SCIENCE CHINA
Information Sciences

• LETTER •

March 2021, Vol. 64 139105:1–139105:3
https://doi.org/10.1007/s11432-018-9901-0

Efficient outsourced extraction of histogram features over encrypted images in cloud

Yanli REN[1], Xinpeng ZHANG[1], Dawu GU[2] & Guorui FENG[1*]

[1]*School of Communication and Information Engineering, Shanghai University, Shanghai* 200444*, China;*
[2]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China*

Received 28 December 2018/Accepted 24 May 2019/Published online 3 February 2021

Citation Ren Y L, Zhang X P, Gu D W, et al. Efficient outsourced extraction of histogram features over encrypted images in cloud. Sci China Inf Sci, 2021, 64(3): 139105, https://doi.org/10.1007/s11432-018-9901-0

Dear editor,

JPEG steganalysis mainly includes feature extraction and classification [1, 2], and thus the quality of the extracted features has an important influence on the detection performance of classifiers. With the development of JPEG steganalysis, the dimension of extracted features is greatly increased for improving the detecting performance [3].

In recent years, histogram calculation is widely used to create high-dimensional image features for JPEG steganalysis. In [4], the 8000-dimensional discrete cosine transform residual (DCTR) features which utilized 64 filters were proposed, where the decompressed JPEG image was convoluted with each filter and then the first-order residuals were obtained from subsampling images. Further, Song et al. [2] proposed a feature extraction method based on two dimensional (2D) Gabor filters, where the decompressed JPEG image was decomposed with different scales and orientations, and then the image features were extracted from the filtering coefficients. Compared with DCTR features, the 2D Gabor filters can obtain the embedding changes from more scales and orientations, and thus the 17000-dimensional Gabor filters residual (GFR) features were more effective. These two kinds of features are the most important methods of histogram calculation for JPEG steganalysis until now.

It is well known that for massive JPEG images, feature extraction based on histogram calculation is very difficult to be executed in a client due to limited ability. Therefore, it is very important for a client to decrease the computational load without decreasing the detection performance during feature extraction. Securely outsourced computation may be a feasible method to achieve this goal, which could outsource the task of a client to a cloud server and realize histogram feature extraction efficiently for massive JPEG images.

Currently, there are a lot of work for outsourcing expensive operations to an untrusted server. Ren et al. [5] constructed an outsourced scheme of modular exponentiations (MExps) based on a single server, where the client could verify the computation results with a probability of 1. Chen et al. [6] first proposed an efficient outsourced scheme for bilinear pairing, where the client does not need to execute any expensive operation. Ren et al. [7] presented another outsourced scheme, which simultaneously improved efficiency and checkability based on a single server. Wang et al. [8] proposed an outsourced image recovery service architecture under the compressed sensing framework. Ren et al. [9] proposed an outsourced feature extraction scheme based on the co-occurrence matrix, where the original images were protected from the server by using a projection of one to many with trapdoor, and the client could verify and obtain true results of extracted feature.

Our contributions. We propose a verifiable outsourced scheme of histogram feature extraction with a single cloud server. Also, we provide the experiments of extracting GFR features as an examples of histogram calculation in a true cloud environment. The original JPEG images of a client are protected from the server based on a symmetric encryption scheme. The client can obtain the true extracted features and detect any fault with a probability of 1 if the server misbehaves. If the verification is successful, the client accepts the outsourced result. Otherwise, it outputs "error". The proposed outsourced scheme can significantly reduce the cost, and its detection performance is as efficient as that of direct features extraction.

Verifiable outsourced scheme of histogram features extraction. In our algorithm, the client first encrypts the plaintext images X_i for steganalysis, where $1 \leqslant i \leqslant I$, and I denotes the number of plaintext images. Next, the server returns the encrypted results of histogram features extraction. Finally, the client decrypts and obtains the original extraction results of histogram features. We use a subroutine called Rand to accelerate the computation of the client. Once the subroutine Rand is invoked, a matrix R is generated for encrypting the original images. The details are as follows.

(1) For a plaintext image X_i, the client firstly divides the image into four parts $X_{i,j}$ with same size of $M \times N$, and then invokes Rand to get $R_{i,j}^{(k,l)}$, $\overline{R}_{i,j}^{(k,l)}$, where i, j, k,

* Corresponding author (email: grfeng@shu.edu.cn)

© Science China Press and Springer-Verlag GmbH Germany, part of Springer Nature 2021

l are integers, $1 \leqslant j \leqslant 4$, and $k \times l$ denotes the number of convolution kernels.

(2) The client separately encrypts the plaintext sub-images:

$$Y_{i,j}^{(k,l)} = X_{i,j} + qR_{i,j}^{(k,l)}, \quad \overline{Y}_{i,j}^{(k,l)} = X_{i,j} + q\overline{R}_{i,j}^{(k,l)},$$

where q is the value of quantization for extracting the features, and $q = 4$ for DCTR and GFR features. Thus, I plaintext images are encrypted into

$$2 \times I \times 4 \times k \times l = 8Ikl$$

ciphertext images.

(3) The client sends all of the ciphertext images to the server in random order, and the server executes the operations.

(a) Convolution:

$$U_{i,j}^{(k,l)} = Y_{i,j}^{(k,l)} * B_{m\times n}^{(k,l)} = \begin{bmatrix} u_{11}^{(k,l)} & \cdots & u_{1N}^{(k,l)} \\ \vdots & \ddots & \vdots \\ u_{M1}^{(k,l)} & \cdots & u_{MN}^{(k,l)} \end{bmatrix},$$

$$\overline{U}_{i,j}^{(k,l)} = \overline{Y}_{i,j}^{(k,l)} * B_{m\times n}^{(k,l)} = \begin{bmatrix} \overline{u}_{11}^{(k,l)} & \cdots & \overline{u}_{1N}^{(k,l)} \\ \vdots & \ddots & \vdots \\ \overline{u}_{M1}^{(k,l)} & \cdots & \overline{u}_{MN}^{(k,l)} \end{bmatrix}.$$

(b) Quantization and rounding:

$$V_{i,j}^{(k,l)} = \left\langle \frac{U_{i,j}^{(k,l)}}{q} \right\rangle, \quad \overline{V}_{i,j}^{(k,l)} = \left\langle \frac{\overline{U}_{i,j}^{(k,l)}}{q} \right\rangle.$$

(4) The server computes

$$H_{i,j}^{(k,l)} = [h_0, h_1, \ldots, h_{r+q}],$$
$$\overline{H}_{i,j}^{(k,l)} = [\overline{h}_0, \overline{h}_1, \ldots, \overline{h}_{r+q}],$$

as the histograms of ciphertext images $Y_{i,j}^{(k,l)}$, $\overline{Y}_{i,j}^{(k,l)}$, where $1 \leqslant i \leqslant I$, $1 \leqslant j \leqslant 4$.

(5) The client decrypts the histograms of ciphertext sub-images to get the ones of plaintext images. Assume that

$$R_{i,j}^{(k,l)} * B_{m\times n}^{(k,l)} = [s_{i,j}^{(k,l)}]_{M\times N}, \quad s_{i,j}^{(k,l)} \in \{q, \ldots, r\},$$
$$\overline{R}_{i,j}^{(k,l)} * B_{m\times n}^{(k,l)} = [\overline{s}_{i,j}^{(k,l)}]_{M\times N}, \quad \overline{s}_{i,j}^{(k,l)} \in \{q, \ldots, r\},$$

so that we obtain the histograms $H_{i,\mathrm{ori}}^{(k,l)}$, $\overline{H}_{i,\mathrm{ori}}^{(k,l)}$ of plaintext image X_i, where

$$H_{i,\mathrm{ori}}^{(k,l)} = [h_{i,\mathrm{ori}}^0, \ldots, h_{i,\mathrm{ori}}^q], \quad h_{i,\mathrm{ori}}^0 = \sum_{j=1}^{4} h_{s_{i,j}^{(k,l)}},$$

$$h_{i,\mathrm{ori}}^1 = \sum_{j=1}^{4} \left(h_{s_{i,j}^{(k,l)}-1} + h_{s_{i,j}^{(k,l)}+1} \right), \ldots,$$

$$h_{i,\mathrm{ori}}^{q-1} = \sum_{j=1}^{4} \left(h_{s_{i,j}^{(k,l)}-q+1} + h_{s_{i,j}^{(k,l)}+q-1} \right),$$

$$h_{i,\mathrm{ori}}^{q} = 1 - \sum_{d=0}^{q-1} h_{i,\mathrm{ori}}^{d}.$$

Similarly,

$$\overline{H}_{i,\mathrm{ori}}^{(k,l)} = \left[\overline{h}_{i,\mathrm{ori}}^0, \ldots, \overline{h}_{i,\mathrm{ori}}^q \right], \quad \overline{h}_{i,\mathrm{ori}}^0 = \sum_{j=1}^{4} \overline{h}_{s_{i,j}^{(k,l)}},$$

$$\overline{h}_{i,\mathrm{ori}}^1 = \sum_{j=1}^{4} \left(\overline{h}_{s_{i,j}^{(k,l)}-1} + \overline{h}_{s_{i,j}^{(k,l)}+1} \right), \ldots,$$

$$\overline{h}_{i,\mathrm{ori}}^{q-1} = \sum_{j=1}^{4} \left(\overline{h}_{s_{i,j}^{(k,l)}-q+1} + \overline{h}_{s_{i,j}^{(k,l)}+q-1} \right),$$

$$\overline{h}_{i,\mathrm{ori}}^{q} = 1 - \sum_{d=0}^{q-1} \overline{h}_{i,\mathrm{ori}}^{d}.$$

The client verifies whether $H_{i,\mathrm{ori}}^{(k,l)} = \overline{H}_{i,\mathrm{ori}}^{(k,l)}$ holds or not. If yes, it accepts the outsourced result; otherwise, output "error".

Experiment simulations. The experiment environment is established at Alibaba cloud elastic compute service (ECS), where 112 virtual machines are used with Intel Xeon Gold 6149 CPU running at 3.1 GHz and 4 G memory. On the other hand, the client is simulated by a computer with 2 Intel i7 CPU cores running at 2.6 GHz and 4 G memory. In addition, the programming language is MATLAB, using MATLAB2014a library.

In the experiments, we choose 100000 images with quality factor (QF) 95 from ImageNet, and insert secret information into all of the images by using the method of universal wavelet relative distortion for JPEG images (J-UNIWARD) with payload 0.5 bpac.

In Figure 1, we compare the computational cost between the client and server for the images with QF95 when outsourcing GFR features extraction. It is obvious that the computational cost for the client and the server are all much smaller than that of extracting the image features directly. In detail, the computational cost is about decreased to 13% of direct extraction for the client, and it is about decreased to 7% of direct extraction for the server. Thus, the total computational cost of the client and the server is about 20% of direct computation when extracting GFR features.

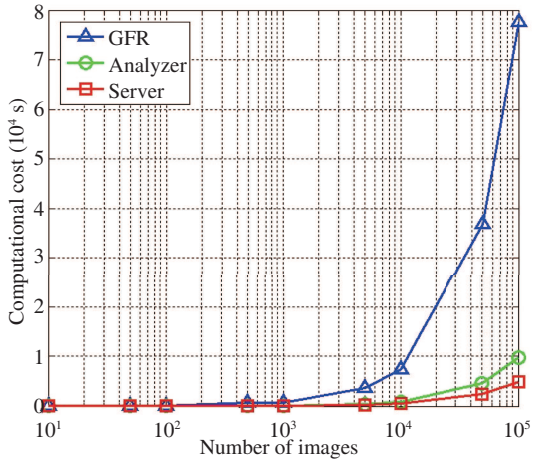

Figure 1 (Color online) Simulation for the outsourcing of GFR features (QF95).

Now we compare the detection performance of the proposed outsourced scheme with that of the original features extraction algorithm. Finally, the extracted image features are detected by ensemble classifiers. We separately compare the probability of detection error (P_E) of the outsourced

scheme with that of the original extraction algorithm for GFR features, where

$$P_E = \min_{P_{\rm FA}} \frac{1}{2}(P_{\rm FA} + P_{\rm MD}(P_{\rm FA})),$$

and $P_{\rm FA}$, $P_{\rm MD}$ are the probabilities of false alarms and missed detection for the training set of ensemble classifiers, respectively. And the decision threshold of each base learner is changed to minimize the total detection error under equal priors on the training set.

During the experiment, we know that the value of P_E decreases with the increase of the number and quality factor of the images, and the effects are more obvious especially for the images with QF 95 during GFR features extraction. The detection performances of features extracted from the outsourced scheme are nearly as same as those from the original extraction algorithm for all of the images. Therefore, the extracted features in the outsourced scheme are also accurate and the detection performances do not decrease compare with the original extraction algorithm during GFR features extraction.

Conclusion. We propose a secure outsourced scheme of histogram features extraction based on an untrusted cloud server by using a symmetric encryption algorithm. The original images and the extracted features are also private for the server. Experimental results show that the outsourced scheme keeps the detection performance of extracted features as well as direct features extraction and greatly decreases the computational loads of the client.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. U1736120, 61572309, U1636206, 61525203, U1536109) and Natural Science Foundation of Shanghai (Grant No. 19ZR1419000).

References

1 Li B, He J H, Huang J W, et al. A survey on image steganography and steganalysis. J Inform Hiding Multimedia Signal Process, 2011, 2: 142–172
2 Song X F, Liu F L, Yang C F, et al. Steganalysis of adaptive JPEG steganography using 2D Gabor filters. In: Proceedings of ACM Workshop on Information Hiding and Multimedia Security, Portland, 2015. 15–23
3 Ma Y Y, Luo X Y, Li X L, et al. Selection of rich model steganalysis features based on decision rough set α-positive region reduction. IEEE Trans Circ Syst Video Technol, 2019, 29: 336–350
4 Holub V, Fridrich J. Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Trans Inform Forensic Secur, 2015, 10: 219–228
5 Ren Y L, Dong M, Qian Z X, et al. Efficient algorithm for secure outsourcing of modular exponentiation with single server. IEEE Trans Cloud Comput, 2018. doi: 10.1109/TCC.2018.2851245
6 Chen X F, Susilo W, Li J, et al. Efficient algorithms for secure outsourcing of bilinear pairings. Theory Comput Sci, 2015, 562: 112–121
7 Dong M, Ren Y L. Efficient and secure outsourcing of bilinear pairings with single server. Sci China Inf Sci, 2018, 61: 039104
8 Wang C, Zhang B S, Ren K L, et al. Privacy-assured outsourcing of image reconstruction service in cloud. IEEE Trans Emerg Top Comput, 2013, 1: 166–177
9 Ren Y L, Zhang X P, Feng G R, et al. How to extract image features based on co-occurrence matrix securely and efficiently in cloud computing. IEEE Trans Cloud Comput, 2017, 8: 207–219