Design and Implementation of Image Forgery Detection System Based on Cloud Computing

Chao Zhang¹, Guoliang Hu³*, Jiajun Hu¹, Yong Zhang¹ and Yitian Xie²

¹Hunan Branch of National Computer Network and Information Security Management Center, Changsha, Hunan, China
²Hunan International Business Vocational College, Changsha, Hunan, China

*Corresponding author. Email: huguoliang@cert.org.cn

Abstract. The masses of people urgently need a platform to help them identify the authenticity of network images, but the existing image forgery detection algorithms generally have high thresholds and poor real-time problems, making it difficult for the public to provide efficient detection services. Therefore, this paper proposes a cloud-based network image forgery detection system that uses B/S architecture, integrates multiple algorithms, and uses cloud computing and GPU computing technologies to improve system throughput and detection speed. Experimental results show that the system can effectively detect copy-move and splicing forgeries, and the GPU's speedup ratio reaches 6.5, which significantly improves the detection speed and throughput of the system.

Keywords: forgery detection, copy-move, image splice, cloud computing, GPU computing.

1. Introduction

With the rapid development and application of computer technology and multimedia technology, network images have provided great convenience to people's daily work and life. At the same time, it is not uncommon to use image editing software to forge with the image content to achieve a special purpose. Forged images have caused serious negative effects on insurance claims, judicial forensics, scientific research, news reports, and even political and military fields, which have seriously affected people's correct perception of social information. Therefore, research and development of digital image forensics technology to identify whether digital images have been falsified [1, 3] has important practical significance for regulating public order, promoting economic and social development, and maintaining judicial justice.

At present, there are many related algorithms for image forgery detection, but the source code is not public or the program is cumbersome, not only does it require professional researchers to use it normally, but also the calculation complexity is too high, and the detection real-time is poor, so it is difficult to provide efficient detection services for the public in the practical application of the software. At the same time, in order to make fake images look more real and natural, forgers often use a variety of forgery methods to perform mixed forgery on the images. Currently, it is often difficult for a single forgery detection method to effectively detect all image forgery attacks. To this end, this article designs and implements a cloud image forgery detection system with a graphical interface, multi-algorithm
fusion, and extensibility. This system integrates DCT,[4] PCA,[5] HDD,[6] SelfConsistency,[7] and other
detection algorithms. It not only uses cloud computing for multi-task parallel processing, but also
computes intensive feature extraction and feature matching during image forgery detection. The stage is
transplanted to the GPU for parallel accelerated computing processing, which significantly improves
the throughput and detection speed of image forgery.

2. Related work

2.1. Copy-move forgery detection
Copy-Move forgery is the most common method of the image forgery methods. It causes some kind of
artifact or masks important targets,[8,9] by copying one area of an image and pasting it to the same image.
In recent years, image Copy-Move forgery detection has become a focus of attention and research by
related scholars and research institutions at home and abroad. There are many algorithms for detecting
image Copy-Move forgery.

In 2003, Fridrich et al. proposed a method for image forgery detection using DCT coefficients as
image features first.[4] On this basis, Popescu et al. Proposed a PCA-based image copy-move forgery
detection algorithm, and used principal component analysis to perform dimension reduction processing
on the extracted DCT coefficients of each image block.[5] Mahdian et al. improved the method proposed
by Popescu et al., using fuzzy invariant moments, PCA, and k-d trees.[10] In 2017, Xie Wei et al.[6]
proposed a pre-press image forgery detection method HDD based on halftone technology, which has
lower time complexity and higher detection rate. Moreover, it has good robustness against rotation
attacks and small-scale scaling attacks in image forgery areas.

2.2. Image splicing forgery detection
Image splicing forgery is another common method of the image forgery methods. Unlike the
Copy-Move forgery method, the copying and pasting areas of the image splicing forgery belong to
different images. Many researchers have done a lot of research and exploration on the splicing forgery
detection of images.

Farid et al. made pioneering research on the splicing forgery detection of images in terms of optical
characteristics.[11] Researchers such as Kee et al. determine whether the image has been forged with
splicing based on the assumption of infinity single light source and matrix solving method.[12] Yuan
Quanqiao et al. proposed an algorithm using wavelet transform to detect image splicing forgery.[13]
With the gradual maturity of deep learning algorithms and neural network technologies, image forgery
detection algorithms based on deep learning and neural network technologies also continue to emerge.
In 2016, RAO et al.[14] applied deep learning algorithms to image forgery detection first. In 2017,
BAPPY et al.[15] proposed a neural network image forgery detection algorithm based on
non-overlapping image blocks. In 2018, HUH M et al.[7] proposed a self-consistency learning splicing
forgery detection algorithm, which based on deep learning technology, with better detection effect.

2.3. Cloud computing technology
Cloud computing is not only a business model, but also a brand-new technology model. Its proposal
fundamentally changes the existing computing service model. It can provide users with efficient
computing services through network autonomy, heterogeneous services, and shared resources. It is an
upgrade and integration of grid computing, utility computing, cluster technology, and distributed
technologies. The cloud computing platform has the advantages of large scale, strong computing power,
high reliability, and dynamic scalability, and has become an indispensable technical foundation for big
data analysis, artificial intelligence and other fields.[16,17].
2.4. CUDA programming model

With the rapid development of general-purpose computing technology for graphics processor GPUs, the floating-point computing capabilities of mainstream GPUs are now more than ten times that of mainstream CPUs. GPU has become a mainstream accelerator in the field of high-performance computing due to its strong parallel computing capabilities and high throughput [18, 19].

CUDA is a programming model, specially developed by NVidia, for parallel computing of large-scale data using the powerful multi-core floating-point computing capabilities of the GPU [20]. Through the interface provided by CUDA, GPU computing resources can be directly called without mapping to a graphics API. The CUDA software stack structure is shown in Fig. 1.

![CUDA software stack](image)

**Figure 1.** CUDA software stack.

3. Image forgery detection scheme based on cloud computing and GPU computing

3.1. Overall scheme design

Aiming at the problems existing in the Copy-Move forgery detection algorithms and image splicing forgery detection in practical applications, this paper designs a cloud-based image forgery detection scheme. This solution is based on the Hadoop cloud platform, move the image feature extraction and feature matching stages in the Copy-Move forgery detection algorithms, which is computationally intensive and expensive, to the CUDA platform, and also move the image feature extraction and classification detection stages in the image splicing algorithms to the CUDA platform, in order to perform GPU-accelerated computing processing. In addition, this solution also provide users with a simple and clear web operation interface.

The scheme of this article is divided into three parts: the first part is the web module that provides users with an intuitive operating interface, including input, selection of detection algorithms, algorithm parameter settings, and display of detection results; the second part is the Hadoop module, which provides multi-task parallel computing and related virtual resource management scheduling functions; the third part is the GPU-accelerated computing module based on CUDA. The overall framework of the scheme in this paper is shown in Fig. 2.
The web graphical interface mainly implements interaction with users and visual configuration of task parameters. The task scheduling module mainly implements task distribution and load balancing, the system configuration module mainly implements the user's configuration of forgery algorithm parameters. The image preprocessing module mainly implements the functions of image segmentation, color conversion, and camera information extraction. The GPU acceleration module mainly performs GPU-accelerated processing on Copy-Move forgery detection algorithms and image splicing detection algorithms. The Copy-move forgery detection module implements forgery detection algorithms such as DCT, PAC and HDD. The image splicing detection module implements the Self-Consistency splicing forgery detection algorithm. The filtering and post-processing module mainly implements filtering and related additional processing operations on the detection results.

3.2. Cloud-based multi-task parallel acceleration

The image forgery detection system under the conventional serial model is deployed on a single physical machine, the device performance is limited, the detection efficiency is average, and the scalability is poor. And the cloud-based image forgery detection system deployed and built based on cloud computing related technologies, has strong computing power, high resource utilization, and can be dynamically expanded. The multi-task parallel processing process based on cloud computing in this paper is shown in Fig. 3.
When a user submits multiple detection tasks, the task scheduling server distributes detection tasks to each computing node according to the task scheduling strategy of the cloud platform and the resource usage of the computing node cluster. And each computing nodes perform the detection tasks that they received. Such effectively improve the throughput of the system, achieve task-level parallel processing.

### 3.3. GPU parallel computing acceleration based on CUDA

The basic flow of the Copy-Move forgery detection algorithm includes image pre-processing, feature extraction, image similar feature matching, and post-processing. The two stages of feature extraction and feature matching are the most computationally intensive and expensive stages in Copy-Move forgery detection methods. They are also the main reasons for the large time overhead of the algorithm [21, 22].

The image splicing algorithm is usually divided into training process and test process. The training process mainly trains the classifier by extracting the features of a large number of pictures, and the test process extracts the features of the tested image, uses the trained classifier to detect, and predicts whether it is a spliced image [23, 24]. The test process mainly includes image pre-processing, feature extraction, classification detection and post-processing. Since the classifier training process was completed before the image splicing forgery detection algorithm was applied, the solution in this article focuses on GPU-accelerated computation of the test process.

Both the block-based image Copy-Move forgery detection method and image splicing forgery detection algorithm, usually need to block the image, and then extract the features of the image block. But the feature extraction between different blocks is independent of each other, which can be directly transplanted to the GPU for parallel computing. The feature matching phase in the image Copy-Move forgery detection method involves operations, such as dictionary ordering of feature vectors, approximate nearest neighbor search of feature vectors, etc. can be processed in parallel. Through parallel design of the processing program, it can be transplanted to the GPU for accelerated calculation.
The image splicing algorithm needs to use a trained classifier to classify image blocks during the classification detection phase. The classification process of these image blocks is independent of each other which can be processed directly in parallel. At the same time, the classification process usually involves a large number of parallel computations such as matrix multiplication, which can be transplanted to the GPU for accelerated calculations [7][25, 26].

This paper uses the powerful parallel computing performance of the GPU, and migrates computationally intensive image feature extraction, feature matching or classification detection during the image forgery detection process to the GPU for parallel accelerated processing to achieve rapid image forgery detection, such as Shown in Fig. 4.

![Figure 4. GPU-Accelerated image forgery detection scheme.](image)

Since the parallelization process of the classification detection stage in the image splicing forgery detection is relatively simple, and it is basically the same as the GPU parallel computing method for the feature extraction of image blocks. Next we mainly introduce the GPU parallel computing method for feature extraction of image blocks and the GPU parallel computing method for image feature matching.

### 3.3.1 GPU Parallel Computing Method for Image Block Feature Extraction

In the image copy-Move forgery detection method, an image of size $M \times N$ is usually overlapped and partitioned with a size of $B = b \times b$, and the size of the obtained overlap area is 1 pixel. The number of blocks is: $N_B = (M - b + 1)(N - b + 1)$. Similarly, image splicing detection algorithms usually perform block processing on images and then extract the features of each block.

The traditional CPU-based serial calculation method usually calculates the characteristics of each block one by one. In order to improve the efficiency of image block feature extraction, this paper uses the advantages of high-performance parallel computing of GPU to realize the parallel processing of image block feature extraction. The feature extraction method for parallel computation of image block features using the CUDA programming model is as follows:

**Algorithm 1: Image block feature extraction method based on GPU parallel computing**

Input: N image blocks after image block;  
Output: image feature vectors corresponding to N image blocks;  
1: Start CUDA and set the GPU device;  
2: Allocate video memory space for the GPU and copy the block data to the video memory;

![Algorithm 1](image)
3. Allocate graphics memory space for the GPU to store image block feature vectors;
4. Call the kernel function that calculates the feature vector of the image block, and return the result;
5. Allocate memory space for the CPU to store the image block feature vector returned by the GPU;
6. Write the image block feature vector data in the video memory back to the memory;
7. Release memory and video memory space;
8. Exit CUDA;

3.3.1. GPU parallel computing method for image feature matching. In the image Copy-Move forgery detection method, after extracting the feature vectors of each image, it is necessary to match the feature vectors of each block, find similar feature vectors and analyze their geometric position information, to determine whether the image blocks are suspicious Copy-Move forged areas.

Because there are overlapping areas between adjacent blocks when the image is divided, and there may be areas with similar characteristics in the image itself, in order to accurately determine whether the image is copy and paste areas, the k most similar image blocks of the target image block need to be compared when comparing the similarity of image blocks.

Find the k most similar image blocks of the target image block, commonly known as the k-nearest neighbor (KNN) problem. The KNN query algorithm is widely used. After years of development, it has been basically mature. However, with the rapid development of GPU computing technology, in order to further improve the efficiency of KNN algorithms, many scholars have proposed GPU-based KNN query algorithms, such as GPU-based k-d tree nearest neighbor algorithm [18][27] and GPU- FS-kNN [28] etc.

Among them, the GPU-FS-kNN algorithm has the advantages of fast calculation speed and strong scalability to large-scale data sets. The k-nearest neighbor parallel search process based on CUDA of this algorithm is implemented by two kernel functions. The first kernel function is a distance calculation function (Distance Kernel), which is responsible for calculating the distance value corresponding to the position of each chunk in the original distance matrix. The second kernel function is the k-nearest neighbor query function (kNN Kernel), which finds k-nearest neighbors from chunks. The specific steps of the GPU-FS-kNN algorithm are as follows.

Algorithm 2: Fast and Scalable k-Nearest GPU Parallel Algorithm(GPU-FS-kNN)

Input: feature matrix $I_n$, dimension $n_{size}$ of each block, number of nearest neighbors $k$;
Output: kNN query result $G_k$;

1. Create $G_k$;
2. $G_k[i].weight \leftarrow \text{float}_\text{max}$, for $i \leftarrow 0 \ldots (n_{row}-1)$;
3. Initialize(segments, $n_{GPU}$);
4. foreach segment $\in$ segments do
5. create $D$;
6. create $G_k'$;
7. host $\rightarrow$ device(in, D, Gk');
8. initialize(splits, segment);
9. create Maxk;
10. foreach split $\in$ splits do
11. initialize Maxk;
12. host $\rightarrow$ device(Maxk);
13. initialize(chunks, split);
14. foreach chunk $\in$ chunks do
15. call Distance Kernel$<<<\text{grid1, block1}>>>(I_n, n_{size},$
16. split, chunk, b);
17. call kNN Kernel$<<<\text{grid2, block2}>>>(D, n_{size},$ split,
18. chunk, Maxk);
19. device $\rightarrow$ host(Gk');
20. return Gk;
In this paper, GPU-FS-kNN algorithm is used to realize k-nearest neighbor search of image features, and then k-nearest neighbor map is generated. Because the similarity matching process of image blocks is independent, a kernel function can be created for parallel processing on the GPU. If the image block matches successfully, the image block is a suspicious forged image block.

4. Analysis of experimental results

4.1. System detection effect

In order to verify the effectiveness of the Copy-Move forgery detection algorithms and image splicing forgery detection algorithms integrated in this system, we tested it on the Benchmark Data dataset and Columbia dataset [9][7]. The detection results of some algorithms are shown in Fig.5 and Fig.6. The implementation results show that the image forgery detection system proposed in this paper can effectively detect the image forgery of Copy-Move mode and image splicing mode.

![Figure 5. Detection effect of image Copy-Move forgery detection algorithm (HDD).](image)

(a) Original picture (b) Forgeryed picture (c) Detection

![Figure 6. Detection effect of image splice forgery detection algorithm (SelfConsistency).](image)

(a) Input picture (b) Algorithm detection effect (c) Real forged area (d & e) Real picture

4.2. System detection speed

In order to compare the processing performance of the image forgery detection method based on GPU-based parallel computing acceleration, this paper uses the GPU-based parallel computing strategy to improve the traditional DCT, PCA, HDD and SelfConsistency algorithms in the feature extraction, feature matching or parallel classification detection phases. And compare the performance with the original method. The server used in the comparison experiment is configured with Ubuntu 16.04, Intel i5 7400, 8G memory, and equipped with Nvidia GTX 1060 discrete graphics card.

A comparison of the average processing time overhead between GPU-based parallel computing acceleration detection algorithms and traditional typical serial algorithms is shown in Fig.7. The experimental results show that the GPU parallel computing acceleration is performed on both the feature extraction and matching stages in the Copy-Move forgery detection process and the feature extraction and classification detection stages in the image splicing forgery detection process, and the detection speed is significantly improved.
4.3. System detection efficiency

In order to compare the efficiency of the cloud-based image forgery detection system, this article uses three servers with Ubuntu 16.04, Intel i5 7400, 8G memory and Nvidia GTX 1060 discrete graphics cards to build the cloud platform, and compares the performance with the traditional single task method experiment.

The experimental results show, the throughput of the traditional serial Self-Consistency algorithm in a single computing node is 0.4 pictures/minute, the GPU-accelerated Self-Consistency algorithm has a throughput of about 2.6 pictures/minute for a single computing node, when using three compute nodes of the same configuration, its detection throughput can reach 6.8 pictures/minute. It can be seen that compared to conventional forgery detection, the image forgery detection based on cloud computing platforms not only improves the throughput significantly, but also has good horizontal scalability. In the future, you can further increase the detection efficiency by adding computing nodes to the cluster.
5. Summary
This paper proposes a multi-algorithm integrated image forgery detection scheme based on cloud computing and GPU computing. This solution implements task-level parallelism of the algorithm through cloud computing technology. And the parallel computing of the GPU is used to achieve data-level parallelism of the algorithm. Experimental results show that the system is simple to operate, simple to apply, and highly scalable. The image forgery detection method of this paper, which compared with single CPU serial processing detection method, has a significant improvement in detection speed and system throughput. At the same time, the system throughput is further improved with the expansion of the cloud computing platform.

Acknowledgement
This research was financially supported by the Youth Fund of National Computer Network and Information Security Management Center.

References
[1] Lynch G, Shih F Y, Liao H Y M. An efficient expanding block algorithm for image copy-move forgery detection, J. Information Sciences. 239(2013) 253-265.
[2] Wu Qiong, Li GuoHui, et al. A Survey of Blind Digital Image Forensics Technology for Authenticity Detection, J. ACTA Automatix Sinica. 34(2008) 1458-1466.
[3] Birajdar G K, Mankar V H, Digital image forgery detection using passive techniques: A survey, J. Digital Investigation. 10(2013) 226-245.
[4] Fridrich, J., Soukal, D. and Lukas, J. Detection of Copy-Move Forgery in Digital Images. Proceedings of Digital Forensic Research Workshop, Cleveland, August 2003, (2003) 55-61.
[5] Popescu, A. and Farid, H. Exposing digital forgeries by detecting duplicated image regions, TR2004-515. Dartmouth College, Hanover, (2004) 11.
[6] Xie Wei, Wan Xiaoxia, et al. Copy-Move Forgery Detection for Pre-Printing Image Using Digital Halftoning Technolog, J. Journal of Software. 28(2017) 1835-1846.
[7] Huh M, Liu A, Owens A, et al. Fighting fake news: Image splice detection via learned self-consistency. The 15th European Conference on Computer Vision, Munich, Germany, (2018) 106-124.
[8] Al-Qershi, O.M. and B.E. Khoo, Passive detection of copy-move forgery in digital images: State-of-the-art, J. Forensic Science International. 231(2013) 284-295.
[9] Thajeel S A, Sulong G B. State of the art of copy-move forgery detection techniques: a review, J. International Journal of Computer Science Issues. 10(2013) 174-183.
[10] Mahdian B, Saic S. Detection of copy-move forgery using a method based on blur moment invariants, J. Forensic science international. 171(2007) 180-189.
[11] Farid H.A survey of image forgery detection, J. IEEE Signal Processing Magazine. 26 (2009) 16-25.
[12] Kee E, O’Brien J F, Farid H. Exposing photo manipulation from shading and shadows. ACM Transactions on Graphics. 33 (2014).
[13] Yuan Quanqiao, Su Bo, et al. Image splicing detection based on high frequency wavelet Markov Features, J. Journal of Computer College, (2014) 1477-1481.
[14] Rao Y and NI Jiangqun. A deep learning approach to detection of splicing and copy-move forgeries in images. 2016 IEEE International Workshop on Information Forensics and Security. Abu Dhabi, UAE, (2016) 1-6.
[15] Bappy J H, Roy-Chowdhury A K, Bunk J, et al. Exploiting spatial structure for localizing manipulated image regions. 2017 IEEE International Conference on Computer Vision. Venice, Italy, (2017) 4980–4989.
[16] Raoul Hentschel, Christian Leyh. Cloud Computing: Yesterday, Today, Tomorrow, J. HMD Praxis der Wirtschaftsinformatik. 53 (2016) 563-579.
[17] Xia Jingbo, Wei Zekun, et al. Review of Research and Application on Hadoop in Cloud Computing, J. Computer Science. 43(2016) 6-11.

[18] Liu Xin, Xu Huarong, A Comparison of Image Feature Detection and Matching on CPU and GPU Implementation, J. Journal of Computer-Aided Design & Computer Graphics. 25(2013) 1496-1502.

[19] Deng Bosheng, An Improved Algorithm of the Screen Space Ambient Occlusion, J. Modern Computer. 9 (2017) 54-57.

[20] Liu Duanyang, Zheng Jiangfan, et al. Study on Parallel K-means Algorithm Based on CUDA, J. Computer Science. 45(2018) 292-297.

[21] Mahmood T, Nawaz T, Ashraf R, et al. A survey on block based copy move image forgery detection techniques. Emerging Technologies (ICET). Peshawar, Pakistan: 2015 International Conference on. IEEE. (2015).

[22] Chauhan D, Kasat D, Jain S, et al. Survey on Keypoint Based Copy-move Forgery Detection Methods on Image, J. Procedia Computer Science. 85(2016) 206-212.

[23] Yin Liguo. Research on Image Splicing Forgery Forensics Based on Deep Learning, D. KunMing: Yunnan University (2015).

[24] Cai Jia. Research on digital image splicing detection based on image transformation and support vector machine, D. HeFei: AnHui University (2017).

[25] Tang Gexuan. A Parallel Optimization Algorithm of Deep Learning on Heterogeneous Platform, D. BeiJing: Beijing University of Technology (2017).

[26] Gao Chen. Research on the Parallel Key Technology of Image Feature Extraction Based on GPU, D. NanJing: Nanjing University of Posts and Telecommunications (2018).

[27] Hu L, Nooshabadi S, Ahmadi M. Parallel randomized KD-tree forest on GPU cluster for image descriptor matching. 2016 IEEE International Symposium on Circuits and Systems (ISCAS). Montreal, Canada (2016).

[28] Arefin A S, Riveros C, Berretta R, et al. GPU-FS-k NN: A Software Tool for Fast and Scalable k NN Computation Using GPUs, J. PloS one. 7(2012) 1-13.