Privacy-Preserving Outsourcing of Medical Image Data using SIFT Descriptor

Shubhangi D.C.1*, Sabahat Fatima2

1HOD, Dept. Computer Science and Engg, VTU PG Center, VTU University, Kalaburagi, India
2Dept. Computer Science and Engg, VTU PG Center, VTU University, Kalaburagi, India

Corresponding Author: shubhangidc@vtu.ac.in,

Received 17th May 2017, Revised 29th May 2017, Accepted 20th Jun 2017, Online 30th Jun 2017

Abstract—Outsourcing huge amount of personal multimedia data in these days become a challenging task for the data owners which is greatly motivated by the advances in cloud computing by using its several resources for cost saving and flexibility. Despite these facts, outsourcing of multimedia data may leak the data owner’s private information, such as the personal identity, locations, or even financial profiles. In this paper, we present an effective and practical privacy-preserving computation outsourcing protocol for persuading scale-invariant feature transform (SIFT) over huge encrypted image data. We first explain the previous solutions to this problem which is either efficiency or security issues, and no one can well maintain the important functionality of the original SIFT in terms of distinctiveness and robustness. Next, we present a new scheme that achieves practicality requirements along with the maintenance of its key functionality, by first splitting the original image data and designing two novel efficient protocols for secure calculations like multiplication and comparison, then carefully distributing the feature extracted onto two independent cloud servers. Which results into practically secure solution and outperforms the state-of-the-art, with the original SIFT in terms of various characteristics, including rotation invariance, image scale invariance, robust matching across affine distortion, and an addition of noise and change in 3D viewpoint and illumination. To deal with the privacy of important medical multimedia data we took brain tumor as our case study. The Brain Tumor is affecting many people worldwide. It is not only limited to the old age people but also detected in the early age. The encrypted images are stored in the cloud. From the encrypted images we will check for brain tumor using OpenCV and preserve this information by getting revealed using our proposed method.

Keywords—Image matching, scale invariant feature transform (SIFT), Difference of Gaussian (DoG).

I. INTRODUCTION

With the advancement in big data and cloud-based data services, owners of the data are overly encouraged to store their large amount of personal multimedia data onto the cloud. Apart from enjoying the great storage, cost saving and the flexibility, the outsourcing of data and assess to the cloud also increase privacy and security concerns [2]-[5]. Now a day’s large number of users are disposed to outsource the computation of feature extraction to the cloud directly [6] but the fact is exposing the original image data directly to some semi-trusted cloud service provider may automatically reveal data owners private information such as the personal identity, locations, or even financial profiles etc. To avoid this problem best approach [7]-[10] is to encrypt the personal multimedia data before outsourcing. In order to provide powerful end to end privacy, encryption of data also becomes a hurdle to data computation and utilization. Now the main challenging task [11] is to determine authorization for privacy preserving feature extraction over massive image data while it would appear that relieving the high computation burden of the database owner and depending on the cloud for fast and effective feature extraction, it is still unfit to remove the edge responses such that the identified key points are unstable to small amount noise. Motivated by all these observations, in this paper, we present [1] an effective and practical privacy-preserving computation outsourcing protocol for persuading scale-invariant feature transform (SIFT) over huge encrypted image data. The main idea of all image processing techniques is the visualization under consideration. Segmentation or splitting of images holds a key position in the field of image processing. Segmentation is one of the main steps in feature extraction, measurements, and displaying of the image, especially for medical imaging. A brain tumor is usually defined as a mass which develops because of abnormal cell growth within the brain. There are two categories of brain tumor one is benign and another is the malignant tumor [12]. A benign tumor is slow growing, cancerous tumor whereas malignant are fast growing tissues. Almost all of the tumors are life frightening.
the brain tumor is one among them. Some of the brain tumors directly originated in the brain itself and some are results from another part of the body. Here we deal with the privacy of important medical multimedia data and also from the encrypted images we will check for brain tumor using OpenCV.

II. PROBLEM STATEMENT

Previous attempts on privacy-preserving outsourcing computation have been constant to different mathematical problems including linear equations [13], modular exponentiation [14], and kNN search [15]. Numerical problems of engineering computations have mainly focused on these works. Now in recent years, privacy-preserving data search in the ciphertext area has been extended to content-based multimedia retrieval [16], face recognition [17], and fingerprint identification [18]. The Author can only be explored how to enable secure image search in the data outsourcing environment. Nevertheless, they all assume that the images have been pre-processed by some feature extraction algorithms to obtain their vector representations. Due to the importance of image feature extraction in multimedia data processing and its heavy operations on massive data, especially for biomedical data for its huge size and a large number of feature points, the extraction of image features from the ciphertext area has started to attract more and more research interest. They all lack comprehensive analysis and evaluations with respect to the preservation of the key characteristics of the original image feature extraction algorithm. It is unable to eliminate edge responses such that the detected key points are unstable to small amount noise. It is expensive and less flexible.

III. PROPOSED SYSTEM

To overcome the limitations of the existing system and to improve the world we put forward[1] an effective and practical privacy-preserving computation outsourcing multimedia protocol for persuading scale invariant feature transform (SIFT) over huge multimedia data. Initially, we randomly split the data into two parts and distribute them to two different cloud servers and we propose two secure interactive protocols that are batched secure multiplication protocol (BSMP) and batched secure comparison protocol (BSCP) using somewhat homomorphic encryption (SHE) [19] along with the latest batching technique single-instruction multi-data (SIMD) [20],[21]. The BSMP [22] allows the two cloud servers to carefully enumerate the products of their multiple inputs concurrently, while BSCP [23] allows them to compare these multiple pairs of private input simultaneously with privacy preservation. Using these two interactive protocols, we then further design a new approach which allows the two servers combinedly detect the exact location of the points via the difference-of-Gaussian (DoG), and their main orientations by calculating it from orientation range instead of taking it from encrypted versions of orientation histogram. Lastly, by utilizing the add-on properties of encrypted images, the data holder can retrieve the original features from the encrypted descriptors produced by the two cloud servers and stopping them from taking original information. Later we are making use of this encrypted brain images to detect the brain tumor and further processing using the same. It provides both a detailed security analysis and an extensive privacy evaluation to demonstrate the privacy-preserving guarantee of our design. It is secure, efficient, and outperforms the original SIFT practically.

IV. PROPOSED METHODOLOGY

A. Image Encryption

The data owner O, who holds a private image I, encrypts it and sends the encrypted sub-images I1 and I2 to servers S1 and S2, respectively. Then, S1 builds their own Gaussian scale spaces Li (x, y, σ) and difference-of-Gaussian spaces Di (x, y, σ) based on Ii (i = 1, 2).

B. Keypoint Localization

S1 and S2 run a keypoint localization protocol based on BSCP to find the candidate keypoint locations without compromising the privacy of their own inputs. Then they will eliminate edge responses to obtain stable keypoints with the aid of BSMP. Finally, the locations are revealed to the two servers.

C. Orientation Assignment

S1 and S2 run an orientation assignment protocol based on BSCP. By using the orientations of each sample point around the key point (computed in Step 1), they will further build their orientation histograms H1 and H2, respectively. Then, the peaks are found in the original orientation histograms H by using H1 and H2, and each peak corresponds to the main orientation (computed in Step 2). Finally, the image data will be rotated relative to the main orientations, and each rotation generates a feature descriptor for a key point.
D. Descriptor Generator
S1 and S2 build orientation histograms with the directions that have been computed in the above steps without interacting with each other. Then, they respectively transform the orientation histograms into encrypted feature descriptors V1 and V2 and send them to the data owner. This phase is called Descriptor Generation Protocol. Finally, the data owner can recover the real feature descriptors from V1 and V2.

E. Preprocessing and Enhancement of an Image
This is the first step of image processing it is used to enhance the chances of detecting the suspicious region. Finer details of the image are enhanced and noise is removed from the image. Clinical MRI, when corrupted by noise, reduces the accuracy of the image. Various filters are used to remove this noise. The anisotropic filter is used to remove background noise, a weighted median filter is used to remove salt and pepper noise. The wavelet-based denoising method makes wavelet and scaling coefficient biased. The original image and image after enhancement is shown in figure 2.

![Original image and Enhanced image](image)

**Fig. 2: Image enhancement**

F. Segmentation method
Image segmentation method involves dividing the image into several small parts. This method helps in the analysis of data. The three different types of segmentation method are as follows:

1. Boundary approach or Thresholding
   One of the common methods of segmentation is boundary approach. It is the gray value remapping method where if we consider \( p \) to be as an operation then given by the following equation (1),
   \[
   p(v) = \begin{cases} 
   0 & \text{if } v < t \\
   1 & \text{if } v \geq t 
   \end{cases} \quad (1)
   \]
   where \( v \) represents gray value and \( t \) represents threshold value.
   This method used to convert gray image into a binary image. After this method image will be split into two values 0 and 1.

2. Edge approach
   In this edge-based segmentation method, the edges of the image which are detected will be assumed as object boundaries which will be helpful in identifying these objects. This method has more chances of giving false edge detection hence it rarely gives distinct, absolute and closed boundaries needed for a direct segmentation and many of the times it requires edge linking to join the partial edges into an object boundary.

3. Region approach
   This type assumes that all the pixels at the edges within one region will have similar values. It only interested in object region not on its edges. It compares one pixel with its neighbours, if the congruence criteria satisfy, then the pixel can be set to belong to the cluster as one or more of its neighbours. PSO clustering algorithms are used in this type of approach.

G. PSO (Particle Swarm Optimization)
   It is a population-based search algorithm which is initiated with the randomly selected populations, also called as particles. All the particles in the PSO have their individual fitness value, which can be calculated by the fitness function. They also have the velocity which directs the flying of the particle in search space. Unlike GA, PSO does not have a direct recombination operator. The drawback of PSO is, the swarm may prematurely converge as there is rapid information flowing between particles. It is also problem reliant as the output relies on the parameter setting of the algorithm.

H. Feature Extraction
   Extracting the exact tumor is a crucial task in case of the brain tumor because of the complex structure of the brain. Certain parameters are taken into account for feature extraction as size, shape, composition and a location of the image. As per the results obtained from the feature extraction the classification of the tumor is done.

V. RESULTS AND DISCUSSION
   We have conducted various experiments to evaluate the effectiveness and the efficiency of our proposed scheme using representative real world image dataset.

A. Effectiveness evaluation
   In this first, we deal with descriptor evaluation, where we compare our proposed method with the existing schemes. In fig.1, we plot recall VS.1-precision [24] for image matching experiment by varying the distance ratio threshold. In Fig.1 (a), the target images are rotated by 200 and scaled by 20%. The result indicates that previous schemes will generate much more false matches than our proposed scheme. Fig.1 (b) is obtained when the target images have a 3D viewpoint change of 200. The result shows both the scheme having the same performance. Fig.1(c) measures the performance for images with a significant amount blur which is introduced by changing the camera focus. The result shows all descriptors generated by all schemes are affected by this type of image degradations. But our scheme clearly dominates previous schemes. Fig. 1(d) shows the results for illumination changes which have been obtained by changing the camera setting. It again shows that our scheme performs better than the
competing approaches. After descriptor evaluation we put key point matching experiment, we manually set the threshold to have each scheme return only 10 matches, which contain correct matches and false positives. It clearly shows that our approach outperforms the others in finding correct matches. Then we put image retrieval experiment [25] to evaluate the descriptors inspired from. By examining it clearly, shows that our proposed scheme receives much more votes than the original SIFT and our scheme gets more key point generated and less false positives.

**B. Efficiency evaluation**

We evaluate the computation efficiency of privacy preserving outsourcing of SIFT outsourcing with the increase of image size on the data owner side. Fig.2 (a) shows the time cost of performing SIFT algorithm locally and that of outsourcing of SIFT scheme. As for the communication cost on the data owner side as illustrated in Fig.2 (b), since the data owner only sends two split images to the two cloud servers and receive two split descriptors with fixed size, our scheme and previous to that having same communication overhead which grows linearly with the image size.

In Fig.3, we evaluate the time cost and the communication cost of our scheme on the server side. Fig.3 (a) shows the time cost on the servers. With the increase of image size, the time cost in garbled circuit grows much faster than that of BSCP, and SPP [26] also consumes much more than BSMP. Fig.3 (b) evaluates the communication cost between two servers which is generated by using BSCP and BSMP.

Finally, for the memory cost on the servers, for a \( n \times n \) image it at most needs \( 12n \times n \) bytes where 12 is a predefined parameter to decide the number of scales in scale space. Thus when \( n=3000 \) the memory cost is about 103MB, which is still acceptable for an off-the-shelf machine, let alone a powerful cloud server.

**VI. CONCLUSIONS**

Privacy-preserving outsourcing of medical image gives the assurance of acquiring feature descriptors which depend on private data without leaking privacy of our data holders, along with the huge cloud computation resources. Nevertheless, existing solutions for secure outsourcing SIFT have many issues like security or efficiency, and none can effectively protect important characteristics that are robustness and distinctiveness of the original SIFT. In our proposed system we suggested two novel secure interactive protocols BSMP and BSCP for privacy preserving SIFT outsourcing of medical data. We attentively examine effectiveness and security of our approach. Our experimental evaluation shows that proposed work beat the most recent ideas comparable to the original SIFT and is feasible for real-world practice.

**REFERENCES**


