, and L. Guo, "SEISA: Secure and efficient encrypted image search with access control," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Hong Kong, Apr. 2015, pp. 2083–2091.

[18] X. Zhang and H. Cheng, "Histogram-based retrieval for encrypted JPEG images," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process. (ChinaSIP)*, Jul. 2014, pp. 446–449.

[19] M. Kouzehgar, Y. K. Tamilselvam, M. V. Heredia, and M. R. Elara, "Self-reconfigurable façade-cleaning robot equipped with deep-learning-based crack detection based on convolutional neural networks," *Autom. Construct.*, vol. 108, Dec. 2019, Art. no. 102959.

[20] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*. [Online]. Available: http://arxiv.org/abs/1409.1556

[21] K. Shankar and P. Eswaran, "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography," *China Commun.*, vol. 14, no. 2, pp. 118–130, Feb. 2017.

[22] S. U. Nimbhorkar and L. G. Malik, "A survey on elliptic curve cryptography (ECC)," *Int. J. Adv. Stud. Comput., Sci. Eng.*, vol. 1, no. 1, p. 1, 2012.

[23] P. E. Black, "Manhattan distance," in *Dictionary of Algorithms and Data Structures*. Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST). Accessed: Feb. 2020. [Online]. Available: https://www.nist.gov/dads/HTML/manhattanDistance.html

[24] G.-H. Liu. *Corel-10k Dataset*. Accessed: May 27, 2020. [Online]. Available: http://www.ci.gxnu.edu.cn/cbir/Dataset.aspx

[25] M. K. Alsmadi, "An efficient similarity measure for content based image retrieval using memetic algorithm," *Egyptian J. Basic Appl. Sci.*, vol. 4, no. 2, pp. 112–122, Jun. 2017.

[26] B.-H. Yuan and G.-H. Liu, "Image retrieval based on gradient-structures histogram," *Neural Comput. Appl.*, vol. 32, pp. 11717–11727, Jan. 2020.

[27] H. M. Pandey, "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography," *Future Gener. Comput. Syst.*, vol. 111, pp. 213–225, Oct. 2020.

[28] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *J. Elect. Comput. Eng.*, vol. 2012, pp. 1–14, Mar. 2012.

[29] I. V. Pustokhina, D. A. Pustokhin, J. J. P. C. Rodrigues, D. Gupta, A. Khanna, K. Shankar, C. Seo, and G. P. Joshi, "Automatic vehicle license plate recognition using optimal K-means with convolutional neural network for intelligent transportation systems," *IEEE Access*, vol. 8, pp. 92907–92917, 2020.

[30] K. Shankar, Y. Zhang, Y. Liu, L. Wu, and C.-H. Chen, "Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification," *IEEE Access*, vol. 8, pp. 118164–118173, 2020.

[31] R. J. S. Raj, S. J. Shobana, I. V. Pustokhina, D. A. Pustokhin, D. Gupta, and K. Shankar, "Optimal feature selection-based medical image classification using deep learning model in Internet of medical things," *IEEE Access*, vol. 8, pp. 58006–58017, 2020.

[32] V. Porkodi, A. R. Singh, A. R. W. Sait, K. Shankar, E. Yang, C. Seo, and G. P. Joshi, "Resource provisioning for cyber–physical–social system in cloud-fog-edge computing using optimal flower pollination algorithm," *IEEE Access*, vol. 8, pp. 105311–105319, 2020.

[33] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan, "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique," *J. Ambient Intell. Hum. Comput.*, vol. 11, pp. 1821–1833, Dec. 2018.

[34] K. Shankar and P. Eswaran, "A new k out of n secret image sharing scheme in visual cryptography," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Jan. 2016, pp. 1–6.

• • •