Improved Copy-Move Forgery Detection Using Interest Point Detectors

Devi Mahalakshmi

Associate Professor, Department of Computer Science and Engineering
Mepco Schlenk Engineering College, Sivakasi
Email: *sdevi@mepcoeng.ac.in*

Abstract: The main problem in the real world is to determine whether an image is forged or not. Any alteration in an original image in bad faith is called image forgery. Copy–Move (region duplication) is a common attack in which at least one part of an image is copied and pasted onto another area of the same image to add or remove an object. Detection methods use either block-based methods, or point-based methods. Here we propose a novel copy-move forgery detection scheme that can accurately localize the tampered regions. A new interest point detector is proposed in which the detected key points adaptively cover the entire image, even low contrast regions, based on the uniqueness metric. An adaptive matching is performed to find the similar key points. Moreover, a new filtering algorithm is utilized, which can effectively remove the falsely matched regions. Then the whole procedure is iterated regarding the prior information.

Keywords: Copy-Move Forgery, Digital Image Forensics, Duplicated Region Localization, Interest Point Detection

I. INTRODUCTION

Nowadays, digital images are inseparable parts of the human life. Images can save the moments very easily. There is also a lot of powerful editing software. Although they are helpful, they may facilitate the possibility of tampering and counterfeiting. The main goal of creating fakery is altering the semantic, and the most important outcome is the reduction of trust to photos. For instance, it is not assured to rely on an image as a clue in a court. As a consequence, the image forensic tools are essentially required to discriminate the tampered images from real ones. A lot of efforts have been conducted to overcome this problem.

Digital images are manipulated in such a perfect way that the forgery cannot be visually perceived by naked eyes. Nowadays, in the society, we can come in contact with a lot of tampered images, in news report, business, law, military affairs, academic research. More particularly, the forgery images could be used to distort the truth in news reports, to destroy someone's reputation and privacy, e.g. by changing a face of a person in the image with someone else's face. Law enforcement today uses emerging various technological advances in the investigation of crimes. In fact, Image Forensics techniques are used mainly when an image is presented as the proof to influence the judgment. During last decade, various techniques for validating the integrity of digital images have been developed. There are three main branches [2] in Digital Image Forensics:

- ***Finding the Source -*** aims to identify which device was used to capture an image (model or exemplar of scanner, of digital camera).
- ***Discrimination of Computer Generated Images,*** to detect if an image is real or synthetic.

- ***Image Forgery Detection,*** to discern if an image has been intentionally modified by human intervention.

Digital image forgery detection techniques are categorized into active and passive approach. In active approach, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and authenticity is established by verifying if the retrieved signature matches the original one, or if it is corrupted. There are more digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the forgery of the image. Passive techniques use the intrinsic content of an image to detect if it has been tampered, without any superimposed information.

One of the main objectives of Image Forensics techniques is to understand what kind of tampering has been applied. Images can be doctored in several ways [3]: photo-compositing, re-touching, enhancing are only some examples of typical image alterations.

II. RELATED WORK

Copy-move is a specific type of image tampering, where a part of the image is copied and pasted into another part of the same image (Fig 1). Copy-move forgery [4] is performed with the intention to make an object "disappear" from the image by covering it with a small block copied from another part of the same image.

The main goal is to conceal objects or overemphasize a concept by duplicating some regions.

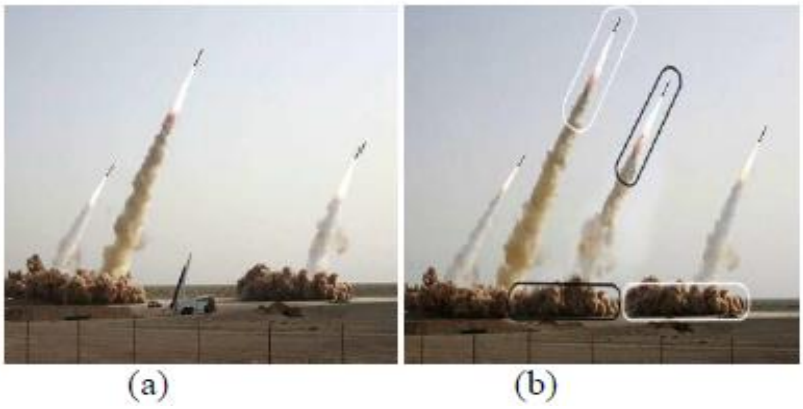

Fig 1: An example of copy-move forgery: (a) three missiles in original image (b) four missiles in tampered image.

The simple approach to detect if an image has been tampered by a copy-move forgery is exhaustive search, i.e. to compare an image with every cyclic-shifted version of itself. However, this approach is computationally very expensive and takes $(MN)^2$ steps for an image of size M × N, and does not work when the copy-pasted object is modified by geometric transformations (rotation, scaling, distortion) [5]. Mostly all of them are mainly categorized into two classes: key point-based methods and block-based methods. They both try to extract features, describing the local patches robustly, then evaluate similarity scores among various regions.

In block-matching, an image is first divided into overlapping blocks, significant features are extracted from each block, and compared to each other to find the most similar areas. At last, results are analyzed and decision is made only if there are several pairs of similar image blocks found within

the specified proximity. Several different features have been proposed to search copy alterations within a block-matching based system: Discrete Cosine Transform (DCT) coefficients [5], Principal Component Analysis (PCA) and Eigenvectors of the covariance matrix [6], Discrete Wavelet Transform and Singular Value Decomposition [7], color information [8], Fourier Mellin descriptors [9]. In [10] Ryu et al. proposed a method which is based on Zernike moments, which proved to be robust against several attacks. Block-matching approaches, depending on the selected features, are typically robust to noise addiction, compression, filtering, but lack of robustness against geometrical transformations (rotation, scaling, and distortion).

The point based approaches extract interest points and use local features, rather than blocks, to identify duplicated regions [11]. SIFT [12] and SURF [13] detectors are used to find points of interest in the images, and the related local descriptors are used to find matches between these points. To eliminate the false matches, they are typically filtered by using post-processing techniques, as RANSAC. RANSAC is also used [12] to estimate the geometric transformation applied to the copy-moved area. Point-based approaches proved to be robust to geometric transformation (rotation and scaling), but do not work if homogenous areas are used to hide an object, as key points cannot be extracted from those areas. An interesting work by Christlein et al. [14] compares and evaluates the results obtained with different approaches to the problem of copy-move forgery detection.

III. PROPOSED APPROACH

In this paper, a new interest point detector specifically designed for copy-move forgery detection (CMFD) is proposed. In this method, the entire image, even low contrast regions, is covered adaptively based on the distinctiveness metric. In order to concentrate more on the suspected regions, the interest key point density can also be automatically adjusted over the image. Finally, an appropriate descriptor for the detected interest points is employed. The architectural design for copy-move forgery detection is shown in the Figure 2. First, the interest key points are detected and those points are described using Polar Cosine Transform (PCT). After that, an adaptive matching is performed. Next, falsely matched pairs are removed by an effective filtering algorithm. In order to enhance the result, the whole process can be iterated regarding the prior information

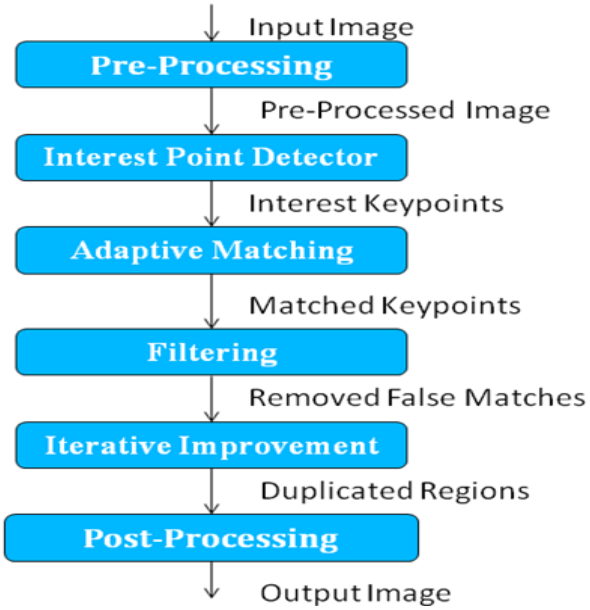

Fig 2: Architecture of the proposed system.

A. PreProcessing

The input natural image which might be in RGB is converted into gray scale image since the proposed copy-move forgery detection system operates on gray scale images only.

B. Interest Point Detector

In the existing method, the interest points are extracted using Speeded-Up Robust Features (SURF). This method cannot cover the whole image. The whole image can be covered adequately by interest points is essential in CMFD. The proposed scheme provides a full coverage of interest points whose density is adapted based on the local uniqueness. In order to estimate the visual complexity, different metrics can be used. The lower probability of observing a patch means more uniqueness [15]. The uniqueness metric, ,μi, for the i^{th} point is defined as follows:

$$\mu_i = \frac{1}{B}\sqrt{\sum_x \sum_y \left(\nabla^2 I(x,y)\right)^2}$$

$$\|(x,y) - (x_i,y_i)\| \le \frac{B}{2}$$

where B is the block size, ∇^2 - denote the Laplacian, ||.|| denote the Euclidean norm, I(x,y) denotes intensity of the input image. The proposed criterion is calculated for each point considering its surrounding block. The metric shows that the variations among less unique areas are insignificant. Hence it is reasonable to represent them more sparsely (with a fewer number of interest points). A local capacity $\xi_i^t)$ is calculated based on the uniqueness and the certainty level in order to adjust the density of interest points:$\xi_i^t = \gamma_i^t \mu_i$ in which γ_i^t (certainty level) informs the interest point detector of prior knowledge about suspicious regions. In the first iteration, the certainty levels γ_i^t are considered the same for all points. As the image resolution is increased, the local variations are restricted. As a result, the initial value of γ should be dependent to the size of the image. In the next iteration, the certainty levels are adjusted based on the previously achieved result.

In this case, all points are investigated based on their uniqueness, i.e., select more unique points are first. The chosen point is considered as an interest point provided that its capacity is greater than its local density d_i. The local density of each candidate point is calculated using a Gaussian window:

$$d_i = \sum_{k \in V} e^{-\frac{\|\chi_k - (x_j,y_j)\|^2}{2\sigma^2}}$$

$$V = \left\{k | \chi_k \epsilon \chi, \|\chi_k - (x_j,y_j)\| \le \frac{B}{2}\right\}$$

in which σ controls the distance weights and χ is the set of interest point locations. Smaller σ increases the sensitivity on close points and hence disperses the interest points. Considering the neighborhood radius of the local density which is equal to *B*/2, the feature extraction stage is forced to certainly represent the whole image. The appropriate value of σ should be dependent to *B*.

The detected interest points should be represented by a robust, invariant and distinctive feature utilizing the regions around them. Here, The PCT is utilized due to its maximal discrimination property. The PCT features of a continuous image, *g*, of order *n* with repetition *l* are defined as follows [16]:

$$f = \{|M_{n,l}| \text{ such that } n + l \leq 3, 0 \leq n, l < 3\}$$

in which $M_{n,l} = \Omega_n \int_0^{2\pi} \int_0^1 [H_{n,l}(r,\theta)]^* g(r,\theta) r dr d\theta$, $\Omega_n = \begin{cases} 1/\pi & n = 0 \\ 2/\pi & n \neq 0, \end{cases}$, $H_{n,l}(r,\theta) = \cos(\pi n r^2) e^{jl\theta}$

$g\ (r,\ \theta)$ indicates the representation of image in the polar coordinate. To describe the selected interest points, a $B \times B$ block around each interest point is transformed to the feature space. The feature set, F, consists of the representation of all selected points.

C. Adaptive Matching

After the image representation, the descriptors are compared to find candidate matches. To achieve a higher performance, the adaptive matching is utilized [17]. A linear function of the standard deviations of two blocks is employed to estimate their similarity threshold:

$$T_{sim}(S_i, S_j) = \alpha^t \frac{S_i + S_j}{2} + \beta^t$$

in which T_{sim} is the threshold function, S_i and S_j represent the standard deviation of the corresponding blocks estimating the energy of high frequency components, α^t and β^t are user-defined parameters should be adjusted based on the selected feature space and the similarity distance measure and t indicates the iteration number.

Adaptive threshold is employed in the matching procedure using lexicographic sorting. The feature matrix, *F*, is lexicographically sorted.

The sorted feature matrix is indicated as F.S is also the reordered version of *S* based on the sorted feature matrix. The Euclidean distances between the adjacent pairs of the sorted set are calculated. If the similarity distance of two interest points is lower than an adaptive threshold, they will be considered as a candidate match:

$$\|\hat{F}_p - \hat{F}_{p+q}\| \leq T_{sim}(\hat{S}_p, \hat{S}_{p+q})$$

$$-T_{search} \leq q \leq T_{search}$$

where T_{search} denotes the search range. It should be noted that high similarity between neighboring regions may cause a huge number of false matches. Therefore, a minimum spatial distance criterion is also calculated in conjunction with the above equation:
$\|\chi_i - \chi_j\| \geq B$

where x_i and x_j are locations of the interest points under investigation. The two keypoints considered as a potential match if the conditions presented in the above two equations are satisfied. The matching table,w, is used to denote the potential matches as follows:

$$\omega_{i,j} = \begin{cases} 1 & i^{th} \text{ and } j^{th} \text{ interest points are matched} \\ 0 & \text{otherwise} \end{cases}$$

D. Filtering

Due to the intrinsic self-similarity of natural images, a considerable number of candidate matched pairs may be falsely assigned. Nevertheless, matches that originate from the same copy-move action present a common behavior. Examining this common behavior can be helpful to discard falsely matched pairs. It is common to estimate the relationship between each copied region with its corresponding in term of an affine transform.

The proposed filtering algorithm increases the probability of finding correct matches in addition to decrease the computational cost. The segmentation is performed by Simple Linear Iterative Clustering (SLIC) algorithm [18] using vlFeat library. The orientation of matches was estimated using the phase of PCT [10]. The rotation angle between pairs can be determined by analyzing the phase of PCT coefficients. In this implementation, the phase information is extracted from :

$$\varphi = \measuredangle M_{0,1} mod\ 2\pi$$

The phase difference is calculated as follows: $mod\ 2\Delta\varphi_{ij} = min(|\varphi_i - \varphi_j|, \quad 2\pi - |\varphi_i - \varphi_j|)\pi$

RANSAC can only concentrate on pairs with the same phase differences. Thus, the search space for the affine estimation is more confined to matched pairs with a similar orientation. The phase similarity threshold is called . is used for validating based on the scale information. Lastly, the achieved affine transform can be generalized to other pairs with compatible orientations. Threshold T_g is exploited to differentiate inlier matches from outliers. The number of inliers must be greater than another threshold $T_{inliers}$.

The *Transform Estimation* function gets a set of matched points as the input and then estimate an affine transform, using RANSAC algorithm. Ψ is a 3×3 matrix:

$$\Psi = \begin{bmatrix} \Psi_{11} & \Psi_{12} & \Psi_{13} \\ \Psi_{21} & \Psi_{22} & \Psi_{23} \\ 0 & 0 & 1 \end{bmatrix}$$

which can describes the geometric relationship between two points (x,y) and (x',y'): $\Psi(1:2,1:2)$ consists of the scaling and rotation information of transformation. At least three non-collinear pairs are required to estimate Ψ At the end of this stage, the pairs which are not detected as correct are removed from the matching table w

E. Iterative Improvement

Some time, the whole duplicated regions may not be detected precisely due to the discrete nature of interest points. T o address this issue it is proposed to use iterative improvement method where this procedure utilizes the achieved prior information in order to more accurately determine the duplicated regions. The suspected duplicated regions (*SR*) along with their geometric relationships are available. *SR* is defined as neighbors of the matched interest points:

$$SR^t(x,y) = \begin{cases} 1 & \min_{j \in H^t}(\|(x,y) - \chi_j\|) \le \frac{B}{2} \\ 0 & otherwise \end{cases}$$

in which *H* is the collection of paired interest points: $H^t = \left\{ j | \sum_k \omega_{j,k}^t \ge 1 \right\}$

The detection process is iterated considering the available information. In each iteration, firstly, the interest point density is increased in suspected regions (*SR*) by λ_γ^c while in the other regions density is decreased by λ_γ^f

By modifying the certainty level γ, the capacities are adjusted as follows:

$$\gamma_i^{t+1} = \begin{cases} \lambda_\gamma^c \gamma_i^1 & if\ SR^t(x_i, y_i) = 1 \\ \lambda_\gamma^f \gamma_i^1 & otherwise \end{cases}$$

Certainty level parameter allows the procedure to iterate and control the density of interest points. The i^{th} interest point in the t^{th} iteration must satisfy the following condition to be considered in the next stages:

$$\exists (x, y)\ such\ that\ \|(x, y) - \chi_i^t\| \leq \frac{B}{2}$$

$$\wedge \forall k \in \{1, \dots, t-1\} SR^k(x, y) \neq 1$$

To validate the newly detected pairs, the filtering stage only uses the previous estimated transforms. The final forgery map (*FR*) is determined through union of all detected suspected regions:

$$FR(x, y) = SR^1(x, y) \vee SR^2(x, y) \vee \dots$$

This procedure can be iterated until either two successive iterations achieve similar results or a certain number of repetitions. In this implementation, the number of iterations is limited to two to achieve the maximum efficacy of the iterative strategy.

F. Post-Processing

At the end of the copy-move forgery detection, for the better visualization the grayscale image is again converted into the RGB image. Different colors are used to represent the tampered regions.

IV. EXPERIMENTAL RESULTS

Experiments were conducted by taking sample images from GRIP and SBU-CM16 dataset. Experiment result obtained was shown for one sample image in figure 3. The input tampered image and the corresponding grayscale image are shown in figure 3 (a) and (b) respectively. Figure (c) and (d) shows the image after performing the 1st and 2nd iteration respectively. Figure (e) shows the duplicated regions

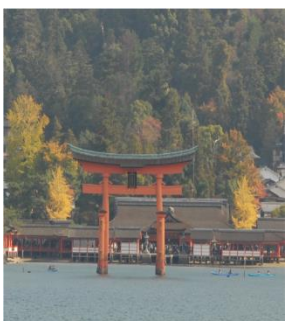

Fig-3 (a)

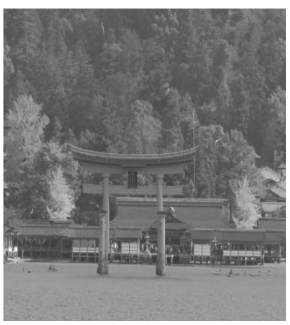

Fig-3 (b)

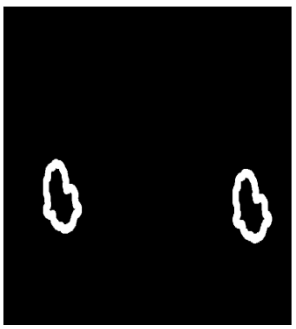

Fig-3 (c)

Fig-3 (d)

Fig-3 (e)

To evaluate the accuracy of the proposed work, precision (*P*), recall (*R*), True Positive Rate (*TPR*) and False Positive Rate (*FPR*) are also calculated.

$$P = \frac{|\{Forged\ Pixels\} \cap \{Detected\ Pixels\}|}{|\{Detected\ Pixels\}|}$$

$$R = \frac{|\{Forged\ Pixels\} \cap \{Detected\ Pixels\}|}{|\{Forged\ Pixels\}|}$$

$$TPR = \frac{|\{Images\ Detected\ Correctly\}|}{|\{Total\ Images\}|}$$

$$FPR = \frac{|\{Images\ Detected\ Wrongly\}|}{|\{Total\ Images\}|}$$

Table 1 shows the performance analysis for the comparison between the proposed method and the existing method using Precision and Recall and Table 2 shows the performance analysis for the comparison between the existing method and the proposed method using True Positive Rate and False Positive Rate.

Table 1 Performance Analysis using Precision and Recall

Methods	Precision (%)	Recall (%)
Existing Method	85	73
Proposed Method	93	86

Table 2 Performance Analysis using True Positive Rate and False Positive Rate

Methods	True Positive Rate (%)	False Positive Rate (%)
Existing Method	78	22
Proposed Method	90	10

V. CONCLUSION

The proposed method is used to find whether the image is forged one or not. This work deals with the detection of copy-move forgery. The interest points are detected using new interest point detector. The adaptive matching process is done for the detected keypoints. A new filtering algorithm is utilized to remove the false matches. Then the whole detection process is iterated in order to achieve a precise result. This method is robust to geometric transformations.

VI. FUTURE WORK

The proposed work does not identify other types of image forgery techniques such as enhancing and splicing attack and it identifies only the copy-move forgery. The future work is to improve the proposed interest point detector by means of scale-space techniques in order to deal with the resizing attack more effectively.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical statement: The authors declare that they have followed ethical responsibilities.

REFERENCES

[1] M. Zandi, A. Mahmoudi-Aznaveh and A. Talebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector," in IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,2499-2512, 2016.
[2] H. Farid, "Image forgery detection," IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.
[3] H. T. Sencar and N. Memon, "Overview of state-of-the-art in digital image forensics," Algorithms, Archit. Inf. Syst. Secur., vol. 3, pp. 325–348, Dec. 2008.
[4] B. L. Shivakumar and S. S. Baboo, "Detecting copy-move forgery in digital images: A survey and analysis of current methods," Global J. Comput. Sci. Technol., vol. 10, no. 7, pp. 61–65, 2010.
[5] J. Fridrich, D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, USA, Aug. 2003, pp. 342–358.
[6] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.
[7] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Proc. IEEE Int. Conf. Multimedia Expo, 2007, 1750–1753.
[8] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Proc. 18th Int. Conf. Pattern Recognit., 2006, pp. 746–749.
[9] W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in Proc. 17th IEEE Int. Conf. Image Process. (ICIP), Sep. 2010, pp. 2113–2116.
[10] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Proc. Inf. Hiding Conf., Jun. 2010, pp. 51–65.
[11] X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.
[12] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[13] L. Jing and C. Shao, "Image copy-move forgery detecting based on local invariant feature," J. Multimedia, vol. 7, no. 1, pp. 90–97, Feb. 2012.
[14] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, 2012.
[15] M. Loog and F. Lauze, "The improbability of Harris interest points," IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 6, pp. 1141–1147, Jun. 2010.
[16] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," Forensic Sci. Int., vol. 224, pp. 59–67, Jan. 2013.
[17] M. Zandi, A. Mahmoudi-Aznaveh, and A. Mansouri, "Adaptive matching for copy-move forgery detection," in Proc. IEEE Int. Workshop Inf. Forensics Secur., Atlanta, GA, USA, 2014, pp. 119–124.
[18] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, "SLIC superpixels," School Comput. Commun. Sci., École Polytechn. FédÉrale Lausanne, Lausanne, Switzerland, Tech. Rep. 149300, Jun. 2010.