IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 22-26
www.iosrjournals.org

Image Retrieval using Sparse Codewords with Cryptography for Enhanced Security

Munmun N. Bhagat
Department of Computer Engineering
Sinhgad Academy of Engineering,
Kondhwa, Pune, India.

Prof. B. B. Gite
HOD, Department of Computer Engineering
Sinhgad Academy of Engineering,
Kondhwa, Pune, India.

Abstract: *Now days face image of people is the interesting area of users. Most of the time images are in digital form. Thus, content-based face image retrieval is a technique which facilitates for many emerging applications. In this paper, automatically detected human attributes are used to enhance the performance of content based face image retrieval. Here, low level features of image are combined with high level features of image to get more efficient results about image retrieval. In this work, semantic codewords for face retrieval are constructed by using semantic cues of the face image to improve content based face image retrieval. Secured Quick Crypt (SQC) encryption algorithm is applied on images when they are transferred via network. This will protect image from getting attacked. The proposed method can achieve a set of relevant and secured results as compared to the existing methods.*

Key Words: *Content based image retrieval, human attributes, encryption, decryption.*

I. Introduction

In this paper, the challenge of large scale face image retrieval is getting addressed. The challenge like large scale face image retrieval is seen in retrieval technique as content based face image retrieval. In traditional face retrieval methods low level features are used to represent faces [1,2]. But the drawback of low level features is that they lack of semantic meanings whereas face images have variance in expressions, posing, etc. Face images of different people might match according to low level features. This might produce ambiguous result. By combining high level human attributes and low level features; better retrieval results are achieved along with better representation of feature.

Attributes which are extracted automatically from human face image are the source of high level feature description about a particular human being[3]. Automatic human attribute detection helped many recent researchers to get efficient results in areas like verification of face [3], identification of face [5], keyword based face image retrieval [6] and similar attribute search. Though human attributes are very useful for operations related to face image but it is not the case with content based face image retrieval task. There are two major reasons behind this and the first reason is that vector of floating points will not work well with large scale indexing methods. Vectors of floating points represent human attributes. This results in low response and scalability issues as it is not completely supporting huge amount of data. Second reason is that the limited dimensions of human facial characteristics. Although the dataset consist of lots of images, but it may lose some people which may look similar because of similarity in some attributes.

Content base face image retrieval detects automatically and take advantage of the features of human in order to improve the image retrieval. This proposes to combine the two orthogonal methods; attribute enhanced sparse coding and attribute embedded inverted indexing. The attribute enhanced sparse coding utilizes high level features like human attributes along with low level features which construct semantic codewords in offline stage. Attribute embedded inverted indexing considers human attributes in binary signature of particular query image and provides efficient retrieval in online stage [3]. By combining these two methods, a large scale content based face image retrieval system is built by having advantages of both low level and high level facial features.

In this technique, there is a chance of attack on image when it is getting transferred from one system to other. SQC encryption algorithm is applied on image to avoid any type of attack. After indexing, a set of retrieved images is produced. These images from set are then encrypted by SQC algorithm.

II. Literature Survey

Content based image retrieval technique works with low level attributes as color, shape, and texture of the query image. This method can achieve high precision on retrieval of rigid object, causes low recall problem because of semantic gap [9]. Many researchers have been focused on the task of bridging semantic gap; by which performance of content based image retrieval is improved. In traditional content based image retrieval, intensive human annotations are used for constructing semantic codewords. In this paper, automatically detected attributes are used to construct semantic codewords for retrieval of face image instead of using tags.

Taking advantage of the simplicity and effectiveness of the sparse coding to local binary pattern (LBP) feature improved characteristics of Face images, the same approach as Chen et al. Combining component based LBP with sparse coding to construct sparse codewords [2]. However, rather than using manual tags for identity information, this system have utilized automatically detected human attributes to construct sparse codewords by attribute enhanced sparse coding.

In addition, we further characterized the information from the orthogonal view to construct attribute embedded inverted indexing for online stage. The proposed methods can combine both advantages of identity information and automatically detected human attributes [2].

Although, the advantages of both the methods are combined, but this may fail in terms of security measure of images. Hence to protect the images from any attack when they are transferred in online stage SQC encryption algorithm is applied. SQC algorithm is applied on image before it is getting transferred from one system to other. The input to the encryption and decryption algorithms is a single 128-bit block. The key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words. Each word is four bytes, and the total key schedule is 44 words for the 128-bit key. Note that the ordering of bytes within a matrix is by column. So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the in matrix, the second four bytes occupy the second column, and so on. Similarly, first four bytes of the expanded key, which form a word.

The cipher is based on the same basic principle of the AES technique [7]. Block Ciphering is performed; each block of plain text as well as that of the Cipher Key is128bits. As key size is 128bits, 10 rounds will be applied for encryption. Each round will consist of XOR operation, sub-bytes operation and shift rows operation.

Here, to compensate for the less number of rounds that each block of plain text undergoes, send the round key of the last round to be the cipher key of the next round. Thus level of pseudo-randomness is generated amongst the entire text. Cryptanalyst would find different Cipher text for the same plain text repeated in the course of document [11].

III. Implementation Details

For each image in the database, first apply a viola-Jones face detector to find the locations of the faces from image. Use the structure proposed in [4] in order to find 73 different attribute scores. 68 different facial landmarks are located by applying active shape model. Extract 7x5 grids, where each grid looks like a square patch. Here, we get a total of 175 grids from five components and that are two eyes, one nose tip, and two mouth corners. A local binary pattern is extracted from each grid. After receiving the local descriptor , sparse coding properties increased use of embedded codewords in each descriptor quantize the inverted index is built for efficient retrieval features. These retrieved images will then go under SQC encryption algorithm. Then image will get converted into coded format so that no unauthorized person can read it. The complete system of image retrieval is illustrated in figure 1.

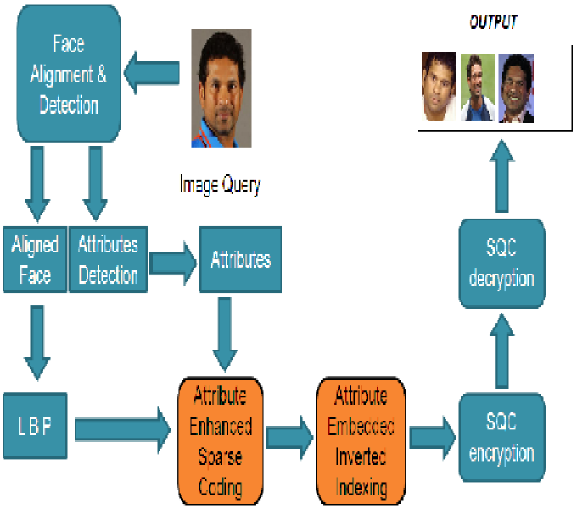

Face Alignment & Detection
Image Query
OUTPUT
Aligned Face
Attributes Detection
Attributes
SQC decryption
LBP
Attribute Enhanced Sparse Coding
Attribute Embedded Inverted Indexing
SQC encryption

Figure 1: proposed architecture of image retrieval system   with enhanced security

3.1. Attribute enhanced sparse coding

Sparse coding exploits the global structure of the feature space for the construction of code words and meanings, combined with low level features. Many important uses human characteristics to consider in the sparse representation, we first codewords contain different images with different attribute values to force the dictionary selection propose to use. For a single human characteristic, we divided two distinct subsets dictionary centroids, with scores of positive attributes and negative attributes images will use a subset of the images with scores of other. If an image is a positive male trait scores, for example, the dictionary will use the first half of centroids and vice versa. These are the images with different characteristics would certainly different codewords. Several characteristics of the cases, we have a number of features based on sparse representation is divided into several segments, and each segment characterized by sparse representation is generated.

$$\min_{V} \sum_{i=1}^{n} \|x^{(i)} - Dv^{(i)}\|_2^2 + \lambda \|z^{(i)} \circ v^{(i)}\|_1$$

$$z_j^{(i)} = \begin{cases} \infty, & \text{if (1) } j \geq \lfloor \frac{K}{2} \rfloor \text{ and } f_a(i) \geq 0 \\ & \text{(2) } j < \lfloor \frac{K}{2} \rfloor \text{ and } f_a(i) < 0 \\ 1, & otherwise, \end{cases} \quad (1)$$

Where, “o” shows the multiplication between two vectors, *fa* (i) denotes the attribute score for ith image, and z(i) is a mask vector which decides codewords used by image i. if an input image has positive attribute value then only the first half of the sparse representation contains non-zero value for the image patches, and if not then sparse representation contains zero value for the image patches. Human attributes are encoded by equation (1) in sparse representation. The detection of possible errors in attributes is not strong as automatically detected human attributes are not error free. Human attributes are encoded as binary indicators but in real they are relative confidence scores. To overcome these limits, half of the dictionary centroid is set to +1 which will represent positive attribute and remaining half is set to -1 which will represent negative attribute of image; illustrates equation 2. If the attribute scores are similar then they have similar weight vector as attribute score decides weight. This results in similar codewords and hence results in similar sparse representation. Attribute vector is defined as a€{1,-1}^k where, the attribute scores of the jth centroids are contained in aj.

$$a_j = \begin{cases} +1, & \text{if } j \geq \lfloor \frac{K}{2} \rfloor \\ -1, & otherwise, \end{cases} \quad (2)$$

Hence, equation (1) becomes as;

$$z_j^{(i)} = \exp(\frac{d(f_a(i), a_j)}{\sigma}) \quad (3)$$

Where, d(fa(i),aj) is the distance between the jth dictionary centroid and the attribute score of the ith patch of image, and σ adjusts the decaying weights.

3.2. Attribute embedded inverted indexing

The method described here is to adjust the block inverted index structure using human attributes.

3.2.1. Image Ranking And Inverted Indexing

Non zero entries in sparse representation creates a set of codewords. The similar identity is then computed by as follows,

$S(i,j) =$ || c^i ∩ c^j || (4)

3.2.2. Attribute Embedded Inverted Indexing

As shown in figure 2, sparse codewords and binary attribute signatures will produce the result for attribute embedded inverted indexing. The binary attribute signature is used to embed attribute details to index structure along with sparse codewords.

$$b_j^{(i)} = \begin{cases} 1 & \text{if } f_a^{(i)}(j) > 0 \\ 0 & otherwise, \end{cases} \quad (5)$$

The modified similarity score is,

$$S(i,j) = \begin{cases} \|c^{(i)} \cap c^{(j)}\| & \text{if } h(b^{(i)}, b^{(j)}) \leq T \\ 0 & otherwise, \end{cases} \quad (6)$$

Where, hamming distance between I and j is denoted by h(i,j) and T is fixed threshold.

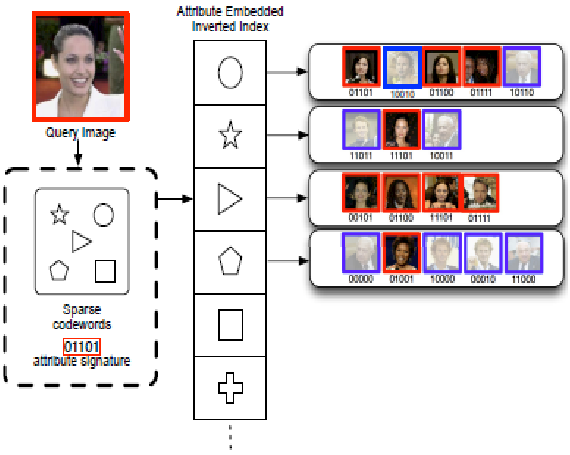


Figure 2: attribute embedded inverted indexing

3.3. 3. SQC Encryption Algorithm

The steps involved in SQC encryption algorithm are listed below;

1. XORing each cell of the Block with the respective cell of the cipher key.
2. Perform the Sub-bytes operations on each cell as done in AES.
3. Shift the rows; Left Rotate 2nd row once, Left Rotate 3rd row twice and Left Rotate 4th row thrice.
4. Perform a simple matrix multiplication between Rijndael mix column matrix and the current block.
5. Generate the round key (directions given below) and XOR with each cell of the block.

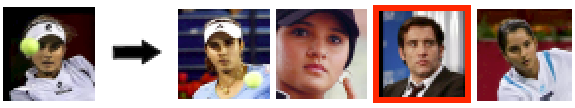
After performing these 5Steps, we receive a block of the cipher text (in Unicode). Only one round is applied for each block.

A chaining mechanism is provided by sending the current round key to be the cipher key of the next round. The method to generate the round key is as follows:

1. Swap the first and last columns of the cipher key.
2. Right rotate 2nd row of the cipher key once.
3. Left rotate 3rd row of the cipher key twice.
4. XOR first and last rows of the cipher key.

IV. Results

The proposed system makes use of different algorithms at each stage so as to achieve better performance. The proposed system will assure to retrieve similar images. When at input side an query image is provided for similar images as result then after all image processing operations are done on image; set of similar images is get as output. This is shown in figure 3.



(a) (b) (c) (d) (e)

Figure 3: expected output (a) is the query image. (d) Dissimilar retrieved image. (b), (c), (e) similar retrieved images as output.

In case of online image retrieval system, these images from output set are encrypted. At receivers side these are decrypted to retrieve them in original form.

V. Conclusion

Here two orthogonal methods are combined to utilize automatically detected human attributes to significantly improve content-based face image retrieval. Here, by combining low-level features and automatically detected human attributes for content-based face image retrieval, the image retrieval is efficient. Attribute-enhanced sparse coding uses automatically detected human attributes to construct semantic code words in the offline stage. Attribute-embedded inverted indexing further considers the local attribute signature of the query image and still ensures efficient retrieval in the online stage. This technique may reduce the quantization error and achieve salient gains in face retrieval on two public datasets. As SQC algorithm is applied on final output; the chances of attack on output get reduced in case of online stage.

References

[1] Z. Wu, Q. Ke, J. Sun, and H.-Y. Shum, “Scalable face image retrieval with identity-based quantization and multi-reference re-ranking,” IEEE Conference on Computer Vision and Pattern Recognition, 2010.

[2] B.-C. Chen, Y.-H.Kuo, Y.-Y.Chen, K.-Y.Chu, and W. Hsu, “Semisupervised face image retrieval using sparse coding with identity constraint,” ACM Multimedia, 2011.

[3] Bor-Chun Chen, Yan-Ying Chen, Yin-HsiKuo, Winston H. Hsu, “Scalable Face Image Retrieval using Attribute-Enhanced Sparse Codewords”, IEEE Transactions onMultimedia, 2013.

[4] N. Kumar, A. C. Berg, P. N. Belhumeur, and S. K. Nayar, “Describable visual attributes for face verification and image search,” in IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), Special Issue on Real-World Face Recognition, Oct 2011.

[5] W. Scheirer, N. Kumar, K. Ricanek, T. E. Boult, and P. N. Belhumeur, “Fusing with context: a bayesian approach to combining descriptive attributes,” International Joint Conference on Biometrics, 2011.

[6] B. Siddiquie, R. S. Feris, and L. S. Davis, “Image ranking and retrieval based on multi-attribute queries,” IEEE Conference on Computer Vision and Pattern Recognition, 2011.

[7] William Stalling, “Cryptography and Network Security: Principles and Practices”, fourth edition, Pentice Hall.

[8] P.Karthigaikumar, SoumiyaRasheed, “Simulation of Image Encryption using AES Algorithm”, IJCA: Computational Science - New Dimensions & Perspectives” NCCSE, 2011

[9] O. Chum, J. Philbin, J. Sivic, M. Isard and A. Zisserman, “Total Recall: Automatic Query Expansion with a Generative Feature Model for Object Retrieval,” IEEE International Conference on Computer Vision, 2007.

[10] TimoAhonen, AbdenourHadid, and MattiPietikainen,” Face Recognition with Local Binary Patterns”, Springer-Verlag Berlin Heidelberg 2004.

[11] Hiroki Endo, Yoshihiro Kawahara, and TohruAsami, ―A Self-Encryption Based Private StorageSystem Over P2P Distribution File SharingInfrastrure‖, 12-13 May 2008, 69 – 76.