International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Impact Factor (2018): 5.426

# PPCBIR: Privacy Preserving Content Based Image Retrieval

**Athira Nair M[1], Asha Vijayan[2]**

[1] Post Graduation Student, College of Engineering Kidangoor

[2]Assistant Professor, College of engineering kidangoor

**Abstract:** ***The amount of unstructured data such as images, videos being generated and shared everyday is growing at a faster rate. The storage need for such large amount of data is a driving factor for outsourcing services such as cloud storage and computing. However it actually raises new challenges in terms of data privacy. One solution is to encrypt the image database before outsourcing it and run all the computation on client side for eg, Earth Mover's Distance or EMD-PPCBIR but this leads to client-overhead. To address this issue various technique has been developed for efficient retrieval of images such as IES-PPCBIR, EDH-PPCBIR, and SIFT PPCBIR, etc. Here CBIR servies are outsourced to the server side. All these method are effective over encrypted images.***

**Keywords:** Content based image retrieval**,** Encrypted difference histogram, Image encryption scheme, Privacy Preserving Content Based Image Retrieval, Scale invariant feature transform.

## 1. Introduction

The amount of images being generated is increasing day by day such as Instagram and flickr, are well known social networking sites which hosts millions of images and new images are uploaded everyday. NASAs earth observing system generates 1 Tera Byte of images everyday [1]. In medical field digital images are produced at increasing rate for diagnosis and therapy. Hence with the increase in quantity, availability and importance of images in our daily life Content Based Image Retrieval (CBIR) applications have been developed rapidly. Content based image retrieval is the process of searching, browsing and retrieving images based on image contents like texture, color, shape, etc. in the database containing digital images. When the user provides a query image system retrieves all the images from image database similar to given query image. Raw image data can't be used straightly in most computer vision tasks, because of high dimensionality of image and lot of information embeded in the image is redundant. Only expressive representation of the most relevant information is extracted [2] [3]. The process of finding the expressive representation is called feature extraction. Feature extraction can also be defined as act of mapping the image from image space to the feature space.

There are two types of feature extraction technique:-
*i) Global feature extraction:* It captures visual property from the entire image such as color histogram, texture feature, shape etc. Extraction is done at high speed however result will be less accurate.
*ii) Local feature extraction:* It captures visual property from the group of pixels. Extraction is done at low speed however result will be more accurate.

CBIR is helpful in many real world image retrieval or matching applications, for eg clinicians may use CBIR to retrieve similar cases of the patients to facilitate the clinical decision. It is also used by law enforcement agencies to identify criminals. The main disadvantage of CBIR is its storage requirement and severe computation so to overcome this database containing digital images and CBIR service is outsourced to cloud serve. Again problem in CS is privacy, in order to protect data privacy, images need to be encrypted before being uploaded to CSP. [4]

The rest of this paper is organized as follows: Section 2 contains scope of this survey, Section 3 gives a detailed description of different types of PPCBIR, and finally we conclude the paper in Section 4.

## 2. Scope of this Survey

The scope of this survey is to find best PPCBIR method that can retrieve images similar to given query image from archive of encrypted images in less time and the result of retrieval must be accurate. Various methods like IES-PPCBIR, EMD-PPCBIR, SIFT-PPCBIR etc have been found.

## 3. Literature Survey

After reviewing the literature in the existing domain, it has been discovered that there exists the following classification for image retrieval over encrypted database of images.

### 3.1 IES-PPCBIR (Image Encryption Scheme With Privacy Preserving Content Based Image Retrieval)

A PPCBIR scheme where features are extracted directly from ciphertexts by the cloud server reducing client overhead. Image privacy is the ability to keep the contents of an image secret from public or unauthorized people. Color is one of the most relevant feature of an image, which helps human recognize images. Image contents are characterized by the combination of its color and texture information. Both the color and texture information can be separated from each other. Color features extraction can be done using color space such as RGB, YCbCr etc. Set of rule that allow describing color with numbers is called color space [5] [6]. Texture information shows the relative positions of pixels and their color values. Texture information is more relevant for object recognition.

Bernardo et.al [7] proposed IES-PPCBIR framework consisting of two main entities that is, cloud and users. Repositories are created by a single user and images are outsourced to the repository which is managed by cloud. Repositories are used by multiple users to store, retrieve or search image by providing query image. The goal here is to ensure the privacy of users, hence all images sent to the cloud are encrypted. After creating a repository, a new repository key is generated by that user which is shared with other authorized users, allowing them to search on the repository and store new images. To access content of encrypted images or to update images, a user needs an image key generated by the owner of that image. Image keys for a particular image are kept secret by their users (image owner). User encrypts image database using repository key and image key and outsource the encrypted image database to the repository managed by the cloud server. When the cloud receives an encrypted database of images for storage it extracts its relevant features from the encrypted images and indexes the image based on these features. The same process is carried out or performed for a query image. The reply to a query will contain a k number of encrypted images relevant to the query image which includes each images id and the id of the user that owns each of the images. For decrypting and access the contents of an image, not only the repository key but also image key is required by the querying user. So based on the image and user id the querying user request the owner of the image for image key to access the full contents of image.

Encryption process consists of feature extraction and feature indexing. Feature extraction consists of extracting a reduced set of feature vectors that describe the image. The cloud server constructs a color histogram by counting the number of pixels in each intensity level from each encrypted image and each HSV color channel. After extracting these color histogram as feature, the cloud can start construction of feature indexing to speedup query execution. A vocabulary tree and an inverted list index for each repository is constructed using the Bag-Of-Visual-Words (BOVW) representation [8] [9]. In the BOVW model, extracted feature-vectors are hierarchically clustered in the form of a vocabulary tree which is also called codebook. In the vocabulary tree each node denotes a feature-vector in the collection and leaf nodes are selected as visual words. The cloud server construct an inverted list index, which contains key and it's corresponding values. All visual words are the keys and, values are list of images. This type of list is also called a Posting List.

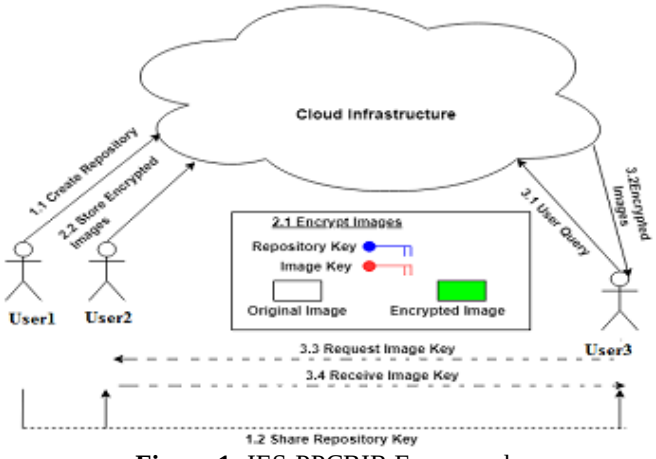


**Figure 1:** IES-PPCBIR Framework.

### 3.2 EMD-PPCBIR (Earth Mover's Distance With Privacy Preserving Content Based Image Retrieval)

Zhihua Xia et.al [10] proposed EMD based PPCBIR model. There are three entities in EMD-PPCBIR, data owner, data user and cloud server. Data owner holds a largescale image database $M = \{m_1, m_2 \ldots m_n\}$ to be outsourced, where n is the number of images in the database. The data owner generates a searchable index for the image database M. For privacy-preserving, the data owner needs to encrypt the image database and the search index, and then outsources the encrypted image database and index to the cloud. Cloud provides the CBIR service without interacting with the data owner once the database is outsourced. During the CBIR query phase, the authorized user submits an encrypted query trapdoor to the cloud server. Then, the cloud server compares the similarity between the query image and the images in the database, and returns the encrypted similar images to the data user. Finally, the authorized user decrypts the received images. CBIR usually involves extraction of features and search in the feature space for similar images. So it has two challenges.

The first challenge is how to mathematically describe an image, which is referred to as the feature extraction step. Feature can be extracted either from the entire image (global feature extraction) or from group of pixels (local feature extraction). The merit of global feature is its high speed for both extracting features and computing similarity but has low accuracy. On the other hand local feature extraction method is more accurate, example of local feature extraction method is called bag-of-words model. In this model, local features are extracted from all images in the database and then jointly clustered. The cluster centers are used as words to form the vocabulary. An image $m_t$, denoted using bag-of-words as:

$$S_t=\{(c_1^{(t)},w_1^{(t)}),\ldots(c_i^{(t)},w_i^{(t)}),\ldots,(c_{kt},w_{kt})^{(t)}\}$$

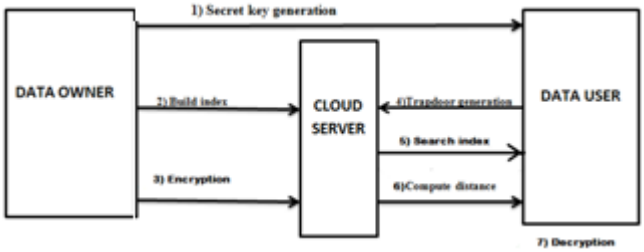


**Figure 2:** EMD-PPCBIR Flowchart.

Similarity between mq and mt is calculated using Earth Mover's Distance (EMD) between their signatures sq and st. The earth mover's distance can be applied to evaluate the similarity between the distributions. Given two distributions, the distribution with smaller sum of weights can be viewed as a mass of earth which rightly spread in space, and the distribution with larger sum of weights can be viewed as an array of holes in the same space. The EMD measures the minimal cost of moving all the earth into the holes. The EMD measures the minimal cost of moving all the earth into the holes. A unit of work will be counted when a unit of earth is transported for a unit of distance. The EMD transforms the matching problem to the transportation problem. Two distributions have the least transportation cost can be

viewed as the most similar ones. The EMD between s1and s2 is defined as:

$$EMD(s_1,s_2) = min\sum_{i,j} f_{i,j} d_{i,j} \div \sum_{i,j} f_{i,j}$$

Before applying EMD Local Sensitive Hashing (LSH) is applied to reduce time complexity. LSH is a two stage structure in the first stage dissimilar images are filtered out by pre-filter table to shrink the search scope. In the second stage the remaining images are compared using EMD metric. LSH is an effective way of reducing dimensionality of data. Several hash functions are applied to the signature centroid to form LSH table. If two signature centroid hashed into same bucket for at least one of the hash function they form candidate pair. Data owner encrypts image DB and signature using different keys and send encrypted DB, signature and secure LSH tables to cloud server. Data user constructs query trapdoor and sends to CS. Data user obtain encrypted images similar to query images, which is decrypted by the user later.

### 3.3 SIFT-PPCBIR (Scale Invariant Feature Transform In Privacy Preserving Content Based Image Retrieval)

A content-based image retrieval system for a tattoo image database is proposed by Anil et.al [11] The system automatically extracts image features based on the Scale Invariant Feature Transform (SIFT). Side information, i.e., body location of tattoos and tattoo classes, is utilized to improve the retrieval. time and retrieval accuracy [12] [13].

SIFT PPCIR system consists of following steps:-
*Image Encryption And Indexing:* The data owner encrypts the database and outsources the database to the cloud server. For an original image I with size of n*n pixels, we use the matrix I(x, y) with each entry of 8-bit length. The data owner randomly selects $n^2$ integers from [0 to 255] to generate a random matrix $I_1(x,y)$ and then encrypts I(x,y) by computing E(x, y) as:

$$E(x,y) = I(x,y)+I_1(x,y)$$

The ciphertext E(x,y) is sent to cloud server. Indexing approach first makes use of the location of the tattoo on body, if available. Tattoo location is a reliable piece of information because it can be tagged precisely and objectively. Hence, searching similar images at the same body location can significantly reduce the matching time without any loss of matching accuracy.

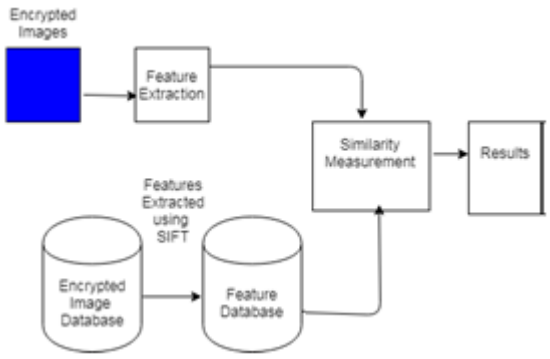


**Figure 3:** SIFT-PPCBIR System Model

*Image Feature Extraction:* Scale Invariant Feature Transform (SIFT) is a local feature based approach. Unlike global feature based approach local feature based approach captures property from group of pixels and generates descriptors that represents texture around feature points. The feature points are invariant to image scale and rotation and provide matching across range of distortion, noise etc.

*Image Retrieval:* For comparing two images a keypoint from set of detected keypoints are compared with each keypoint in the other image and measure how many of them successfully matches. Comparison here means Euclidean distance between keypoint are computed to obtain first and second closest distance. [14] [15] [16] If ratio between them is less than system threshold which is 0.49, then images are smiliar and are retrieved.

### 3.4 LBP-PPCBIR (Local Binary Pattern In Privacy Preserving Content Based Image Retrieval)

There are three entities data owner, cloud server S1 and cloud server S2. Data owner maintains a huge database of images which should be encrypted before outsourcing to cloud server resulting in two encrypted image sets. Extraction of LBP features from the encrypted images is the responsibility of CS. The cloud contains two entities Server 1 and Server 2 both of which rceives the different encrypted image sets. LBP features are extracted by Server 1. During the encryption process, an image is partitioned into non-overlapping blocks and the blocks are shuffled to protect the contents of the image. Finally all the pixels except the center pixel in each block are shuffled. The extracted LBP features can be applied to many applications, such as texture classification, image retrieval, face recognition, and so on.
Steps in LBP PPCBIR framework:-

*Image Encryption:* Our goal is to protect the image content and allowing the cloud server to execute the LBP algorithm. In order to protect the image owner's image privacy, image is encrypted before outsourcing to the cloud severs. The image consists of two types of information, color and texture information, which require appropriate protection. In this method [17] [18] [19] [20], to protect the image color information image segmentation is used, and for the texture information protection pixel position are shuffled. Three times of block permutation, pixel replacement and image segmentation is for encryption of image.

*Local Binary Pattern (LBP) Feature extraction:* In Local Binary Pattern (LBP) image is divided into fixed size 3*3 blocks the center pixel's gray value and its 8 neighbors are compared. If gray values of neighbors are greater than center pixels gray value then the position is marked as 1 otherwise marked as 0. Thus the 8 points which is either 1 or 0 forms an 8-bit binary number which is LBP value. The LBP histograms are constructed from encrypted grayscale values of images. After receiving the encrypted images by S1 and S2 cloud servers, they divide the images as the image owner does. Both S1 and S2 calculate the pixel difference between the center of the block and the pixels around. S2 sends its computed differences to S1 and after obtaining the above information, S1 subtracts the received differences from its own differences.

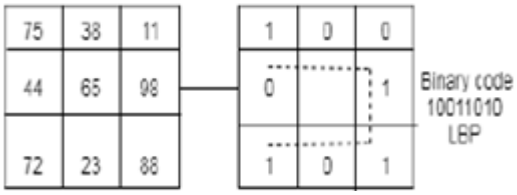


**Figure 4:** LBP-PPCBIR Feature Extraction.

*Image retrieval:* Manhattan distance is used to compute similarity between query image and images in database after extracting LBP features. Mean average precision (mAP) is used to measure the retrieval accuracy extraction. [21] [21] [23]

### 3.5 EDH-PPCBIR (Encrypted Difference Histogram with PPCBIR)

Another scheme for enabling CBIR over encrypted images proposed by Liu et.al [24]. This scheme is based on encrypted difference histogram. Content owner firstly computes order or disorder difference matrices of RGB component and then encrypts these matrices using value replacement and position scrambling. The content owner then outsources the encrypted images to CSP, the server extracts difference histogram as image feature vector directly from the encrypted images. Similarly query is encrypted and feature is extracted. To compute similarity between feature vectors extracted from query and feature vector extracted from all encrypted images Euclidean distance is used.

There are 3 entities in the EDH-PPCBIR scheme.
*Image owner:* Encrypts the image database before outsourcing to CSP using secret key.
*Cloud Service Provider(CSP):* Extracts feature from the received encrypted images and build index. Upon receiving query through trapdoor, extracts features of the query image from trapdoor and search index for most similar feature to query feature by computing Euclidean distance between them and return most k similar images to query image to the user.

*User*: They want access to images and only authorizeduser are allowed. They decrypt the image using a secret key.

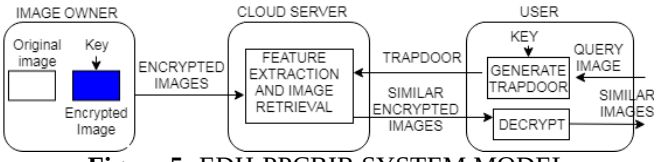


**Figure 5:** EDH-PPCBIR SYSTEM MODEL

Following are the steps involved in EDH-PPCBIR:-
***I) Image Encryption:*** Encryption process consists of two steps:
*A) Difference matrix computation:* To extract difference histogram as image feature directly from encrypted image, difference matrix computation is required which is subdivided into three steps:

1) ***One-dimensional matrix:*** This step converts the image pixel matrix into one dimensional array using some conversion methods and the array size is same as the image size after conversion. Here two conversion methods are used.
   - *Orderly scanning:*- Here pixel values are obtained by orderly scanning the pixel matrix.
   - *Disorderly block scanning:*- Image is divided into blocks, then pixel values are obtained by disorderly scanning each blocks of pixel matrix. Hence after using the above two conversion methods there are two arrays, that is order array and disorder array.
2) ***Difference value calculation:*** We have two arrays, order and disorder arrays, by subtracting adjacent values in both arrays we get one dimensional difference arrays.
3) ***Difference matrix acquisition:*** The difference matrices that are order difference matrix (ODM) and disorder difference matrix (DDM) is obtained by inverse conversion of the difference arrays, arrays are converted back to matrices. [25] [26]

*B) Difference matrix encryption:* The output of Difference Matrix Computation is ODM and DDM. To protect the sensitive contents, difference matrices is encrypted using value replacement and position scrambling.

- *Value Replacement:*- The original in the difference matrix is replaced by value in random sequence of the three independent random permutation keys generated by PRPG.
- *Position Scrambling:*-Shuffles image pixel values. Queue transform algorithm based on one transformation is used for position scrambling. [27] [28] [29]

*II) Feature extraction and index construction:* This task is transferred to CSP to reduce the computation burden of the client. CSP directly extracts the difference histogram of RGB components as feature vector from encrypted image using difference matrix. [30]

*III) Image retrieval:* Query is encrypted in the same way and feature vector from query image is extracted from trapdoor. CSP compute Euclidean distance between query feature vector and feature vector of all the images in the index and return most similar images to the query.

## 4. Conclusion

Efficient management of large number of images being generated everyday is necessary. Privacy Preserving Content Based Image Retrieval has a wide variety of applications in medical applications, biodiversity information systems, digital libraries etc. Privacy of these image retrieval schemes can be ensured by various techniques as described above. Privacy-preserving content based image retrieval scheme, allows the data owner to outsource image database and the CBIR service to the cloud without revealing the actual content of the database. Feature extraction and index generation task is transferred to CS in EDH to reduce client overhead in EMD.

## References

[1] Gudivada, V. N., and Raghavan, V. V., 1995. "Content based image retrieval systems". Computer, 28(9), pp. 18–22
[2] Hirwane, R., 2012. "Fundamental of content based image retrieval". International Journal of Computer Science and Information Technologies.

[3] Smith, J. R., and Chang, S.-F., 1997. "Visualseek: a fully automated content-based image query system". In Proceedings of the fourth ACM international conference on Multimedia, ACM, pp. 87–98.
[4] M¨uller, H., Michoux, N., Bandon, D., and Geissbuhler, A., 2004. "A review of content-based image retrieval systems in medical applicationsclinical benefits and future directions". International journal of medical informatics, 73(1), pp. 1–23.
[5] Ferreira, B., Rodrigues, J., Leitao, J., and Domingos, H., 2015. "Privacy-preserving content-based image retrieval in the cloud". In Reliable Distributed Systems (SRDS), 2015 IEEE 34th Symposium on, IEEE, pp. 11–20.
[6] Lu, W., Swaminathan, A., Varna, A. L., and Wu, M., 2009. "Enabling search over encrypted multimedia databases". In Media Forensics and Security, Vol. 7254, International Society for Optics and Photonics, p. 725418.
[7] Wang, J. Z., Li, J., andWiederhold, G., 2001. "Simplicity: Semantics-sensitive integrated matching for picture libraries". IEEE Transactions on pattern analysis and machine intelligence, 23(9), pp. 947–963.
[8] Rejito, J., Setiana, D., and Rosadi, R. "Image indexing using color histogram and k-means clustering for optimization cbir".
[9] Reddaway, S., 2016. "Pseudo-random number generators".US Patent 3,811,038.
[10] Xia, Z., Zhu, Y., Sun, X., Qin, Z., and Ren, K., 2018."Towards privacy-preserving content-based image retrieval in cloud computing". IEEE Transactions on Cloud Computing, 6(1), pp. 276–286.
[11] Hu, S., Wang, Q., Wang, J., Qin, Z., and Ren, K., 2016. "Securing sift: Privacy-preserving outsourcing computation of feature extractions over e crypted image data". IEEE Transactions on Image Processing, 25(7), pp. 3411–3425.
[12] Jain, A. K., Lee, J.-E., Jin, R., and Gregg, N., 2009. "Content-based image retrieval: An application to tattoo images". In Image Processing (ICIP), 2009 16th IEEE International Conference on, IEEE, pp. 2745–2748.
[13] Lowe, D. G., 2004. "Distinctive image features from scale-invariant keypoints". International journal of computer vision, 60(2), pp. 91–110.
[14] Shen, Y., Guturu, P., Damarla, T., Buckles, B. P., and Namuduri, K. R., 2009. "Video stabilization using principal component analysis and scale invariant feature transform in particle filter framework". IEEE Transactions on Consumer Electronics, 55(3), p. 1714.
[15] Li, Q., Wang, G., Liu, J., and Chen, S., 2009. "Robust scale-invariant feature matching for remote sensing image registration". IEEE Geoscience and Remote Sensing Letters, 6(2), pp. 287–291.
[16] Brown, M., and Lowe, D. G., 2002. "Invariant features from interest point groups.". In BMVC, Vol. 4.
[17] Xia, Z., Ma, X., Shen, Z., Sun, X., Xiong, N. N., and Jeon, B., 2018. "Secure image lbp feature extraction incloud-based smart campus". IEEE Access.
[18] Li, P., Li, T., Yao, Z.-A., Tang, C.-M., and Li, J., 2017. "Privacy-preserving outsourcing of image feature ex traction in cloud computing". Soft Computing, 21(15), pp. 4349–4359.
[19] Ojala, T., Pietikainen, M., and Maenpaa, T., 2002. "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns". IEEE Transactions on pattern analysis and machine intelligence, 24(7), pp. 971–987.
[20] Ahonen, T., Matas, J., He, C., and Pietik¨ainen, M., 2009. "Rotation invariant image description with local binary pattern histogram fourier features". In Scandinavian Conference on Image Analysis, Springer, pp. 61–70.
[21] Zhang, G., Huang, X., Li, S. Z., Wang, Y., and Wu, X., 2004. "Boosting local binary pattern (lbp)-based face recognition". In Advances in biometric person authentication. Springer, pp. 179–186.
[22] Ahonen, T., Hadid, A., and Pietikainen, M., 2006. "Face description with local binary patterns: Application to face recognition". IEEE Transactions on Pattern Analysis & Machine Intelligence(12), pp. 2037–2041.
[23] Guo, Z., Zhang, L., and Zhang, D., 2010. "A completed modeling of local binary pattern operator for texture classification". IEEE Transactions on Image Processing, 19(6), pp. 1657–1663.
[24] Liu, D., Shen, J., Xia, Z., and Sun, X., 2017. "A content-based image retrieval scheme using an encrypted difference histogram in cloud computing". Information, 8(3), p. 96.
[25] Xu, D., Chen, K., Wang, R., and Su, S., 2018. "Separable reversible data hiding in encrypted images based on two-dimensional histogram modification". Security and Communication Networks, 2018.
[26] Li, M., and Li, Y., 2017. "Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding". Signal Processing, 130, pp. 190–196.
[27] Pawar, S. S., and Nandusekar, S., 2016. "Improvised image scrambling technique with shuffling of pixel values and position". In Communication and Electronics Systems (ICCES), International Conference on, IEEE, pp. 1–5.
[28] Wang, D., Chang, C.-C., Liu, Y., Song, G., and Liu, Y., 2015. "Digital image scrambling algorithm based on chaotic sequence and decomposition and recombination of pixel values". International Journal of Network Security, 17(3), pp. 322–327.
[29] Palubov´a, H. "Chaotic sequences in mc-cdma systems".
[30] Liang, C.-W., and Chung, W.-Y., 2016. "Color feature extraction and selection for image retrieval". In Advanced Materials for Science and Engineering (ICAMSE), International Conference on, IEEE, pp. 589–592

## Author Profile

**Athira Nair M,** She is a Post Graduation Student in College of Engineering Kidangoor. Specialization in Computer and Information Science. She received the graduation in Computer Science and Engineering from College of Engineering Kallooppara.

**Asha Vijayan,** She is an Assistant Professor in College of Engineering Kidangoor. Specialization in Software Engineering. She received graduation in Computer Science and Engineering from SJCEG pala