Journal of Cyber Security
DOI:10.32604/jcs.2020.09703
Article

Tech Science Press

Image Feature Computation in Encrypted Domain Based on Mean Value

Xiangshu Ou[1], Mingfang Jiang[2,*], Shuai Li[1] and Yao Bai[1]

[1]Department of Mathematics and Computational Science, Hunan First Normal University, Changsha, 410205, China
[2]Department of Information Science and Engineering, Hunan First Normal University, Changsha, 410205, China
[*]Corresponding Author: Mingfang Jiang. Email: mingfangjiang@hnfnu.edu.cn

Received: 15 January 2020; Accepted: 23 July 2020

Abstract: In smart environments, more and more teaching data sources are uploaded to remote cloud centers which promote the development of the smart campus. The outsourcing of massive teaching data can reduce storage burden and computational cost, but causes some privacy concerns because those teaching data (especially personal image data) may contain personal private information. In this paper, a privacy-preserving image feature extraction algorithm is proposed by using mean value features. Clients use block scrambling and chaotic map to encrypt original images before uploading to the remote servers. Cloud servers can directly extract image mean value features from encrypted images. Experiments show the effectiveness and security of our algorithm. It can achieve information search over the encrypted images on the smart campus.

Keywords: Privacy-preserving; image encryption; cloud computing; mean value

1 Introduction

Nowadays, cloud computing, mobile Internet, Internet of Things, and artificial intelligence have developed rapidly and achieved remarkable progress. Human society has entered a new era of smart technology including smart medicine, smart transportation, and smart education. Public data storage service has become a tendency in the smart era. However, this outsourcing scheme of data storage and data computation brings about the security risk of user data stored in remote the third party. Especially, as for smart education application, those outsourced data stored in the cloud server may contain personal private information of students. Privacy security of outsourced data is becoming an increasingly urgent issue [1]. Privacy-preserving data outsourcing schemes provide an effective way to solve this problem, which can protect user privacy without sacrificing the usability and accessibility of the information [2–4].

In a typical search scheme over encrypted data, encrypted data is stored at the remote server. The query from the clients is transformed into a representation such that it can be processed directly on encrypted data in a remote server. The retrieval results might be processed by the client after decryption to determine the final answers [5]. Park et al. [6] focused on applicable group search schemes over encrypted data. the new schemes enable search over encrypted documents without the need of re-encrypting all documents in a server even though group keys must be updated. Tian et al. [7] proposed an encrypted search scheme based on inverted-index by using encrypted index creation, search, and maintenance strategies. It achieves satisfactory medical data confidentiality without revealing user privacy and can be applied to the privacy protection of medical information. Considering that the scale-invariant feature transform (SIFT) has been widely used in various image processing fields, Hsu et al. [8] proposed a secure SIFT feature extraction and representation method using Paillier cryptosystem. Qin et al. [9] presented a privacy-preserving feature detection approach for encrypted images, which enables a remote server to perform image feature computation while protecting user privacy in image contents. Hu et al. [10] proposed a practical privacy-preserving SIFT feature computation outsourcing protocol. It met efficiency and security requirements simultaneously by randomly splitting original image data, and distributing the feature computations onto two independent cloud servers. Wang et al. [11] designed a privacy-preserving Histogram of Oriented Gradients (HOG) outsourcing scheme. It moves all image feature computation to untrusted cloud servers without revealing the data owner's private information. Qin et al. [12] proposed a secure SIFT feature detection scheme, which avoids the use of a computationally expensive homomorphic encryption system by decomposing and distributing the SIFT computation to a set of independent cloud servers. Sankari et al. [13] proposed a privacy-preserving lightweight image encryption algorithm that maintains user privacy in digital images by performing simple image encryption.

To achieve highly efficient image encryption and image feature computation, we devise a fast privacy-preserving image feature extraction method in cloud computing. A simple block scrambling is used to encrypt original images and mean value-based features can be directly extracted from encrypted images. The main contributions are as follows.

(1) We presented a new secure feature computation outsourcing algorithm. Both users and cloud servers can compute mean value features directly from encrypted images without decryption, which can be used to privacy-preserving multimedia retrieval applications.

(2) Our scheme consists of block scrambling and intra-block permutation. The encryption strategy makes the mean value feature same before and after encryption. This will ensure the feature robustness.

(3) The secure feature extraction can be achieved on only one server, which makes our scheme is secure against the collusion attack of several servers.

The rest of this paper is organized as follows. Our searchable image encryption method is addressed in Section 2. Section 3 describes the mean value feature approach. Some experiments are shown in Section 4. Finally, the conclusions are drawn in Section 5.

2 Searchable Image Encryption

To protect user privacy in image contents, all images will be is encrypted before uploaded to remote cloud centers. During image encryption, a simple block scrambling strategy is employed to encrypt images to meet the real-time requirements in a smart environment. The image encryption procedure consists of two steps including block scrambling, intra-block permutation as shown in Fig. 1.

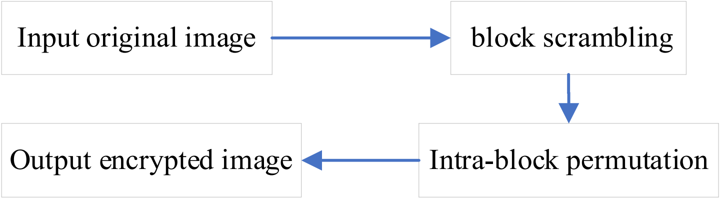


Figure 1: The image encryption procedure

Chaotic encryption has received attention from researchers due to its many good properties, such as ergodicity, sensitivity to initial conditions, and random-like behavior in image encryption. The piecewise linear chaotic map (PWLCM) is first exploited to generate a permutation sequence to scrambling the image blocks. The PWLCM can be described as

$$x_{n+1} = F\left(x_n, q\right) = \begin{cases} \dfrac{x_n}{q}, & x_n \in \left(0, q\right) \\ \dfrac{x_n - q}{0.5 - q}, & x_n \in \left[q, 0.5\right) \\ F\left(1 - x_n, q\right), & x_n \in \left[0.5, 1\right) \end{cases} \tag{1}$$

where $x_n \in (0,1)$, the generated sequence using Eq. (1) evolves into a chaotic state when the control parameter $q \in (0,0.5)$ and the parameter *q* can be used as a secret key [14].

Firstly, we generate pseudo-random sequences to scramble image blocks and change the position of image pixel in each intra-block. The detailed steps are described in Algorithm 1.

```
Algorithm 1: Scrambling sequence generation
Input: initial value $x_0$, control parameter $q$
Output: an ergodic matrix $T$
Initialization: the size $L$ of matrix $T$,
  1: for $i = 1$ to $L$
  2:     do
  3:         produce a new $x$ by iterating Eq. (1), and compute an integer $p$
  4:         using the following formula,
  $p = \mathrm{mod}\left(floor\left(x \times 10^{15}\right), L\right) + 1.$          (2)
  5:     while ($p==i$) or (flag($p$)==1)
  6:      $flag(p) \leftarrow 1, \mathrm{t}(i) = p$
  7: end for
```

The generated sequence *T* is a set and $T = \left\{t(i) \middle| t(i) \in \{1,2,\cdots,L\}, i = 1,2,\cdots,L\right\}$ is ergodic.

The encryption process firstly uses the permutation sequence T_1 to scramble the image blocks. The block scrambling process is depicted in Algorithm 2 as below:

```
Algorithm 2:  Image block scrambling
Input: original image $I$ with size $m \times n$, secret key $key_1$
Output:  encrypted image $I'$
Initialization: image block size $b \times b$
  1: Compute the total number of non-overlapped image blocks in the image $I$ as
     follows,
  $num_b = \frac{m \times n}{b \times b}$          (3)
  2: Update the size $L$ and parameter $q$, $L \leftarrow num_b$, $q \leftarrow key_1$.
  3: Generate the random sequence $T_1$ using algorithm 1.
  4: Divide original image $I$ and encrypted image $I'$ into $num_b$ non-overlapped blocks, denoted as
     $B$, and $B'$ respectively.
  5: for $i = 1$ to $num_b$
  6:         $B'(i) \leftarrow B(T_1(i))$
  7: end for
```

The image block scrambling is followed by a pixel permutation in intra-block which is employed to shuffle the positions of image pixels in each image block. Details are shown in Algorithm 3.

Algorithm 3: Intra-block permutation

```
Input: original image block $B$ with size $b \times b$, secret keys $key_2$ and $key_3$
Output: encrypted image $B'$
Initialization: intra-block size $b_1 \times b_1$
Update the size $L$ and parameter $q$, $L \leftarrow \frac{b \times b}{b_1 \times b_1}$, $q \leftarrow key_2$.
Generate the pseudo-random sequence $T_2$ using algorithm 1.
Reshape image block $B$ and encrypted image $B'$ in 1-dimension
  sequences $intrab$ and $intrab'$.
for $i = 1$ to $L$
    $intrab'(i) \leftarrow intrab(T_2(i))$
end for
Use $key_3$ as parameter $q$ ($q \leftarrow key_3$), and generate random sequence $T_3$ with size $b_1 \times b_1$ using
  algorithm 1.
Denote each pixel if intr-blocks $intrab$ and $intrab'$ as $Pb$ and $Pb'$,
  respectively.
for $i = 1$ to $b_1 \times b_1$
    $Pb'(i) \leftarrow Pb(T_3(i))$
end for
```

During image decryption, authorized users with the correct key can recover the original image by using the inverse process of the encryption process.

3 Mean Value Feature Extraction

In this scheme, the cloud servers are allowed to extract image features in the encrypted domain when users send a query request to the remote server. The same histogram feature based on mean value can be obtained before and after encryption using Algorithm 4 shown below.

Algorithm 4: Feature extraction based on the mean value

```
Input: encrypted image $I'$ with size $m \times n$,
Output: mean value feature vector $H$
Initialization: image block size $b \times b$, intra-block size $b_1 \times b_1$
Compute $num_b$ using Eq. (3).
for $i$=1 to $num_b$
    for $j$=1 to $\frac{b \times b}{b_1 \times b_1}$
        Compute the mean value $M_j$ of each intra-block $intrab$
    end for
    The histogram of all mean values in each intra-block form vector $H_i$
end for
All vectors $H_i$ are used to construct the histogram feature based on mean
```

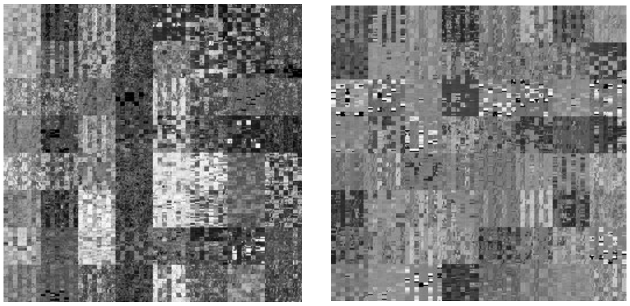
value H .

4 Experimental Results

The proposed scheme has been implemented on MATLAB 2016 platform. All the experiments are performed on a 1.80 GHz Intel(R) Core(TM) i7-8850U PC machine with 16G main memory, running on Microsoft Windows 10. In our experiments, some standard grayscale images with a size of 256 × 256 from the USC-SIPI Image Database are used to evaluate the proposed algorithm. Fig. 2 shows some test images. Here, block size b is set to 32, and intra-block size b_1 is set to 4. The produced encrypted images by our method are shown in Fig. 3. We can think that the encryption strategy is secure since no useful information can be observed from the encrypted image.

(a) Bridge (b) Couple

Figure 2: Test images



(a) Bridge (b) Couple

Figure 3: Encrypted images

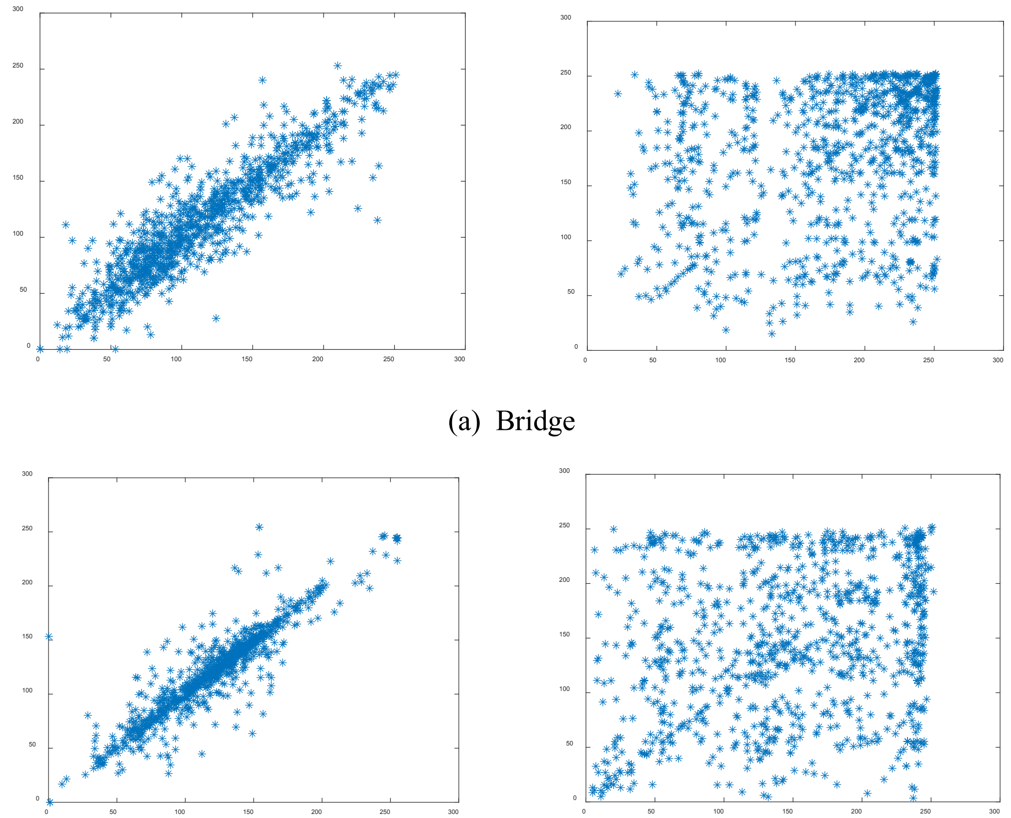
4.1 Security Analysis

In the proposed secure image feature extraction approach, the three secret keys are double-precision numbers with a computational precision of 10^{-16}. The key space is greater than and equal to 10^{48}, $O(10^{48}) \approx O(2^{160})$, which is larger than that of the AES-128 algorithm. The AES-128 algorithm is considered safe against any brute force attacks. So, the proposed privacy-preserving feature computation can be concluded that the PPBTC scheme can defeat brute-force attacks

So, our encryption algorithm has a large enough key space to resist brute-force attacks. That is to say, the encrypted image data cannot be decrypted by unauthorized users with the wrong secret key.

4.2 Pixel Correlation Analysis

In this section, the correlation between two adjacent pixels in plain image and cipher image is tested. The test results are illustrated in Fig. 4, and the correlations of original and encrypted images are shown in the left column and the right column, respectively. From Fig. 4, it can be seen that our image encryption scheme has a low correlation, which is of high-level security.



(a) Bridge

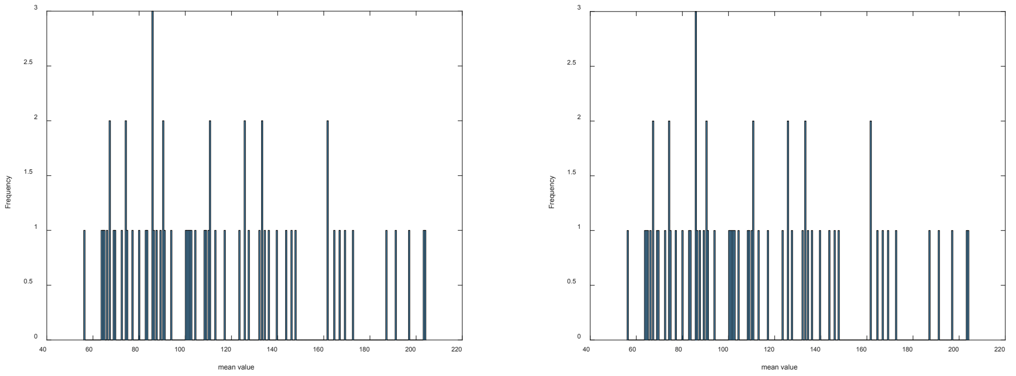
(b) Couple

Figure 4: Pixel correlation analysis

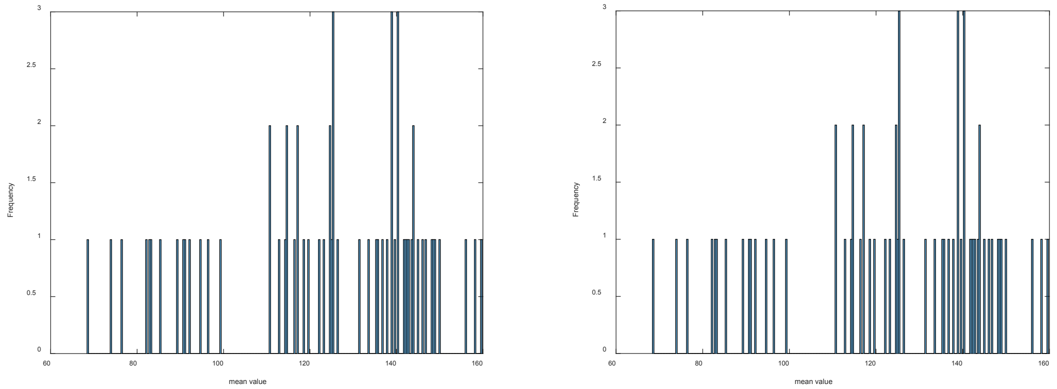
4.3 Feature Extraction Analysis

The extracted mean value-based histogram features are shown in Fig. 5. The features in the left column and right column are extracted from the original image and encrypted image, respectively. According to Fig. 5, it is not difficult to find that the extracted histogram features before and after encryption are the same. The proposed secure feature extraction method enables feature extraction in the encrypted domain.

We perform a comparative analysis of the secure feature extraction algorithm with the schemes of Xia et al.



(a) Bridge



(b) Couple

Figure 5: Histogram features based on the mean value before and after image encryption

5 Conclusion

In this paper, we proposed a privacy-preserving image feature extraction scheme over encrypted image data. It exploits block scrambling based on the chaotic map, intra-block permutation to achieve secure image computation outsourcing. A mean value-based strategy is used to extract histogram features from in the encrypted domain. Experimental results prove that it is secure and effective, and can be applied to secure image computation in the smart campus.

Funding Statement: A This work was supported in part by the National Natural Science Foundation of China (61872408), the Natural Science Foundation of Hunan Province (2020JJ4238), the Social Science Fund of Hunan Province (16YBA102), the Study and Innovative Experiment Project for College Students in HNFNU (YSXS1842), and the Research Fund of Hunan Provincial Key Laboratory of Informationization Technology for Basic Education (2015TP1017).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Yang, M. Yang, S. Salam and J. Zeng, "Research on protecting information security based on the method of hierarchical classification in the era of big data," *Journal of Cyber Security*, vol. 1, no. 1, pp. 19–28, 2019.

[2] E. Ryu and T. Takagi, "Efficient conjunctive keyword-searchable encryption," in *the 21st Int. Conf. on Advanced Information Networking and Applications Workshop*, pp. 21–23, 2007.

[3] M. Jiang and G. Sun, "A chaotic searchable image encryption scheme integrating with block truncation coding," in *Int. Conf. on Cloud Computing and Security,* Hainan, China, 2018.

[4] H. Pham, J. Woodworth and M. A. Salehi, "Survey on secure search over encrypted data on the cloud," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 17, pp. 1–15, 2019.

[5] H. Hacıgümüş, B. Hore, B. Iyer and S. Mehrotra, "Search on encrypted data," in T. Yu and S. Jajodia (Eds.), *Secure Data Management in Decentralized Systems,* Boston, MA: Springer US, pp. 383–425, 2007.

[6] H. Park, D. H. Lee, J. Zhan and G. Blosser, "Efficient keyword index search over encrypted documents of groups," in *IEEE Int. Conf. on Intelligence and Security Informatics*, pp. 17–20, 2008.

[7] Y. Tian, H. Lei, L. Wang, K. Zeng and T. Fukushima, "A fast search method for encrypted medical data," in *IEEE Int. Conf. on Communications Workshops*, pp. 14–18, 2009.

[8] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction," in *the SPIE-IS&T Electronic Imaging,* San Francisco, CA, 2010.

[9] Z. Qin, J. Yan, K. Ren, C. W. Chen, C. Wang *et al.,* "Privacy-preserving outsourcing of image global feature detection," in *IEEE Global Communications Conf.*, pp. 8–12, 2014.

[10] S. Hu, Q. Wang, J. Wang, Z. Qin and K. Ren, "Securing SIFT: privacy-preserving outsourcing computation of feature extractions over encrypted image data," *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411–3425, 2016.

[11]Q. Wang, S. Hu, J. Wang and K. Ren, "Secure surfing: privacy-preserving speeded-up robust feature extractor," in *IEEE 36th Int. Conf. on Distributed Computing Systems,* pp. 27–30, 2016.

[12] Q. Zhan, J. Yan, K. Ren, W. C. Chang and W. Cong, "SecSIFT: Secure image SIFT feature extraction in cloud computing," *ACM Transactions on Multimedia Computing Communications Applications,* vol. 12, no. 4, pp. 65, 2016.

[13] M. Sankari and P. Ranjana, "Privacy-preserving lightweight image encryption in mobile cloud," *Emerging Research in Computing, Information, Communication and Applications,* Singapore, 2019.

[14] X. Wang and D. Xu, "A novel image encryption scheme based on Brownian motion and PWLCM chaotic system," *Nonlinear Dynamics*, vol. 75, no. 1, pp. 345–353, 2014.