International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:5, 2015

Secure Image Retrieval Based On Orthogonal Decomposition under Cloud Environment

Yanyan Xu, Lizhi Xiong, Zhengquan Xu, Li Jiang

***Abstract*—**In order to protect data privacy, image with sensitive or private information needs to be encrypted before being outsourced to the cloud. However, this causes difficulties in image retrieval and data management. A secure image retrieval method based on orthogonal decomposition is proposed in the paper. The image is divided into two different components, for which encryption and feature extraction are executed separately. As a result, cloud server can extract features from an encrypted image directly and compare them with the features of the queried images, so that the user can thus obtain the image. Different from other methods, the proposed method has no special requirements to encryption algorithms. Experimental results prove that the proposed method can achieve better security and better retrieval precision.

***Keywords*—**Secure image retrieval, secure search, orthogonal decomposition, secure cloud computing.

I. Introduction

WITH the rapid development of cloud service, storing images in cloud servers is becoming more and more popular. In order to protect data privacy and to allow restrict access, sensitive images need to be encrypted before being uploaded to cloud server. However, if users want to retrieve images from server, encrypted image need to be decrypted first, then retrieval can be operated on plaintext, which makes the sensitive information being exposed to servers which breaks privacy and hence is not desired. Therefore it is important to develop technologies of image retrieval over encrypted domain. Currently the information retrieval on encrypted domain mainly focuses on text document. Song et al. [1] proposed a ciphertext scanning method based on streaming cipher to make sure whether the search term is existed in the ciphertext. Boneh et al. [2] proposed a keyword search method based on public-key encryption, where the server can identify whether messages encrypted by user's public key contain some specific keyword, but learn nothing else. Swaminathan et al. [3] explored techniques to securely rank-order the documents and extracted the most relevant document(s) from an encrypted collection based on the encrypted search queries. Wang el al. [4] utilized a new crypto primitive called the Order-Preserving Symmetric Encryption (OPSE) to achieve both security and privacy-preserving, although the guarantee to security could be weakened by it. Cao et al. [5] proposed privacy-preserving multi-keyword ranked search over encrypted data.

However, these techniques cannot be applied to content-based image retrieval directly, because effective image retrieval typically relies on comparing the distance of image features, but encrypted data fails to preserve the distance between feature vectors if the employed cryptographic primitive are not designed especially for intended goals [6]. Only recently, secure text document search in the encrypted domain has been extended to secure image retrieval research. Lu et al. [7] proposed three schemes to solve the problem of image retrieval over encrypted domain, including bit-plane randomization, random projection, and randomized unary encoding. Although it is efficient, the security has been compromised. Karthik et al. [8] presented a transparent privacy preserving hashing scheme tailored to preserve the DCT-AC coefficient distributions. But the search engine is insensitive to shapes and descriptions of both natural and artificial objects due to missing space-frequency information. In addition, its security is compromised because the constrained shuffling is used on part of AC coefficients. Hsu et al. [9] proposed a homomorphic encryption-based secure SIFT for image feature extraction, but the size of cipher-text is expanded and the computing is laborious. It should be noted that the above research results are all relying on specific encryption methods, such as shuffling, homomorphic encryption, etc., which preserve the distance of image features after images are encrypted and make the image retrieval in encrypted domain possible. However, these schemes limit the universality of the method. For example, in some situations that have high requirements to security, these methods are not suitable.

Aiming at solving these problems, a secure image retrieval method based on orthogonal decomposition is proposed in this paper. The image is divided into encryption field and feature extraction field by orthogonal decomposition, where encryption operation and feature extraction can be executed separately. Servers can get image features of encrypted image directly without decrypt it, and compare with features of queried image; the one with the closest distance is the retrieved image. Different from other methods, the proposed method has no specific requirements of cipher algorithms. Experimental results show that the proposed scheme has good encryption security and can achieve better retrieval precision.

The organization of this paper is as follows: Section II discusses the related research, and Section III proposes our scheme. Section IV provides experimental results and a performance analysis, and Section V presents conclusions.

Yanyan Xu is with the LIESMARS, Wuhan University, Wuhan, China, 430079. (86-27-68771665, e-mail: xuyy@whu.edu.cn).

Lizhi Xiong and Zhengquan Xu are with the LIESMARS, Wuhan University, Wuhan, China, 430079. (e-mail: xlzwhucs@gmail.com, xuzq@whu.edu.cn).

Li Jiang is with the School of Information Engineering, Zhengzhou University, Zhengzhou, China, 450001(e-mail: yigutong@163.com).

II. Proposed Scenarios

In this paper, a new secure image retrieval method based on orthogonal decomposition is proposed. The theory is given as follows.

A vector can be expressed as different components through orthogonal decomposition, which has such characteristics: component coefficients are mutually independent, thus any change of one coefficient will not affect the others; composite vector is sensitive to any change of component coefficient. Based on such characteristics, we assume that the original image data can be expressed as an-dimensional vector $X=(x_1, x_2, \ldots, x_n)^T$. Denote a transformation matrix $B=(b_1, b_2, \ldots, b_n)$ of size n×n, which satisfies

$$\begin{cases} b_i^T * b_j \neq 0 & \text{if } i = j \\ b_i^T * b_j = 0 & \text{otherwise} \end{cases} \quad i, j \in [1, n] \tag{1}$$

that is, B is an orthogonal matrix. Using orthogonal decomposition based on B, X can be represented as:

$$X = B \cdot Y \tag{2}$$

where the component coefficient vector $Y=(y_1, y_2, \ldots, y_n)^T$ is calculated by:

$$Y = B^{-1} \cdot X \tag{3}$$

Matrix B can be divided into two sub-matrixes, i.e., B=(R, S), where $R = (b_1, b_2, \ldots, b_m)$ and $S = (b_{m+1}, b_{m+2}, \ldots, b_n)$. Vector Y can be divided into two sub-vectors, i.e., $Y=(Y_1, Y_2)^T$. Therefore, X can be expressed as:

$$X = R \cdot Y_1 + S \cdot Y_2 \tag{4}$$

If encryption is operated on Y_1 and feature is extracted from Y_2, respectively, and the encryption operation is defined as $E(X, K_e)$, where K_e is encryption key; feature extraction is defined as $F(X, K_f)$, where K_f is the key for feature extraction, then we get:

$$X_e = E(X, K_e) = R \cdot E(Y_1, K_e) + S \cdot Y_2 \tag{5}$$

$$X_f = F(X, K_f) = R \cdot Y_1 + S \cdot F(Y_2, K_f) \tag{6}$$

According to (5), (6), we can have (7), which X_{ef} is encrypted images, and can be expressed:

$$X_{ef} = R \cdot E(Y_1, K_e) + S \cdot F(Y_2, K_f) = R \cdot Y_{1e} + S \cdot Y_2 = B \cdot Y_{ef} \tag{7}$$

Equation (7) shows that under the proposed orthogonal transformation framework, encryption and feature extraction for X are applied to orthogonal decomposition coefficients Y_1 and Y_2 instead of being directly applied to X, and these two different operations will be independent and will not interfere with each other. Because the orthogonal based vector is mutual independent, the modification of orthogonal decomposition coefficients will not counteract each other on the original data domain after orthographic composition. As a result two different kinds of operations are overlapped and distributed in original host vector X.

Similarly, assuming the decryption is defined as $D(X_{ef}, K_d)$, where K_d is decryption Key, and feature extraction is defined as $F(X_{ef}, K_f)$, then we get:

$$D(X_{ef}, K_d) = R \cdot D(Y_{1e}, K_d) + S \cdot Y_2 \tag{8}$$

$$F(X_{ef}, K_f) = F(Y_2, K_f) \tag{9}$$

From (1), assume that $b_i^T \cdot b_i = \lambda_i$, and $\lambda_i \neq 0$, where $i \in [1, n]$. Given that $P = (B^T B)^{-1}$, then $P = \mathrm{diag}(\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_n^{-1})$, based on (7), we can get:

$$Y_{ef} = P \cdot B^T \cdot X_{ef} \tag{10}$$

Similarly, assume:

$$P_R = (R^T R)^{-1} = \mathrm{diag}(\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_m^{-1}) \tag{11}$$

$$P_S = (S^T S)^{-1} = \mathrm{diag}(\lambda_{m+1}^{-1}, \lambda_{m+2}^{-1}, \ldots, \lambda_n^{-1}) \tag{12}$$

Assume the encryption domain is divided by R_p, and the feature extraction domain by S_p, which satisfy $(R_p, S_p)^T = P \cdot B^T$. Then, (13) is derived as:

$$\begin{cases} Y = (R_p, S_p)^T \cdot X \\ Y_{ef} = (R_p, S_p)^T \cdot X_{ef} \end{cases} \tag{13}$$

Accordingly, $P \cdot (R, S)^T = (R_p, S_p)^T$, $R_p^T = P_R \cdot R^T$ and $S_p^T = P_s \cdot S^T$. Then, the following is derived:

$$\begin{cases} Y_1 = R_p^T \cdot X = P_R \cdot R^T \cdot X \\ Y_2 = S_p^T \cdot X = P_s \cdot S^T \cdot X \end{cases} \tag{14}$$

$$\begin{cases} Y_{1e} = R_p^T \cdot X_{ef} = P_R \cdot R^T \cdot X_{ef} \\ Y_{2f} = S_p^T \cdot X_{ef} = P_s \cdot S^T \cdot X_{ef} \end{cases} \tag{15}$$

Finally, (8)-(9) can be redefined as:

$$\begin{aligned} D(X_{ef}, K_d) &= R * D(Y_{1e}, K_d) + S * Y_2 \\ &= R * D(Y_{1e}, K_d) + X_{ef} - R * Y_{1e} \\ &= R * D\big((P_R * R^T * X_{ef}, K_d\big) + X_{ef} - R * Y_{1e} \\ &= R * D\big((R^T * R)^{-1} * R^T * X_{ef}, K_d\big) + X_{ef} - \\ &\quad R * (R^T * R)^{-1} * R^T * X_{ef} = D(X_{ef}, K_d, R) \end{aligned} \tag{16}$$

$$\begin{aligned} F(X_{ef}, K_f) = F(Y_2, K_f) &= F\big((S^T * S)^{-1} * S^T * X_{ef}, K_f\big) \\ &= F(X_{ef}, K_f, S) \end{aligned} \tag{17}$$

According to (16), (17), we can conclude that decryption is only related to matrix R, and feature extraction is determined by matrix S. If only the S is given, then the feature can be extracted, but the encrypted data cannot be decrypted. That is, decryption operation and feature extraction are mutual orthogonal and kept independent to each other.

According to (1)-(17), the system model for secure image

retrieval under cloud environment is shown in Fig. 1. There are three entities involved in this model: content owner who owns the images, cloud server who stores the encrypted images and performs image retrieval, and users who want to get images.

The retrieval process is given as.

1. Content owner generates B, performs n^{th} order orthogonal transform on X with B, and divides the result Y into encryption field Y_1 and feature extraction field Y_2. According to (5), (6), Y_{1e} is got after Y_1 is encrypted, and feature Y_{2f} is extracted from Y_2. According to (7), X_{ef} is calculated through the orthogonal composition with B from Y_{1e} and Y_2, then X_{ef} is uploaded to cloud server. Content owner only needs to save features Y_{2f} as search index.
2. Users send request to content owner. Content owner sends back features Y_{2f}, users send it to cloud servers as retrieval index.
3. Cloud server gets matrix S and K_f securely from content owner, and operates orthogonal decomposition on encrypted images. According to (17), features can be extracted and compared with the index sent by users, the closest image is the right one, and the encrypted image is returned to users.
4. Users get R and decryption key K_d securely from content owner, use it to decrypt the cipher-image.
5. According to (16), and get the image.

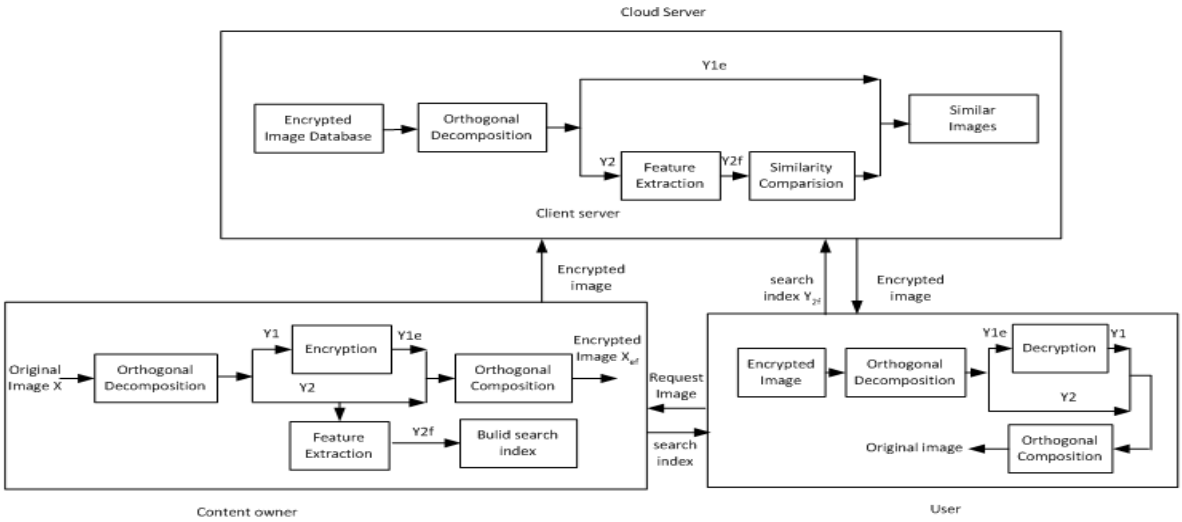


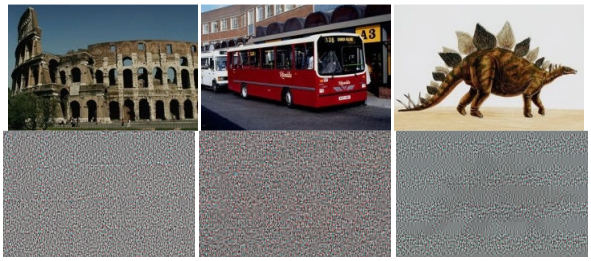
Fig. 1 System model of the proposed method

III. Experimental Results

In the experiments, we generate a 4×4 orthogonal matrix B = (b_1, b_2, b_3, b_4). Considering images need to be compressed for transmission or storage, we choose partial AC coefficients to form original host data X to reduce encryption's influences on compression. AC coefficients will be stored back into their original locations after they are processed. Using the proposed method, AC coefficients can be decomposed into two components. Advanced Encryption Standard (AES) is used to encrypt data and the method proposed in [10] is used to extract features. Then we perform the retrieval on an image database containing 1000 color images from the Corel dataset [11]. These images are grouped by content into 10 categories, with 100 images in each category.

A. Perceptual Security

Different from text/binary encryption, multimedia encryption requires not only cryptographic security, but also perceptual security. That is, both security against cryptographic attacks and perception unintelligibility should be satisfied. Since the proposed method has no specific requirements to cryptographic algorithms, we use the AES to encrypt data to achieve better security. In the proposed method, the encryption is only operated on selected data X, which means other coefficients are transparent, and this may decrease the security to a certain extent. To overcome these difficulties, we encrypt all of other important information, such as DC coefficients and other AC coefficients, in order to improve encryption security further. The encryption results are show in Fig. 2. From these Figs. 1, 2, we can see that encrypted images are unintelligible; also they have low PSNR value, which means good perceptual security.



(a) PSNR = 9.8654 (b) PSNR = 9.7506 (c) PSNR = 9.1041

Fig. 2 Encrypted Image Quality

B. Cryptographic Security

In our scheme, feature extraction operands, i.e. Y_2 and Y_{2f}, are unencrypted in the ciphertext. There exists the possibility that attackers make use of the unencrypted data as a security leak to attack the protected information, the degree to which the protected information may be revealed by the unencrypted data must be assessed.

Assume the protected image is C, C can be expressed as:

$$C = f(X, Z) = f_1(X) + f_2(Z) \quad (18)$$

where $f(\cdot,\cdot)$ is a linear function that is determined by an image encoding algorithm, X is a selected vector set, Z is other data. X can be encrypted by (5). The encrypted image, C_e can be reconstructed as:

$$C_e = f_2(Z_e) + f_1(X_e) = f_2(Z_e) + f_1(R, Y_{1e}) + f_1(S, Y_2) \quad (19)$$

In C_e, only $f_l(S,Y_2)$ is unencrypted, thus it is the only term that may lead to some information leakage. However, if X is properly defined and R, S is appropriately selected, the potential information leakage can be controlled within an acceptable range.

Also in our scheme, key R and S are sub-matrixes of B, they are not fully stochastic and independent numbers like a single secret key, which reduces the valid value space of R and S. Therefore the system is not secure unless two conditions are validated:

Condition 1: as secret keys, R and S can be adjusted independently to satisfy any predetermined security threshold, i.e., its key space is large enough to resist the brute force attack.

Condition 2: It is difficult for the server to deduce R through S.

According to (1), if n×n is the size of B, then the (1) consists of n(n-1)/2 quadratic polynomial simultaneous equations with n2 unknowns over a finite field F. If the elements of B are k-bit fixed word-length integer, then F denotes the field $[-2^{k-1}, 2^{k-1} - 1]$. This is an under-defined multivariate quadratic equations problem. MQ is NP-hard. Some algorithms have been proposed for solving MQ faster than using an exhaustive research, but most of them did not change the general exponential, thus increasing the complexity characteristics.

With respect to this problem, the attacker who does not know any of keys is considered first. Assume an attack of B by (1). Then, the complexity can be expressed as:

$$d_B = d_{MQ} + N_{MQ} d_0 \quad (20)$$

where d_B denote the total measure of complexity for attacking B, d_{MQ} denotes the complexity for solving the MQ solutions of B, N_{MQ} denotes the number of all the expected solutions of B, and d_0 denotes the complexity for checking the whether the solution is the correct solution. Because there are N_{MQ} possible solutions for B, the attacker must check the solutions one by one to find the true result. To do this, he has to substitute (7) with the candidate for B. However, K_d and K_f are unknown, thus the checking complexity nearly equals that of attacking K_d and K_f.

Equation (1) is an instance of MQ, where the number of unknowns is approximately 2 times the number of equations. In the practical applications of (1), d_{MQ} can be roughly estimate as $2^{n^2k-k_m}$, where k_m is the factor that includes the efficiency improvement achieved over an exhaustive achieved over an exhaustive search by using a different algorithm. In most instances, k_m can be ignored because $k_m \ll n^2$kif n and k are sufficiently large. N_{MQ} is approximately $2^{n(n+1)k/2}$. To ensure the security of K_d and K_f, assume there is a threshold K_0, that the keys should exceed, thus d_0 can reasonably be set 2^{k_0}. Thus the complexity for attacking B tends to increase exponentially as $O(n^2k)$ as:

$$d_B \sim 2^{n^2k-k_m} + 2^{\frac{n(n+1)(k-1)}{2}+k_0} \quad (21)$$

From (21), it shows that R and S, which are the B sub-matrixes, can be adjusted independently to satisfy any predetermined security threshold by set rational n and k. Therefore condition 1 is met.

If R and S cannot be mutually derived, condition 2 can be met. The proof is given as follows:

If the server is attacking the encrypted part, (1) and the known S are used to attack R first. If m denotes the number of columns in S, and S is known, then applying (1) to solve R becomes:

$$\begin{cases} r_i^T * r_j = 0 & \text{if } i \neq j \quad 0 \leq i, j \leq n - m \\ s_i^T * r_j = 0 & 0 \ll i \ll m, 0 \ll j \ll n - m \end{cases} \quad (22)$$

Equation (22) consists of (n-m)(n-m+1)/2 quadratic equations and m (n-m) linear equations with n(n-m) unknowns. By using Gaussian elimination, m (n-m) unknowns can be eliminated using the linear equations. The complexity of this step is $O(m^3(n-m)^3)$. Then, the quadratic parts are under defined multivariate quadratic equations, with (n-m) (n-m+1)/2 quadratic equations and $(n-m)^2$ unknowns. It is still a typical MQ equation system, similar to the equations of B, however, n is replaced by n-m. Referring to the result of B from (21), the complexity for attacking R with a known S can be estimated as:

$$d_R \sim 2^{3k\log_2^{m(n-m)}+m^2k-k_m} + 2^{\frac{m(m+1)k}{2}+k_0} \quad (23)$$

According to (22), (23), the complexity of attacking B and R are exponential, increasing with $O(n^2k)$, $O(m^2k)$, respectively. Thus provide the criteria for the proper choice of the parameters B, R to achieve computational security of the scheme. For example, if n=8, m=4, and k=16, the complexity for B and R must be of order $2^{1024-k_m} + 2^{476+k_0}$, $2^{448} + 2^{160+k_0}$, respectively, which satisfies the security requirements of most applications. The parameter Km is neglected in the latter two cases because all currently available QM accelerated algorithms are more effective than an exhaustive search only for massively large cases.

The above analysis proved that condition 2 could also be

met.

C. Security in Retrieval

Content-based Image retrieval relies on comparing different visual features to capture visual or semantic similarity between images. If visual features are used as index, then it is possible that the adversary may compares them with features of other known images, as a result they may probe the content of encrypted images using known images and information leakage is inevitable. In the proposed scheme, we extract features from part of orthogonal decomposition coefficients and use them as index to retrieve images. These extracted features are different from those features extracted from images directly, and it is hard for the adversary to infer image content from this information.

D. Comparison on Retrieval Accuracy

Retrieval accuracy is measured using precision-recall curves, where precision and recall are defined as:

$$\text{precision} = \frac{\text{number of relevant images among retrieved images}}{\text{number of retrieved images}}$$

$$\text{recall} = \frac{\text{number of relevant images among retrieved images}}{\text{number of relevant images in the database}}$$

A higher precision value at a given recall value indicates that the retrieval performance is better. We compare our experimental results with the methods proposed in [7], [8], and the results are shown in Fig. 3. We can see that our methods get a better retrieval performance than other methods in Fig. 3.

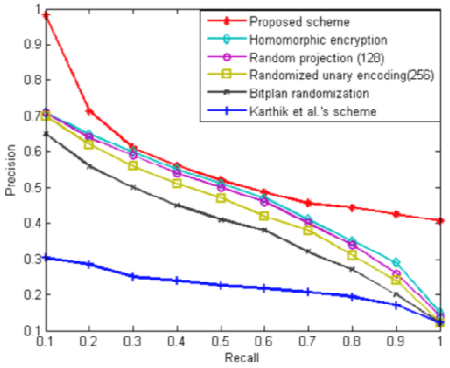


Fig. 3 Comparison of Retrieval Performance

IV. Conclusion

A secure image retrieval method based on orthogonal decomposition is proposed in the paper. By using orthogonal transform, an image is decomposed into two orthogonal fields components, therefore the encryption and feature extraction can be operated separately. Two components are integrated to form the final data after inverse orthogonal transform. By this method, the cloud server can retrieve encrypted image retrieval directly without violating data privacy. Different from other methods reported in the literatures, the proposed method has no restrictions in using specific encryption algorithms; this makes the proposed method more universal, thus accommodating different kinds of applications.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 41371402, 61402421.

References

[1] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches in encrypted data", in Proc. IEEE Symp. Res. Sec. Privacy, Feb. 2000, 44-55.
[2] D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public-key encryption with keyword search", in Proc. Eur., 2004, 506-522.
[3] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L. Varna, S. He, et al., "Confidentiality preserving rank-ordered search",in Proc. ACM Workshop Storage, Sec., Survivability, 2007, 7-12.
[4] C. Wang, N. Cao, J. Li, K. Ren and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data". in Proc. IEEE 30th International Conference onDistributed Computing Systems (ICDCS),2010, 253-262
[5] N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy-Preserving 5Multi-Keyword Ranked Search over Encrypted Cloud Data". IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1), 222-233
[6] W. Lu, A. Varna and M. Wu, "Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization", IEEE Access, Vol.2, 2014, 125-141
[7] W. Lu, A. L. Varna, A. Swaminathan, and M.Wu, "Secure image retrieval through feature protection", in Proc. IEEE Conf. Acoust., Speech Signal Process., Apr. 2009, pp. 1533_1536
[8] K Karthik, S Kashyap. "Transparent hashing in the encrypted domain for privacy preserving image retrieval". Signal, Image and Video Processing. 2013, 7 (4), 647-664
[9] C. Hsu, C. Lu, and s. Pei. "Image Feature Extraction in Encrypted Domain With Privacy-Preserving SIFT", IEEE Transactions on Image Processing, 2012, 21(11), 4593-4607
[10] G. Schaefer, "JPEG image retrieval by simple operators," in 2nd International Workshop on Content Based Multimedia and Indexing, 2001, pp. 207–214.
[11] (Online). Available: http://wang.ist.psu.edu/_jwang/test1.tar