ISSN No:-2456-2165

Bag-of-Encrypted-Words for Cloud-Based Substance-Driven Image Retrieval (BOEW-SCIR)

Dr. G. Amudha M.E, Ph.D[1]. (Professor); Aadhithan. P[2] (UG Scholar); Mano. S[3] (UG Scholar)
[1]Computer Science and Business Systems, R.M.D. Engineering College
[2]Computer Science and Business Systems, R.M.D. Engineering College
[3]Computer Science and Business Systems, R.M.D. Engineering College

Abstract:- With the proliferation of digital images, there has been considerable research into Content-based Image Retrieval (CBIR) techniques. Typically, CBIR services demand substantial computational and storage resources, making it advantageous to outsource these services to cloud servers equipped with abundant resources. However, the challenge arises in ensuring privacy, given the inherent lack of complete trust in cloud servers. In here, we introduce a delegated CBIR approach adapted from a book BOEW model. Our method involves encrypting images through hue value replacement, block and intra-block pixel permutation. Subsequently, cloud server calculates regional histograms from these protected image blocks, binds and employs the resulting cluster centers as encrypted viewable words.

It is this approach allows us to construct a Bag-of-Encrypted-Words (BOEW) model, representing each hue as a feature vector—specifically, a generalized histogram of the encrypted viewable words. To measure the resemblance between images, we utilize the Manhattan space between feature vectors on the cloud server. Experimental output and a security analysis of our proffered scheme illustrate its search precision and security.

I. INTRODUCTION

The global landscape has experienced a rapid evolution in imaging technologies, encompassing a surge in digital cameras, advancements in medical imaging equipment, proliferation of smartphones, and more. Consequently, there has been a substantial escalation in the quantity of digital images. Methodically to retrieve similar images rapidly from huge amount of images, extensive practical Content-based Image Retrieval (CBIR) methods have been created. Nonetheless, a conventional image database is often excessively large, comprising millions of images, each potentially exceeding 40 megabytes [1]. Consequently, providing Content-Based Image Retrieval (CBIR) services typically involves substantial storage and computational resources. The allure of outsourcing CBIR services to a cloud server becomes evident in light of these demands. This approach allows the image owner to avoid the necessity of local image database storage and enables efficient retrieval of desired images from the cloud server [2].

➢ *The Fundamental Contributions can be Outlined as:*

- Our approach involves encrypting images in blocks, ensuring that secure and relevant local features can be directly extracted from these encrypted blocks. The utilization of the k-means clustering algorithm is employed to generate encrypted visual words. Subsequently, final feature vectors, also encrypted, are constructed using these visual words. The similarity between these feature vectors can be directly measured using Euclidean or Manhattan distance. The introduced Blockwise Encrypted Image Processing (BOEW) model stands as a promising solution in the field of encrypted image processing.
- In our case study, we suggest encrypting images through a combination of color value substitution, block permutation, and intra-block pixel permutation. This specially crafted encryption method enables the extraction of secure local histograms directly from the encrypted images on the cloud server side. The construction of indices can also be efficiently executed by the cloud server. When compared to methods employing secure global histograms [3], [4], our approach demonstrates significantly improved retrieval accuracy.

Section 2 explores related works, Section 3 presents the technical overview, and Section 4 details the proposed scheme design. The security analysis is covered in Section 5, experiments and results in Section 6, concluding with final remarks in Section 7.

II. RELATED WORKS

CBIR techniques, studied for over twenty years, demonstrate maturity in numerous real-world applications JOURNAL OF L

CBIR techniques, studied for over twenty years [5], [6], [7], [8], showcase maturity in practical applications. Despite this, direct cloud outsourcing is hindered by privacy concerns. Protecting image features is essential to prevent unintended information leakage about image contents.

Searchable encryption (SE) facilitates cloud storage of encrypted data with support for data search over the ciphertext domain [9]. While many SE schemes are

ISSN No:-2456-2165

tailored for text documents [10], [11], [12], Lu et al. introduced the first privacy-preserving CBIR scheme using visual words and Jaccard distance for similarity measurement [13]. They explored image feature protection techniques, including bitplane randomization and random projection [14]. Lu et al. compared these methods with homomorphic encryption, highlighting computational and communication resource differences [15]. Yuan et al. employed local sensitive hashing for secure similarity search, revealing social connections between image owners [16]. Xia et al. proposed a CBIR scheme based on SIFT and EMD, utilizing linear transformation for privacy protection during EMD calculation [17]. Yuan et al. designed an encrypted image search scheme with a secure kNN algorithm and tree index for improved efficiency [18]. Chen et al. proposed a Markov process-based retrieval scheme encrypting Huffman tables in JPEG files [19]. Weng et al. introduced a multimedia retrieval framework with robust hashing and partial encryption [20], [21]. Xia et al. presented a privacy-preserving CBIR scheme using descriptors, secure kNN, and locality-sensitive hashing, incorporating encryption-domain watermarking to deter illegal distribution [22]. Zhang et al. proposed a secure outsourced CBIR scheme with fine-grained access control, featuring a key-agent to identify accessible images for users [23].

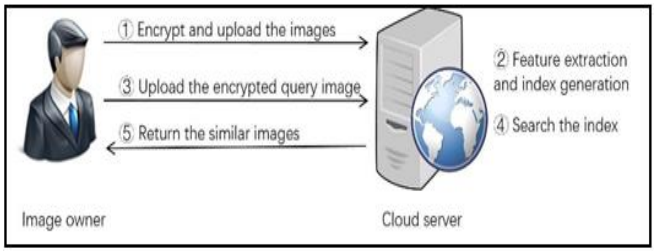

Fig 1 In the system model's initialization phase, the image owner encrypts and uploads images to the cloud server, which subsequently extracts features from the encrypted images to generate an index. During the query phase, the image owner uploads an encrypted query image to the cloud server, where features are extracted from the query image to search the index. Ultimately, images similar to the query image are returned to the image owner.

The mentioned approaches provide effective solutions for outsourcing CBIR services, yet they share a common drawback. Due to the substantial storage volume and computational complexity involved, both image feature extraction and index construction become resource-intensive operations. In previous outsourced CBIR schemes [13], [14], [15], [16], [17], [18], [19], [21], [22], the data owner bears the responsibility for these tasks. Bellafqira et al. [24], [25] introduced two secure CBIR schemes in the homomorphic encryption domain, allowing direct extraction of SIFT [24] and discrete wavelet transform features [25] from encrypted images. However, these features are limited to exact searches due to the sensitivity of encrypted images to tiny differences in plaintext images. Xu et al. [26] proposed a privacy-preserving CBIR scheme based on partial encryption, orthogonally decomposing images and encrypting one part while using the other for feature extraction. Nevertheless, the unencrypted part poses a risk of serious information leakage. Ferreira et al. [3], [4] presented an Image Encryption Scheme tailored for CBIR (IES-CBIR), protecting color values through random permutation and pixel shuffling. HSV color histograms are extracted from encrypted images at the cloud server, and similarities between images are measured using Hamming distances. This way, the image owner handles image encryption only, with other tasks outsourced to the cloud server. However, the global histogram proves inflexible for image retrieval. Liu et al. [27] attempted to enhance retrieval accuracy with a difference histogram, but the improvement was marginal. In this paper, we propose an outsourced CBIR scheme based on secure local features, outsourcing feature extraction, index construction, and search operations to the cloud server. The proposed scheme, leveraging the BOEW model, achieves significantly higher retrieval precision.

III. "INTRODUCTION TO THE SYSTEM AND PRELIMINARY DETAILS

A. System Architecture

Aligned with [28], the proposed scheme encompasses two entities: the image owner and the cloud server, as depicted in Fig. 1.

The image owner possesses an extensive image database, denoted as $\blacksquare = I =$, along with the corresponding identity set , slated for outsourcing to enhance cost-effectiveness and convenience. To ensure privacy, the image database undergoes encryption before uploading, resulting in the creation of an encrypted image set . Beyond image encryption, the image owner aims to delegate computation and storage tasks to the cloud server whenever feasible.

Once the images are stored on the cloud server, the image owner may wish to retrieve images similar to a query image. In our scheme's query phase, the image owner is only required to encrypt the query image and upload it. The cloud server handles feature extraction and the search operation. The cloud server retains the encrypted images for the image owner and offers CBIR services. In addition to search operations, our scheme delegates index generation responsibilities to the cloud server.

B. Security Architecture

Similar to previous SE schemes [12], [16], [28], [29], [30], [31], our scheme assumes an honest-but-curious cloud server. This implies that the cloud server adheres to the specified protocol accurately but has the potential to retain and analyze communication history to obtain sensitive information. The paper does not account for information leakage stemming from access patterns. Additionally, if images Ii and Ij are clustered together or returned as search results for the same query, it becomes evident that they are similar. This type of information leakage, like in many prior works [3], [4], [13], [14], [15], [17], [18], [19], [21], [22], [24], [25], is not considered in this paper.

C. Preliminaries

➢ *Bag-of-Word Model*

CBIR methods involve the extraction of visual features to represent images, and the similarity between images is measured by the distance between their feature vectors. Features can be extracted either globally from the entire image or locally from small regions. Generally, local features are more robust and tend to yield more accurate results [32]. One popular CBIR approach utilizing local features is the bag-of-words (BOW) model [33].

The BOW model originated in natural language processing and information retrieval, treating documents as collections of words, disregarding word order and grammar. This model has been widely adopted in image retrieval [34], [35]. In the BOW model for image retrieval, local features are extracted from images in the database and then clustered jointly. Subsequently, all local features are represented by their nearest visual word, and an image is finally denoted by a histogram of these visual words. The Bag-of-Visual-Words (BOEW) model involves three steps, namely:

- *Local Feature Extraction.*

In the initial step, local features are extracted from the images in the database. Common local features include SIFT [36] and SURF [37], known for their invariance to illumination, deformation, and rotation. With the evolution of cloud computing, researchers have devised secure SIFT feature extraction methods capable of computing SIFT features from specifically encrypted images. However, the extracted features remain encrypted and cannot be directly utilized for image retrieval [38], [39]. For the sake of efficiency and security, we opt to compute color histograms from image blocks as local features.

- *Vocabulary Construction.*

In the second step, the vocabulary is constructed. The k-means method is commonly used to cluster local features into k classes, with the cluster centers defined as visual words. The complete set of these visual words forms the vocabulary.

- *Histogram Calculation.*

In the final step, the histogram of visual words is calculated. It's essential to note that all local features are represented by their nearest cluster centers (visual words). Ultimately, each image is depicted by a k-bins histogram of visual words.

➢ *Color Representation*

This paper utilizes the HSV color model for system description, following the approach in [3], [4]. HSV represents colors in a cylindrical-coordinate system (hue, saturation, value) derived from the RGB color model. In Matlab, HSV components are typically measured in decimals within [0,1], but for local histogram calculation convenience, we quantize them into integers within [0,100]. The experiments also assess our scheme's performance in RGB and YUV color spaces.

IV. THE NOVEL STRATEGY

➢ *Key Formation.*

K ← KeyGen(1κ). Images contain color and texture information, necessitating effective protection [3], [4]. In our approach, color data is safeguarded through color value substitution, while texture information is shielded via pixel position shuffling. Our methodology operates within the HSV color space. To secure image content, we substitute color values in the three components using distinct secret keys. Following this, the image is segmented into non-overlapping blocks, which are then subjected to shuffling. Finally, pixel shuffling within each block is executed to fortify texture information protection.

The entire encryption process involves a pseudo-random permutation generator and various secret keys denoted as K = {RandPerm, {keyHere, secret keysv*} * ∈ {H, S, V}, keyb, {keyp*v*} ** ∈ {}* ∈ {H, S, V}}. These keys are employed for generating random permutations for color substitution in H, S, V components, respectively, within the [0...100] range: {pmtv*,#} ← RandPerm(keyv*,[0...100]),

Where ∗∈{H,S,V },# ∈{1,...,Npmt},

The secret key keyb is used to generate pseudo-random permutations within the range [1...blknum], where blknum is the total number of non-overlapping blocks in an image. The random permutation generated by keyb is utilized to shuffle image blocks and is generated as follows:

pmtb ← RandPerm(keyb,[1...blknum],ID).

The same block permutation secret key is applied to the three components in an image, with different keys for different images, ensuring improved security without affecting retrieval accuracy. In the calculation process, the ID and the secret key keyb are merged as the seed of the pseudo-random permutation generator. The secret keys {keyp*} * ∈ {H, S, V} are used to generate random permutations for shuffling pixels in blocks. The random permutations of the three components are generated as follows,

pmtpj ← RandPerm(keyp,[1...blksize],ID,j),(3)

Where ∗ ∈{H, S, V}. Different keys are generated for distinct image blocks, enhancing security without impacting local histogram calculation, thus preserving image retrieval accuracy. Among the secret keys, RandPerm, blksize, and keyv are necessary to request a valid image query. After receiving the encrypted images, all secret keys are required for image decryption.

➢ *Data Security Measures*

C ← ImgEnc(I,ID,K,blksize). The image encryption process involves three steps: color value substitution, block

permutation, and intra-block pixel permutation. Each step is specified by a sub-algorithm (refer to Algorithm 1, 2, and 3).

Algorithm 1 utilizes a polyalphabetic cipher to encrypt color values. This cipher substitutes values with multiple tables, represented in this paper as permutations of elements in the set {0,..., 255}. Consequently, the same pixel value at different positions can be substituted with different values, enhancing resistance against statistical attacks [40], [41]. Algorithms 2 and 3 generate random permutations for block and intra-block pixel shuffling, respectively, as shown in Algorithm 4, defining the entire image encryption process.

➢ *Generation of Index*

- Generate the index (Idx). Using IndexGen(C, blksize). In our approach, we delegate the index construction task to a cloud server, lightening the load on the image owner. Drawing inspiration from the renowned BOW model, we introduce a fresh perspective with our BOEW model, aimed at facilitating image retrieval while safeguarding image privacy. Following a structure akin to the BOW model, our approach involves three sequential steps.
- Extraction of Local Histograms. Initially, the encrypted images undergo segmentation into non-overlapping blocks, mirroring the block division utilized in the image encryption procedure.

➢ *Algorithm 1 : Pixel Transformation*

- *Input: Image I and secret keys {key∨∗}∗∈{H,S,V }*
- *Output: I′*

✓ Generate the secret permutations pmtv, pmtvS, and pmtvV, where # ∈ {1,...,Npmt};
✓ Generate three random sequences sqntH, sqntV, sqntS. The length of sequences is equal to the pixel amount of the image I, and the elements of these sequences are within the set [1,...,Npmt];
✓ Denote pi as the ith pixel in image I, and piH, piS, piV as the three components of the pixel;
✓ Denote p′i as the corresponding pixel in the encrypted image I′, and pi′H, pi′S, pi′V as the three components of the pixel;
✓ For each p′i ∈ I′ do
✓ *p′iH ← pmtvH, sqntH[i][piH], p′iS ← pmtvS, sqntS[i][piS], p′iV ← pmtvV, sqntV[i][piV];*
✓ End the loop.

$^{H,\#}$

➢ *Algorithm 2 : Block Shuffling*

- *Input: I′, ID, keyb, blksize*
- *Output: I″*

✓ */* blksize signifies the size of image blocks, a configurable parameter in our scheme.*/*
✓ *Blksize signifies the size of image blocks, a configurable parameter in our scheme.*
✓ Segment the image I′ into non-overlapping blocks, labeled as blk′;
✓ Partition the resulting image I″ into blocks, denoted as blk″;
✓ For each blk″[i] in I″ do
✓ Perform block shuffling: blk″[i] ← blk′[pmtb[i]];
✓ End the loop.

In contrast to traditional local features like SIFT, known for their robustness to scaling, rotation, affine distortion, and illumination changes, local histograms have their limitations. Certain researchers have suggested outsourcing the calculation of SIFT features while preserving privacy [38], [39], [42]. However, these methods involve multiple rounds of communication between non-colluding cloud servers. Furthermore, employing outsourced SIFT in secure Content-Based Image Retrieval (CBIR) introduces additional communication between the server and query users, posing an undesirable burden on the users.

- *Generation of Vocabulary:*

Employ the k-means clustering algorithm [43] to cluster all the local histograms {hij} into k classes. The resulting k cluster centers are designated as encrypted visual words, forming the vocabulary.

- *Extraction of Global Features:*

Following the generation of the vocabulary, each local histogram in an image is represented by its nearest visual word. Subsequently, the occurrence histogram of these visual words is calculated and normalized, serving as the representation of the image.vector $\mathbf{f} = (f_i)_{i=1}^{k}$. Finally, the image identities and

➢ *Algorithm 3 : Intrablock Permutation*

- *Input: ID, {keyp∗}∗∈{H,S,V }, blksize*
- *Output: I″C*

✓ Refer to the final encrypted image as C, composed of components CH, CS, and CV. Partition CH, CS, and CV into non-overlapping blocks denoted as blkHc, blkSc, and blkVc;
✓ Divide the components of image I″ into non-overlapping blocks represented by blk″H, blk″S, and blk″V
✓ For each ∗∈ H, S, V:
✓ Begin a loop:
✓ Generate the secret permutation for the j-th block blk″∗j as pmtp∗j;
✓ For each i:
✓ *Update blkc∗j[i] to blk″∗j[pmtp∗j[i]];*
✓ End the loop.

➢ *Algorithm : 4 Image Encryption*

- *Input: I,ID,K, and blksize,*

✓ For each Ii in I do
✓ *Ii‴ = ValuePermutBlockPermut((Ii′, ID, {keyi, keyv∗}∗∈{H, S, V, blksize}));*

ISSN No:-2456-2165

- ✓ Ci = IntrablockPermut(Ii″, IDi, {keyp∗}∗∈{H, S, V}, blksize);
- ✓ *End the loop.*

Table 1 The Linear Index

Image Identity	Feature Vector
ID(*C*1)	**f**1 = {*f*11,*f*12,...*f*1*j*,...,*f*1*k*}
...	...
ID(*Ci*)	**f***i* = {*fi*1,*fi*2,...*fij*,...,*fik*}
...	...
ID(*Cn*)	**f***n* = *fn*1,*fn*2,...*fnj*,...,*fnk*

➢ *Creation of Trapdoor*

TD ← TrapGen(K, Iq, IDIq, blksize). In our approach, the trapdoor is created through the encryption of the query image using color value substitution, block permutation, and intrablock pixel permutation. The resulting encrypted query image is subsequently transmitted to the cloud server, serving as the trapdoor..

➢ *Search Procedure*

Rq ← Search(C, Idx, TD) Upon receiving the trapdoor, which is the encrypted query image, the cloud server segments it into blocks and computes the set of local histograms {hqj}, where blknumq is the total number of blocks in the query image Iq. Subsequently, a feature vector f is generated using the vocabulary and {hqj}. The Manhattan distance between fq and the feature vector fi in the index can be directly computed. Finally, the θ most similar images are provided to the image owner as the search results.

➢ *Image Restoration*

The procedure of restoring the original image, Iq, from its encrypted counterpart, Rq, involves reversing the encryption steps. This includes undoing the intrablock pixel permutation, reverting the block permutation, and ultimately reconstructing the color value permutation. The decryption process, although not explicitly detailed, is straightforward in its execution.

➢ *Updating Image Information*

Idx ← ImgUpdate(Idx, ID, TD, updatetype). In the process of incorporating new images, the owner encrypts the image and provides the encrypted image along with its ID to the cloud server. The server, utilizing the trapdoor generation process, generates the relevant feature vector and adds the image ID-feature vector pair to the index. For image deletions, the owner informs the server to eliminate both the encrypted image and the corresponding entry in the index.

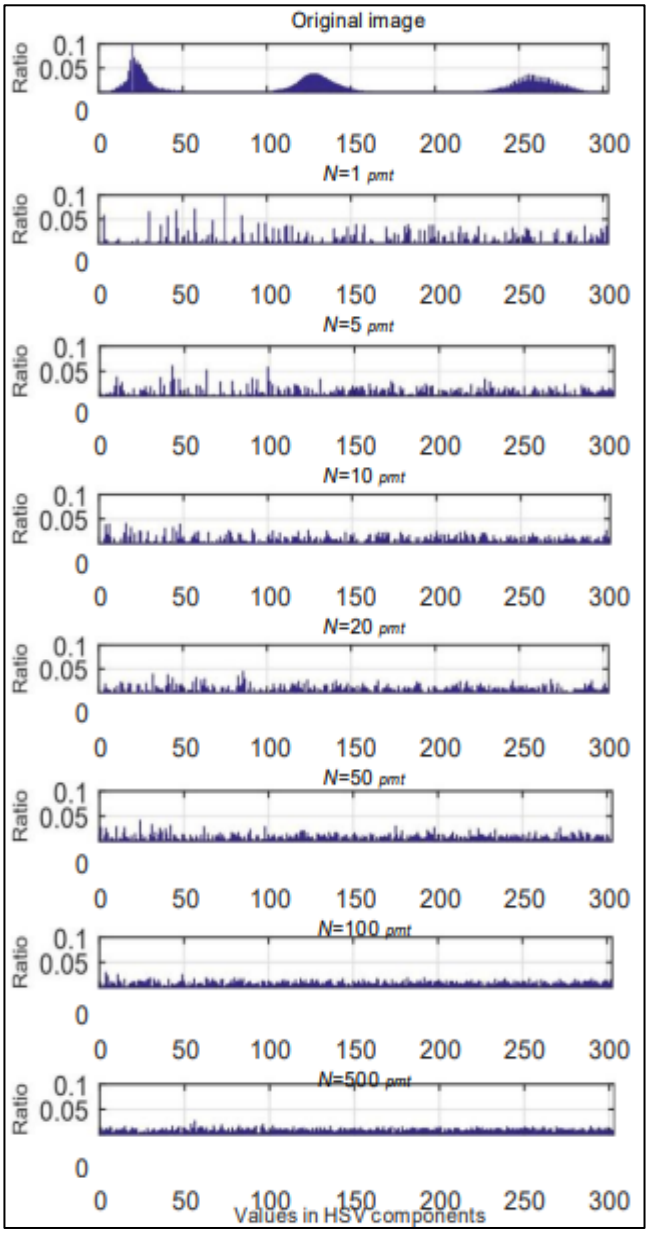

Fig 4 The occurrence ratios of color values are compared between an original image and its encrypted versions with different Npmt values. It is evident that as the image is encrypted with more permutations, the histogram becomes more flattened, showcasing the effectiveness of the protective measures.

As illustrated in Fig. 6 (b), a small blksize in a large image leads to minimal protection of image content through intra-block pixel permutation, resulting in some blurring but almost full visibility of the content. On the contrary, block permutation (Fig. 6 (c)) provides effective randomization for images with a small blksize. Color value substitution with Npmt = 1 fully permutes color information but leaves much texture information revealed (Fig. 6 (d)). Further blurring of image content can be achieved by increasing the number of permutations, as shown in Fig. 6 (e-f). Ultimately, effective protection of image content is achieved by combining all three steps, as depicted in Fig. 6 (g-h).

ISSN No:-2456-2165

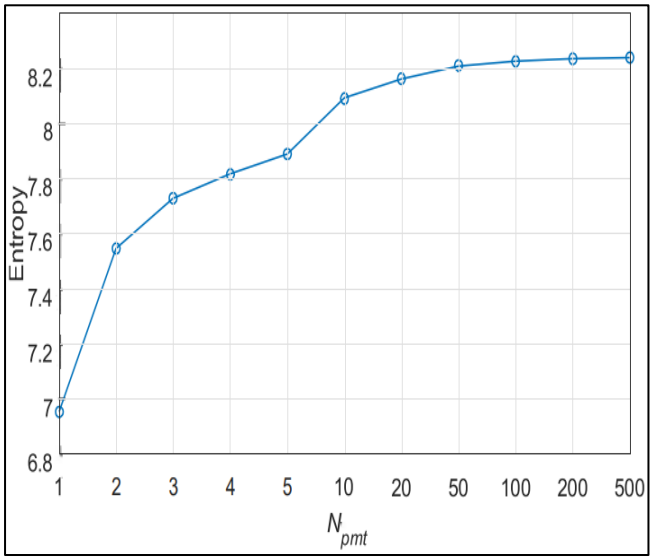

Fig 5 Entropies Computed for Global Histograms of Encrypted Images Employing Varying values of Npmt

Table 2 Symbol of Parameters

Parameters	Symbol
Size of block	*blksize*
Number of cluster centers	*k blknumT*
Total number of local histograms	*blknumU*
Number of used local histograms in clustering	*Npmt*
Number of permutations in color value substitution	

➢ *Exploration and Analysis*

The proposed scheme not only demonstrates robustness across diverse parameters but also achieves commendable retrieval accuracy within specified ranges for blksize (15×15 to 100×100) and k (500 to 8000). Its unique approach of outsourcing index construction to the cloud server sets it apart, offering a streamlined solution that lessens the burden on image owners, distinguishing it from earlier privacy-preserving CBIR schemes.

In contrast to methodologies using global histograms, our scheme exhibits a significant improvement in mean Average Precision (mAP) from 0.56544 to 0.64244, highlighting its effectiveness.

To further enhance the scheme, future research could explore refining local feature extraction under the BOEW model, potentially incorporating techniques like gradient or texture information while addressing potential information leakage. Additionally, addressing storage concerns related to uncompressed images and extending the application of the BOEW model to encrypted JPEG images represent promising avenues for future advancements. These considerations underscore the ongoing potential for innovation in privacy-preserving image retrieval systems.

➢ *Key Findings*

In this study, we introduce an innovative privacy-preserving Content-Based Image Retrieval (CBIR) scheme. The proposal features a novel Bag-of-Encrypted-Words (BOEW) model, designed to enhance retrieval accuracy.

As demonstrated in a case study, image content protection is achieved through color value substitution, block permutation, and intra-block pixel permutation.

Local histograms serve as the basis for calculating local features, and the k-means algorithm is employed to generate encrypted visual words.

V. FUTURE DIRECTIONS

In our future endeavors, we aim to enhance the design of local descriptors within our Bag-of-Encrypted-Words (BOEW) model. Exploring improved techniques for safeguarding image content under the chosen Cryptographic Privacy Amplification (CPA) model will be a focal point for further research.

Additionally, the application of the BOEW model to JPEG images presents an intriguing avenue for investigation.

REFERENCES

[1]. C. S. Lu, “Homomorphic encryption-based secure sift for privacypreserving feature extraction,” Proceedings of SPIE The International Society for Optical Engineering, vol. 7880, no. 2, pp. 788 005–17, 2011. [3] B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, “Privacy-˜ preserving content-based image retrieval in the cloud,” in IEEE 34th Symposium on Reliable Distributed Systems. IEEE, 2015, pp. 11–20.

[2]. B. Ferreira, J. Rodrigues, J. Leitao, and H. Domingos, “Practical privacypreserving content-based retrieval in cloud image repositories,” IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2017.

[3]. Y. Rui, T. S. Huang, M. Ortega, and S. Mehrotra, “Relevance feedback: a power tool for interactive content-based image retrieval,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 8, no. 5, pp. 644–655, 1998.

[4]. Y. Liu, D. Zhang, G. Lu, and W.-Y. Ma, “A survey of content-based image retrieval with high-level semantics,” Pattern Recognition, vol. 40, no. 1, pp. 262–282, 2007.

[5]. C. B. Akgul, D. L. Rubin, S. Napel, C. F. Beaulieu, H. Greenspan,¨ and B. Acar, “Content-based image retrieval in radiology: current status and future directions,” Journal of Digital Imaging, vol. 24, no. 2, pp. 208–222, 2011.

[6]. X. Zhang, W. Liu, M. Dundar, S. Badve, and S. Zhang, “Towards largescale histopathological image analysis: Hashing-based image retrieval,” IEEE Transactions on Medical Imaging, vol. 34, no. 2, pp. 496–506, 2015.

[7]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

[8]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in 2010 Proceedings IEEE INFOCOM. IEEE, 2010, pp. 1–5.
[9]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, vol. 25, no. 1, pp. 222–233, 2013.
[10]. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016.
[11]. Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacypreserving content-based image retrieval in cloud computing," IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 276–286, 2018.
[12]. J. Yuan, S. Yu, and L. Guo, "Seisa: Secure and efficient encrypted image search with access control," in 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015, pp. 2083–2091.
[13]. H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov process-based retrieval for encrypted jpeg images," EURASIP Journal on Information Security, vol. 2016, no. 1, pp. 1–9, 2016.
[14]. L. Weng, L. Amsaleg, A. Morton, and S. Marchand-Maillet, "A privacypreserving framework for large-scale content-based information retrieval," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 152–167, Jan 2015.
[15]. L. Weng, L. Amsaleg, and T. Furon, "Privacy-preserving outsourced media search," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 10, pp. 2738–2751, 2016.
[16]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2594–2608, 2016.
[17]. L. Zhang, T. Jung, K. Liu, X. Y. Li, X. Ding, J. Gu, and Y. Liu, "Pic: Enable large-scale privacy preserving content-based image search on cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 28, no. 11, pp. 3258–3271, Nov 2017.
[18]. R. Bellafqira, G. Coatrieux, D. Bouslimi, and G. Quellec, "Contentbased image retrieval in homomorphic encryption domain," in 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). IEEE, 2015, pp. 2944–2947.
[19]. "An end to end secure cbir over encrypted medical database," in Engineering in Medicine and Biology Society (EMBC), 2016 IEEE 38th Annual International Conference of the. IEEE, 2016, pp. 2537–2540.