Inpainting forgery detection using hybrid generative/discriminative approach based on bounded generalized Gaussian mixture model

Received 12 November 2019
Revised 1 December 2019
Accepted 9 December 2019

Abdullah Alharbi and Wajdi Alhakami
College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
Sami Bourouis
College of Computers and Information Technology, Taif University, Taif, Saudi Arabia and
Université de Tunis El Manar, LR-SITI Laboratoire Signal, Image et Technologies de l'Information, Tunis, Tunisia
Fatma Najar
Université de Tunis El Manar, LR-SITI Laboratoire Signal, Image et Technologies de l'Information, Tunis, Tunisia, and
Nizar Bouguila
The Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, Canada

Abstract

We propose in this paper a novel reliable detection method to recognize forged inpainting images. Detecting potential forgeries and authenticating the content of digital images is extremely challenging and important for

The authors would like to thank the Deanship of Scientific Research at Taif University, Kingdom of Saudi Arabia, for their funding support under Grant No.: 1-439-6116.

Declaration of Competing Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Publishers note: The publisher wishes to inform readers that the article "Inpainting forgery detection using hybrid generative/discriminative approach based on bounded generalized Gaussian mixture model" was originally published by the previous publisher of *Applied Computing and Informatics* and the pagination of this article has been subsequently changed. There has been no change to the content of the article. This change was necessary for the journal to transition from the previous publisher to the new one. The publisher sincerely apologises for any inconvenience caused. To access and cite this article, please use Alharbi, A., Alhakami, W., Bourouis, S., Najar, F., Bouguila, N. (2019), "Inpainting forgery detection using hybrid generative/discriminative approach based on bounded generalized Gaussian mixture model", *Applied Computing and Informatics*. Vol. ahead-of-print No. ahead-of-print. https://10.1016/j.aci.2019.12.001. The original publication date for this paper was 19/12/2019.

Applied Computing and Informatics
Vol. 20 No. 1/2, 2024
pp. 89-104
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1016/j.aci.2019.12.001

many applications. The proposed approach involves developing new probabilistic support vector machines (SVMs) kernels from a flexible generative statistical model named "bounded generalized Gaussian mixture model". The developed learning framework has the advantage to combine properly the benefits of both discriminative and generative models and to include prior knowledge about the nature of data. It can effectively recognize if an image is a tampered one and also to identify both forged and authentic images. The obtained results confirmed that the developed framework has good performance under numerous inpainted images.

Keywords Forgery detection, Mixture models, Bounded generalized Gaussian mixture model, SVM kernels, Statistical machine learning, Big data

Paper type Original Article

1. Introduction

With the advancements in computer-related technologies more multimedia data are created in digital form allowing easy control over the handling, collection, and storage of such data. The rapid technological advances have amplified the amount of multimedia data generated every day. Analyzing these huge data is generally known as the BIG DATA analysis problem. This is especially true for visual data (images and videos) generated in the Web and social networks. These multimedia data can be used for example to discover digital evidences before, when, after a cybernetic security attack has occurred [1]. This scenario is often called digital forensics. The challenging problem in this case is the insurance of the completion of evidences which is considered one of the high priority principals that must be taken into account in any forensics investigation. Indeed, if some parts are deleted from original image, it will be very difficult to investigate forensically. Furthermore, any missing data can lead to erroneous investigation conclusions and make the evidences lose their credibility in the judiciary court. Today's digital image forensics has become an emerging research field due to this big amount of generated digital image files [2,3] In this context, digital images and videos can be used for example for inpainting purposes. Indeed, image (resp. video) inpainting [4–6] is one of the interesting techniques used for data restoration that can restore lost and deteriorated information. Inpainting is known as a problem of filling the missing content in an image in order to repair a possible damage and manipulation. This research topic has positive impact for a variety of applications such as restoring old corrupted films and movies, producing new stories, improving the quality of noisy movies, etc.

Existing inpainting techniques can be divided into two categories: interpolation-based methods, and exemplar-based methods. The interpolation-based methods perform filling-in the areas by interpolation of the available data mostly using non-linear partial differential equations (PDEs) [7]. The exemplar-based methods on the other hand are very similar to the texture synthesis-based image inpainting methods, except that the texture (structure) sampling task is carried out by considering all the frames and also the moving objects, not only a single image as in the case of the texture synthesis-based image inpainting techniques [4]. Criminisi's algorithm [4] is one of the most known algorithms among other exemplar-based inpainting approaches. Nevertheless, image inpainting techniques might be exploited to alter and delete content for malicious motives and can be used to generate the so-called forged image. Forgery aims at duplicating or hiding some parts in such image. Indeed, given the recent technology progress, it has become extremely easy to manipulate digital images and so it is difficult to guarantee their authenticity. In many cases, it is impossible for a viewer to judge the authenticity of a given image. Therefore, it is increasingly important to guarantee the integrity of the vast volumes of multimedia data before using them in many situations such as courts of law.

Providing efficient methods to digital forgery detection was and still a fundamental goal for researchers to establish the authenticity and origin of digital multimedia contents. Digital authenticity detection (e.g. inpainting, cloning, resampling, etc.) is becoming one of the attractive research areas in image (resp. video) processing [8] and this problem can be viewed as the problem of constantly distinguishing between forged and original real images (resp. videos). Figure 1 illustrate an example of copy-move forgery.

2. Related works and motivations

Basically, there are two major approaches for protecting digital multimedia data against tampering: active [10] and passive [11] approaches. For the case of active one, tampered region can be extracted using watermarking techniques while passive techniques have been developed in response to watermarking limitations.

In the recent past, some efforts have been devoted to solve this hot topic. Many of them are block-based methods that involve a feature extraction step to each block. Some effective block-based methods were developed to detect forgeries using robust features such as DCT, DWT, SVD (singular value decomposition), and PCA (Principal Component Analysis) [12–15,11]. For instance, DWT and SVD are combined and matched to detect duplicate regions in [15]. DCT is also used to extract features and to improve the detection precision in [13]. Zernike moments, which are invariant to rotations, are also applied in [16] to judge tampering. Other techniques exploit inconsistencies or unnatural high coherence observed in an image to detect duplicated elements. For instance in [17] authors proposed a method based on inspecting lighting conditions. In another effort [14], authors used the correlation characteristics between segments to detect duplicated regions. In [18] pattern noise is computed and then used to compare between the studied image and the reference pattern. Other works proposed to handle local transformations using keypoint-based methods like the scale-invariant feature transform (SIFT) features and descriptor algorithms, which are broadly applied in computer vision applications [19–21]. These algorithms are based on local features extraction and cost in general less time. In [19] authors proposed to apply the scale and rotation-invariant SIFT in order to extract and to match similar local features. Then, an agglomerative hierarchical clustering is performed to identify multiple cloned and forged regions. SIFT is also applied in [20] to determine keypoints and their visual features which are used in conjunction with RANSAC algorithm. An iterative detection algorithm was developed in [22] to localize duplicated regions based on both a keypoint-based and block-based methods so as to enhance the expected results. Furthermore, false matched regions are removed through a novel designed filter algorithm. So as to improve the copy-move forgery detection accuracy, some recent works proposed to take into account a segmentation step [23,24]. Indeed, in [23] the computational complexity is minimized by segmenting a suspicious image into independent patches. More specifically, SIFT and SURF are employed to identify salient points and the expectation–maximization (EM) algorithm is used to filter false patches and to increase the detection accuracy. In [9], interest points are extracted and clustered on the basis of some geometric constraints. Then, a multi-scale analysis process is utilized to examine the generated clusters and to detect duplicated regions. Even though most of the proposed methods are considered robust against blur and noise and can help in detecting forgery, however, most of them are computationally expensive, fail to handle images containing smooth and low contrast

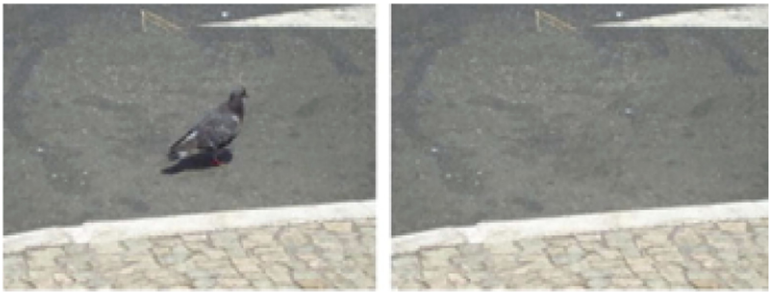

Figure 1.
Inpainting copy-move forgery example (here the bird is fully hidden). Original image in the left and copy-move forgery in the right side [9].

regions, and may not be able to detect some complex attacks (i.e inpainting forgery). Moreover, it is not expected to think about the possibility to exploit these methods and extend them for the case of video forgery detection.

Artificial intelligence and machine learning are a growing areas of research that offer potential benefits to solve difficult problems like forgery. Statistical approaches provide a formal way for image modelling and classification [25,26]. In particular, finite mixture models have attracted great interest among other approaches [25,27,28] [29]. Recently, some developed mixtures were applied successfully in the case of forgery detection problem [21,30]. In this context, we address the problem of image forgery detection by investigating recent developed mixture model named finite bounded generalized Gaussian mixtures (BGGMM) [31,32]. The consideration of BGGMM is encouraged by the fascinating results exposed recently and show this model as more effective for data classification and modeling than the conventional Gaussian mixtures [31,26]. Indeed, BGGMM has the advantage to fit data with different shapes defined within a bounded support and to maintain the goodness of fit. However, a crucial problem when we consider deterministic algorithms (such as the EM algorithm) to learning generative mixture models (in particular BGGMM) is their convergence to saddle points and their dependency on the initialization step [31,26,25].

3. A hybrid of bounded generalized gaussian mixture model and SVM

To cope with generative models limitations, one can think in using discriminative models instead of generative ones. Indeed, it has been shown in many contexts that discriminative classifiers (eg. SVM) are generally higher than generative models [33–35]. However, traditional discriminative classifiers fail also to reach high performances for all possible applications. In particular, the main problem with standard SVM kernels is that they are unable to consider the nature of training data and therefore they can not handle proportional data properly like the problem of image forgery. For all these reasons, we propose in this manuscript to develop a more powerful generative-discriminative approach based new implemented kernels. The key idea is to combine the strengths of both generative and discriminative models into one same hybrid framework. In particular, we intend to develop more appropriate and flexible SVM kernels from the generative bounded generalized Gaussian mixture model (BGGMM) for tampering detection. The ultimate goal is to improve the SVM capability in data forgery detection which is actually a challenging task and to achieve better performance when new hybrid learning approach is developed instead to motivate more this particular choice. To the best of our knowledge the generating of new SVM kernels from bounded generalized Gaussian mixtures and its application to the problem of image forgery detection have never been tackled before.

In the past, some standards SVM kernels (like linear kernel, RBF, polynomial) have been proposed [36] and it should be noted that these kernels pay no attention to the intrinsic structure of input data. As indicated in [37], if the selected kernel is constructed directly from data then this process yields to have more effective classification performances. Among the most valuable probabilistic kernels in this context we can cite especially the Information-based kernel (known also as Kulback-Leibler kernel), the Fisher kernel, and the Bhattacharyya-based kernel [37–39]. In the following sections we will expose our developed new probabilistic SVM kernels from bounded generalized Gaussian mixture model to deal with the forgery detection challenge.

3.1 Bounded generalized Gaussian mixture model

Although conventional Gaussian and generalized Gaussian mixture models have achieved acceptable results previously for data modelling and classification [40,41], nevertheless, their distributions are not bounded which limit their performances. Then again, a lot of real-life applications and sources have a bounded support. Consequently, considering this constraint when proceeding with mixture models will definitely enhance classification results and also the detection precision. In this work, we propose to investigate a flexible mixture model known as bounded generalized Gaussian models for forgery detection. This model has been proposed earlier in [31] for image segmentation. In this paper we propose to investigate the BGGMM in conjunction with discriminative approaches. The bounded generalized Gaussian distribution (BGGD) is considered among the recent successful finite mixture models for machine learning and pattern recognition applications [31,26] and it is proposed to generalize several other statistical distributions as such as the Gaussian, Uniform, and Laplacian distributions. It has the advantage to better fit different non-Gaussian shapes.

Let $x = (\overrightarrow{X}_1, \ldots, \overrightarrow{X}_N)$ be a set of N images. Each image $\overrightarrow{X}_i$ is represented by an d-dimentional vector generated by a linear combination of M bounded generalized Gaussian distribution given as follows:

$$p(\overrightarrow{X}_i|\Theta) = \sum_{j=1}^{M} p_j \psi(\overrightarrow{X}_i|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j) \tag{1}$$

where p_j is the mixing parameter that should satisfy for each component $j(0 \leq p_j \leq 1, \sum_{j=1}^{M} p_j = 1)$ and $\Theta = (\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)$ is the set of the parameters for the component j represented by a BGGD which is characterized by mean parameter $\overrightarrow{\mu}_j = (\mu_{j1}, \ldots, \mu_{jd})$, covariance matrix $\overrightarrow{\sigma}_j = (\sigma_{j1}, \ldots, \sigma_{jd})$, and shaper parameter $\overrightarrow{\lambda}_j = (\lambda_{j1}, \ldots, \lambda_{jd})$.

$$\psi(\overrightarrow{X}_i|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j) = \frac{p(\overrightarrow{X}_i|\vec{\mu}_j, \vec{\sigma}_j, \vec{\lambda}_j) H(\overrightarrow{X}_i|\Omega_j)}{\int_{\delta_j} p(\overrightarrow{X}_i|\vec{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j) dx}, \tag{2}$$

where $p(\overrightarrow{X}_i|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)$ is the probability density function of the generalized Gaussian mixture model (GGMM) given by:

$$p(\overrightarrow{X}_i|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j) = \prod_{k=1}^{d} F(\lambda_{jk}) exp\left(-G(\lambda_{jk})\left|\frac{X_{ik} - \mu_{jk}}{\sigma_{jk}}\right|\lambda_{jk}\right) \tag{3}$$

where

$F(\lambda_{jk}) = \frac{\lambda_{jk}\left[\frac{\Gamma(3/\lambda_{jk})}{\Gamma(1/\lambda_{jk})}\right]^{1/2}}{2\sigma_{jk}\Gamma(1/\lambda_{jk})}$, $G(\lambda_{jk}) = \left[\frac{\Gamma(3/\lambda_{jk})}{\Gamma(1/\lambda_{jk})}\right]^{\lambda_{jk}/2}$, $\Gamma(.)$ is the gamma function, and $H(\overrightarrow{X}_i|\Omega_j)$ is the indicator function, δ is a bounded support region defined for each region Ω_j).

$$H(\overrightarrow{X}_i|\Omega_j) = \begin{cases} 1 & If\ \overrightarrow{X}_i \in \delta_j \\ 0 & Otherwise \end{cases} \tag{4}$$

3.2 Generative model estimation

Given the set of images x, the complete log-likelihood corresponding to M mixture of BGG distributions is introduced as follows:

$$L(x|\Theta) = \sum_{i=1}^{N} \log \sum_{j=1}^{M} p_j \psi(\overrightarrow{X}_i | \overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j) \tag{5}$$

The parameters of this model BGGMM are learned by maximizing the log likelihood using the expectation-maximization algorithm (Algo.1). During the expectation stage, the posterior probability (known also as responsibility) is calculated as:

$$p(j|\overrightarrow{X}_i) = \frac{p_j \psi(\overrightarrow{X}_i | \overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)}{\sum_{m=1}^{M} p_m \psi(\overrightarrow{X}_i | \overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)} \tag{6}$$

Based on those calculated responsibility, the parameters of the mixture are determined in the maximization step and are updated according to:

$$\Theta^{(t+1)} = \underset{\Theta}{argmax}\; L(x|\Theta) \tag{7}$$

when maximizing the above equation, we obtain:

- Mixing weight estimation:

$$p_j^{(t+1)} = \frac{1}{N} \sum_{i=1}^{N} p(j|\overrightarrow{X}_i) \tag{8}$$

- Mean estimation:

$$\widehat{\mu}_{jk} = \frac{\sum_{i=1}^{N} p(j|\overrightarrow{X}_i)(|X_{ik} - \mu_{jk}|^{\lambda_{jk}-2} X_{ik} + T_{jk})}{\sum_{i=1}^{N} p(j|\overrightarrow{X}_i)|X_{ik} - \mu_{jk}|^{\lambda_{jk}-2}} \tag{9}$$

where:

$$T_{jk} = \frac{\sum_{m=1}^{M} sign(\mu_{jk} - s_{mjk})|\mu_{jk} - s_{mjk}|^{\lambda_{jk}-1} H(s_{mjk}|\Omega_j)}{\sum_{m=1}^{M} H(s_{mjk}|\Omega_j)} \tag{10}$$

- Covariance matrix estimation:

$$\widehat{\sigma}_{jk} = \left[\frac{\lambda_{jk} A(\lambda_{jk}) \sum_{i=1}^{N} p(j|\overrightarrow{X}_i)|X_{ik} - \mu_{jk}|^{\lambda_{jk}}}{\sum_{i=1}^{N} p(j|\overrightarrow{X}_i)(1 + Q_{jk})} \right]^{1/\lambda_{jk}} \tag{11}$$

where

$$Q_{jk} = \frac{\sum_{m=1}^{M} (-1 + \lambda_{jk} A(\lambda_{jk})|s_{mjk} - \mu_{jk}|^{\lambda_{jk}} (\sigma_{jk})^{-\lambda_{jk}}) H(s_{mjk}|\Omega_j)}{\sum_{m=1}^{M} H(s_{mjk}|\Omega_j)} \tag{12}$$

- Shape parameter estimation:

$$\widehat{\lambda}_{jk} = \lambda_{jk} - \left\{ \frac{\partial^2 log[p(X|\Theta)]}{\partial \lambda_{jk}^2} + \gamma \right\}^{-1} \frac{\partial log[p(X|\Theta)]}{\partial \lambda_{jk}}, \tag{13}$$

where γ denotes a scaling factor. $\frac{\partial^2 log[p(X|\Theta)]}{\partial \lambda_{jk}^2}$ and $\frac{\partial log[p(X|\Theta)]}{\partial \lambda_{jk}}$ are detailed in [31].

Algorithm 1 Parameter estimation of the Bounded Generalized Gaussian Mixture Model

```
Require: $\mathcal{X}, M$
Ensure: $\Theta*$
  Initialization: Applying k-means algorithm to initialize the
  mixture's parameters.
  repeat
    for j:=1 to do
      Expectation-step: Evaluate the responsibility using Eq. 6
      Maximization-step: Calculate $\vec{\mu}_j$ $\vec{\sigma}_j$ and $\vec{\lambda}_j$ using Eqs. 9,
  11, and 13 respectively.
    end for
  until Convergence
```

3.3 Deriving SVM kernels from BGGMM

A crucial step for image forgery detection is visual features extraction. In this work we proceed with SURF (Speeded-Up Robust Features) descriptor [42] which is robust and invariant to geometric transformations. The proposed methodology is as follow: first, visual features are extracted using SURF detector. Each image is encoded as a vector of SURF features and then modeled through the finite mixture models (BGGMM). Secondly, kernel matrices are constructed on the basis of the mixture models. The generated kernels are Fisher information, Bhattacharyya kernels, and probabilistic-based distances between each of these mixture models. The SVM-based classifiers are developed to find the optimal estimated parameters. Thus, the main objective is to investigate the forgery detection results when using different SVM kernels while the BGGMM represent the core of these kernels. A flowchart summarizing and describing the proposed method is depicted in Figure 2. In the next subsections, we presented all necessary details regarding the different developed kernels.

3.3.1 Fisher kernels. The key intuition behind the Fisher kernel [37] is that it measures the similarity of two distributions (mixtures). Moreover, similar distributions imply same log-likelihood gradients in the mixture space. Thus, in order to construct Fisher kernel, we need to calculate the log-likelihood gradient of every distribution or mixture. In our case, we investigate the concept of the Fisher kernel for forgery detection since it is considered as a generic bridge between discriminative methods and probabilistic generative models and so it combines the benefits of both of them. In the following we replace the standard SVM kernels by developing our proper Fisher kernel based on the BGGMM.

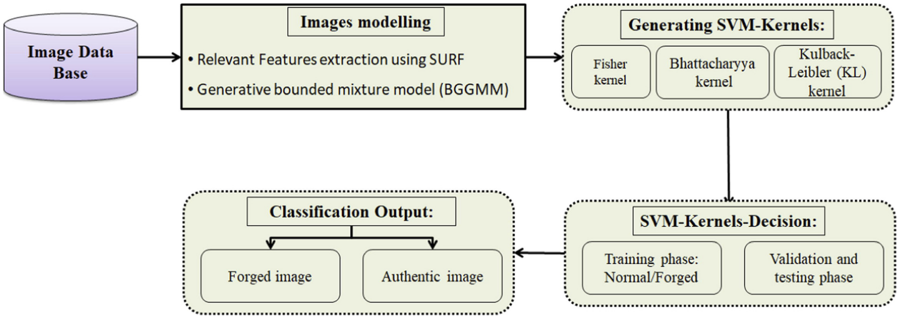
Image Data Base
Images modelling
• Relevant Features extraction using SURF
• Generative bounded mixture model (BGGMM)
Generating SVM-Kernels:
Fisher kernel
Bhattacharyya kernel
Kulback-Leibler (KL) kernel
SVM-Kernels-Decision:
Training phase: Normal/Forged
Validation and testing phase
Classification Output:
Forged image
Authentic image

Figure 2.
Flowchart of the proposed method.

$$k(X,X^{'}) = U_X^{tr}(\Theta)I^{-1}(\Theta)U_{X'}(\Theta^{'}) \tag{14}$$

$$\frac{\partial L}{\partial \mu_{jk}} = B(\lambda_{jk})\frac{\lambda_{jk}}{\sigma_{jk}^{\lambda_{jk}}}\sum_{i=1}^{N} Z_{ij}|X_{ik} - \mu_{jk}^{\lambda_{jk}-2} \left[X_{ik} + \mu_{jk} - \frac{R_j}{|X_{ik} - \mu_{jk}|^{\lambda_{jk}-2}}\right] \tag{15}$$

where

$$R_j = \frac{\sum_{m=1}^{M} sign(\mu_{jk} - s_{mj})|s_{mj} - \mu_{jk}|^{\lambda_{jk}-1}H(s_{mj}|\Omega_j)}{\sum_{m=1}^{M} H(s_{mj}|\Omega_j)} \tag{16}$$

$$\frac{\partial L}{\partial \sigma_{jk}} = \sigma_{jk}^{-1}\sum_{i=1}^{N} Z_{ij}\left[-1 + B(\lambda_{jk})|X_{ik} - \mu_{jk}|^{\lambda_{jk}}\lambda_{jk}\sigma_{jk}^{\lambda_{jk}} - G_j\right] \tag{17}$$

where

$$G_j = \frac{\sum_{m=1}^{M}(-1 + \lambda_{jk}B(\lambda_{jk}))|s_{mj} - \mu_{jk}|^{\lambda_{jk}}\sigma_{jk}^{-\lambda_{jk}}H(s_{mj}|\Omega_j)}{\sum_{m=1}^{M} H(s_{mj}|\Omega_j)} \tag{18}$$

$$\frac{\partial L}{\partial \lambda_{jk}} = \sum_{i=1}^{N} Z_{ij}\left[f(X_{ik}|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)) - \frac{\int_{\delta_j}\psi(\overrightarrow{X}_i|\overrightarrow{\mu}_{j,} \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)f(X_{ik}|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)dx}{\int_{\delta_j}\psi(\overrightarrow{X}_j|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j)dx}\right] \tag{19}$$

where

$$f(X_{ik}|\overrightarrow{\mu}_j, \overrightarrow{\sigma}_j, \overrightarrow{\lambda}_j) = \left[\frac{1}{\lambda_{jk}} + \frac{3\psi(1/\lambda_{jk}) - 3\psi(3/\lambda_{jk})}{2\lambda_{jk}^2}\right] - B(\lambda_{jk})\left|\frac{X_{ik} - \mu_{jk}}{\lambda_{jk}}\right|^{\lambda_{jk}}\log\left|\frac{X_{ik} - \mu_{jk}}{\lambda_{jk}}\right| - B(\lambda_{jk}) \tag{20}$$

$$\frac{\partial L}{\partial p_j} = \sum_{i=1}^{N}\left[\frac{p(j|\overrightarrow{X}_i)}{p_j} - \frac{p(1|\overrightarrow{X}_i)}{p_1}\right], j = 2, \ldots, M \tag{21}$$

3.3.2 Information divergence kernels. In order to combine the best of both discriminative methods and generative mixture models, we derive here a kernel distance based on the Kullback–Leibler (KL) divergence [38] between BGGMM mixtures. The key idea consists of constructing kernels on the basis of information divergence which is an interesting family allowing the measure of dissimilarity between different probability distributions and has direct connections to many existing probabilistic kernels. In this work, we opt for a common metric derived from the Kulback-Leibler (KL) divergence which is one of the essential quantities in machine learning. Hence, the dissimilarity between two probability distributions $p(\overrightarrow{X}|\Theta_1)$ and $q(\overrightarrow{X}^{'}|\Theta_2)$ is given as:

$$k(p(\overrightarrow{X}|\Theta_1), q(\overrightarrow{X}^{'}|\Theta_2)) = e^{-AD(p(\overrightarrow{X}|\Theta_1), q(\overrightarrow{X}^{'}|\Theta_2))} \tag{22}$$

where the factor $A > 0$ is used for numerical stability reason, and

$$D(p(\overrightarrow{X}|\Theta_1), q(\overrightarrow{X}^{'}|\Theta_2)) = \int_{\omega} p(\overrightarrow{X}|\Theta_1)\log\frac{p(\overrightarrow{X}|\Theta_1)}{q(\overrightarrow{X}^{'}|\Theta_2)} + q(\overrightarrow{X}^{'}|\Theta_2)\log\frac{q(\overrightarrow{X}^{'}|\Theta_2)}{p(\overrightarrow{X}^{'}|\Theta_1)} \quad (23)$$

Given that it is not possible to have a closed form equation for the KL divergence kernel, therefore we opt for numerical approximation techniques such as the well-known Monte Carlo method [43,44].

$$k(p(\overrightarrow{X}|\Theta_1), q(\overrightarrow{X}^{'}|\Theta_2)) \approx \frac{1}{L}\sum_{i=1}^{L}\log\frac{p(\overrightarrow{X}_i|\Theta_1)}{q(\overrightarrow{X}^{'}_i|\Theta_2)} \quad (24)$$

3.3.3 Bhattacharyya kernels. In this section, we opt for another distance called "Bhattacharyya distance" [45], which allowing us the measure of the similarity between two probability density functions such as BGGMM. Then, we name the derived kernel from this distance as Bhattacharyya kernel. As it is impossible to estimate a closed form for the Bhattacharyya kernel for the bounded mixture model BGGMM which is intractable, therefore, we proceed like the case of Kullback-Leibler (KL) divergence by approximating a Bhattacharyya kernel using Monte Carlo simulation method [43,44].

$$k_{\frac{1}{2}}(\overrightarrow{X}_1, \overrightarrow{X}_2) = \int_0^1 p(\overrightarrow{X}|\Theta_1)^{1/2} q(\overrightarrow{X}|\Theta_2)^{1/2} d\overrightarrow{X} \quad (25)$$

$$k_{\frac{1}{2}}(\overrightarrow{X}_1, \overrightarrow{X}_2) \approx \frac{\beta}{N_1}\sum_{i=1}^{N_1}\frac{p^{1/2}(\overrightarrow{X}_i|\Theta_1)}{Z_1}p^{1/2}(\overrightarrow{X}_i|\Theta_1) + \frac{1-\beta}{N_2}\sum_{i=1}^{N_2}\frac{q^{1/2}(\overrightarrow{X}_i|\Theta_2)}{Z_2}q^{1/2}(\overrightarrow{X}_i|\Theta_2) \quad (26)$$

where $\beta \in [0, 1]$ and the normalized factors Z_1, Z_2 are used for the densities p and q.

4. Experimental results

We have carried out experiments to assess the ability of the proposed approach in forgery detection problem. We present here comparative study with other well known mixture models which are broadly applied in the context of data classification. Please note that the purpose here is to evaluate our model against comparable methods and not against all state of the art algorithms which is out of the scope of this manuscript. The problem of image forgery detection can be seen as the issue of identifying forged images from authentic ones. It can be seen therefore as a classification problem.

4.1 Synthetic dataset

First of all, we begin by investigating the efficiency and the flexibility of our generative BGGMM-based method. The evaluation is done by employing two synthetic datasets that we have constructed. The first one represents a mixture of two bounded generalized Gaussian distributions (BGGD) and each mixture contains 3000 vectors in each cluster. The second dataset represents a mixture of three BGGD containing also 3000 vectors in each component. Our main focus here is to study the BGGMM's performance. Both real and estimated parameters found using the BGGMM are given in Tables 1 and 2. Based on these tables, we find that the estimated values for different parameters are very close to the real ones. For example, the real and estimated values for the first cluster using the synthetic dataset1 are $(\mu = 4, \sigma = 0.1, \lambda = 2)$ and $(\widehat{\mu} = 3.9, \widehat{\sigma} = 0.08, \widehat{\lambda} = 2.004)$ respectively. This experiment shows that the BGGMM can accurately estimate the mixture parameters and therefore can be used with success for forgery detection problem.

4.2 Forgery detection

We apply our approach to the challenging problem of image tampering detection. Our experiments are based on two public data sets: MICC-F220 and MICC-F2000 [19].

The first dataset is the MICC-F220 which is composed by 220 images: 110 are forged images and 110 originals. These images comprise for example plants, artifacts, and animals. The second publicly available dataset named MICC-F2000 is composed of 2000 images of which 700 are tampered and 1300 are authentic. In both datasets, the forged images are obtained by inserting a rectangle patch (copy-paste operation) on the original authentic images after performing some attacks like translation, scaling, and rotation. Sample images from these data sets are given in Figure 3 and Figure 4. In our experiments, the computed SVM kernels are trained using 10-fold cross-validation. Moreover, different number of components are considered to identify the suitable value as illustrated in Figure 5.

Results and comparative study w.r.t other methods from the state of the art, which are performed on the MICC-F220 dataset, can be viewed in Table 3. Quantitative results are determined in term of accuracy, TPR (true positive rate) and FPR (false positive rate) measures when applying different kernels generated from bounded generalized Gaussian mixture model. The accuracy metric represents the percentage of correctly classified images into normal or forged classes compared to the total number of images in the dataset. The used metric is defined as:

$$\begin{aligned} TPR &= \frac{TP}{TP+FN} \\ FPR &= \frac{FP}{TN+FP} \\ Accuracy &= \frac{percentage\ of\ correctly\ classified\ images\ into\ normal\ or\ forged\ classes}{total\ number\ of\ images} \\ &= \frac{TP+TN}{TP+FP+TN+FN} \end{aligned} \tag{27}$$

where TP, FN, FP, TN denote the number of true positives, false negatives, false positives and true negatives, respectively. The objective of this study is to evaluate the implemented probabilistic kernels and to compare them w.r.t some conventional generative mixture models.

Table 1.
Real and estimated parameters of synthetic dataset 1 using the BGGMM.

Synthetic data	μ	σ	λ
X_1	4	0.1	2
X_2	2	0.5	1
Estimated data	$\widehat{\mu}$	$\widehat{\sigma}$	$\widehat{\lambda}$
X_1	3.9	0.08	2.004
X_2	1.92	0.44	1.92

Table 2.
Real and estimated parameters of synthetic dataset 2 using the BGGMM.

Synthetic data	μ	σ	λ
X_1	1	0.3	2
X_2	2	0.5	1
X_3	0.5	1	1.5
Estimated data	$\widehat{\mu}$	$\widehat{\sigma}$	$\widehat{\lambda}$
X_1	1.5	0.19	2.001
X_2	1.86	0.67	1.9
X_3	1.1	1.02	1.99

Accordingly, very encouraging results are obtained with our approach (see Table 3). Our proposed approach requires O(NK) operations for each iteration, where N represents the number of input images and K is the number of components in the mixture. Moreover, the complexity of training SVM is $O(N^3)$.

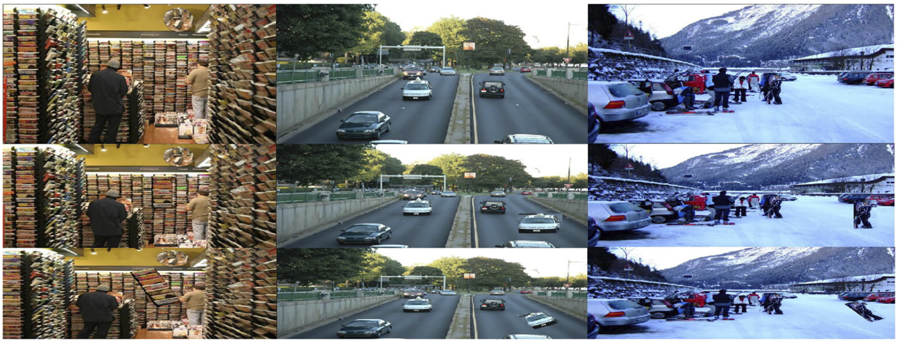

Figure 3. Samples images from MICC-F220. First row shows the original authentic examples. Second and third rows show tampered examples.

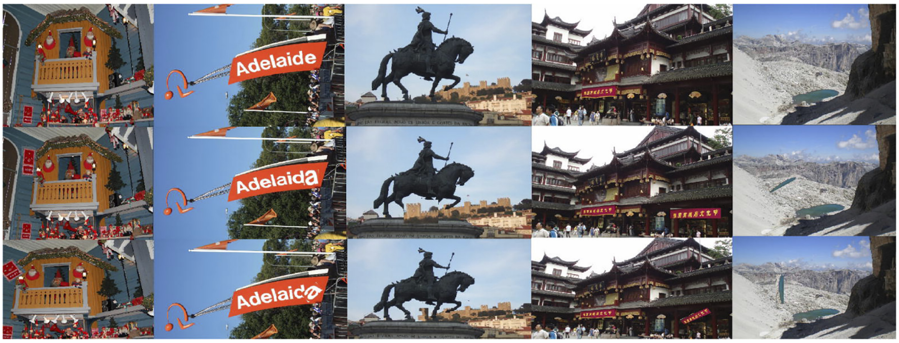

Figure 4. Samples images from MICC-F2000. First row shows the original authentic examples. Second and third rows show tampered examples.

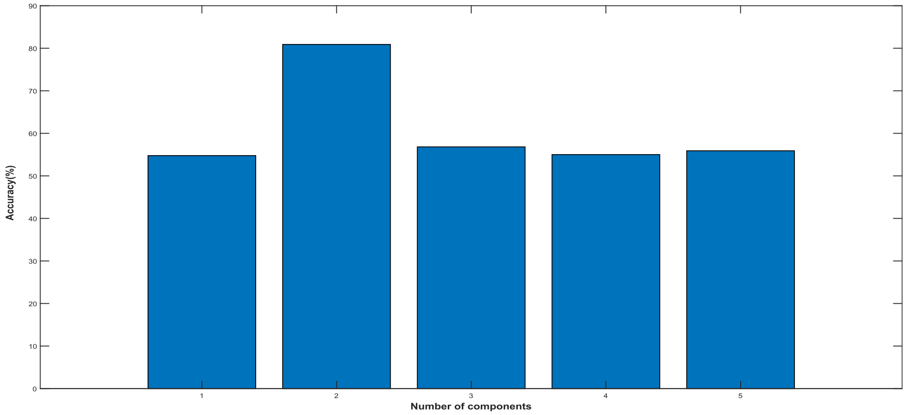

Figure 5. Accuracy rates using different number of components for MICC-F220 (Fisher kernel).

The first main deduction is that the proposed hybrid framework is able to increase the performance for all possible SVM kernels as compared to the conventional generative models such as Gaussian (GMM), generalized Gaussian (GGMM), and Bounded generalized Gaussian (BGGMM) models. In spite of the success of generative models – especially mixture models – for certain data classification problems, our current experiments have exposed the limits of generative models and indicated that hybrid models have shown substantial improvement in terms of detection accuracy. Therefore, there is an interest to develop hybrid approaches in order to yield better results. The second conclusion here is that the Fisher kernel generated from the bounded generalized Gaussian mixture model provides the best result. It bring great enhancement w.r.t other kernels in terms of accuracy which is well explained by the fact that this kernel is considered as an extension of the popular bag-of-visual-words (BOV) and might be calculated from much smaller vocabularies. It should also be noted that the best generative model that offers the best results is the bounded generalized Gaussian mixture model (BGGMM).

To further deepen our analysis of the developed approach, we apply it to another dataset: MICC-F2000. As in the previous experiment, the forgery detection is performed by using different methods as depicted in Table 4 and the best results are obtained for our developed hybrid method named BGGMM-fisher kernel (i.e while BGGMM is deployed with fisher kernel). It has the best accuracy with 81% than Gaussia, generalized Gaussian, Bounded GGMM, BGGMM-kulback-leibler, and BGGMM-Bhattacharyya kernel. In general, the proposed framework helps in obtaining good results for forgery detection as well illustrated in Figure 6 which summarizes the comparative study between different methods for both datasets MICC-F220 and MICC-F2000. According to this plot it is clear that proposed hybrid framework outperforms the generative statistical models for both datasets. This can be justified by the complexity of the datasets while the performance is improved using both discriminative and generative approaches.

Models	Accuracy(%)	TPR (%)	FPR (%)
Zernike [46]	–	20.91	6.36
GoDeep [9]	–	45.45	41.82
Zandi [22]	–	78.18	48.18
Li [47]	–	70.91	17.27
Cozzolino [48]	–	84.55	17.27
GMM	50.45	54.55	40.00
GGMM	53.64	64.09	36.36
BGGMM	55.45	58.33	45.94
BGGMM-Bhattacharyya kernel	57.65	58.99	40.96
BGGMM-kulback-leibler	60.19	63.76	52.20
BGGMM-fisher kernel	**80.90**	**85.42**	**17.85**

Table 3.
Accuracies (%) for forgery detection using different approaches for the dataset MICC-F220.

Models	Accuracy (%)
GMM	55.65
GGMM	55.80
BGGMM	56.00
BGGMM-kulback-leibler	57.30
BGGMM-Bhattacharyya kernel	67.86
BGGMM-fisher kernel	**81.00**

Table 4.
Accuracies (%) for forgery detection using different approaches for the dataset MICC-F2000.

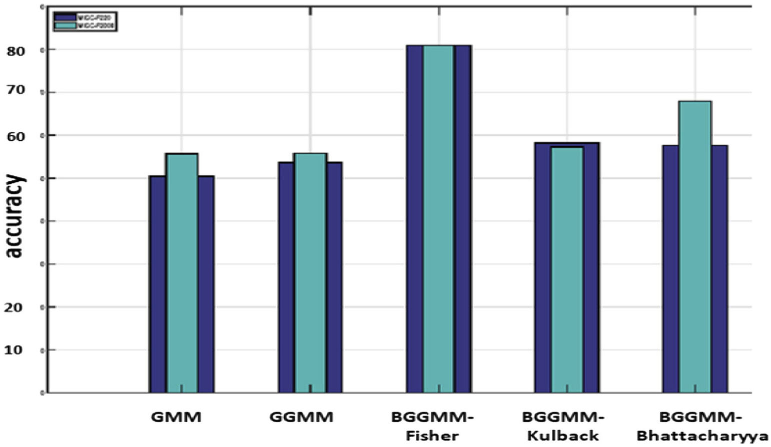

Figure 6. Comparative analysis of obtained results from different methods.

5. Conclusion

We have developed a novel hybrid statistical approach based on both bounded generalized Gaussian mixture model (BGGMM) and SVM kernels. Experiments have concerned a challenging application called image forgery detection. Our choice for BGGMM is motivated by the fact that bounded models have better modeling capabilities than conventional unbounded Gaussian-based models, have the advantage to fit data with different shapes and allowing to avoid under and over-fitting. Therefore, they are considered more suitable for data classification and in particular forgery detection. On the other hand, our solution involves the developing of new probabilistic support vector machines (SVMs) kernels from the BGGMM. Thus the developed learning framework has the advantage to combine properly the benefits of both discriminative and generative models.

According to the experiments we can conclude that the developed probabilistic kernels are helpful to achieve good performances and they outperform generative models (such as GMM, GGMM and BGGMM) for the current problem. Future works could be devoted to extending the current framework by integrating a feature selection mechanism able to take into account a weight for each feature. The purpose is to improve more the results. Moreover, it is interesting to investigate and to validate the proposed framework on other related applications such as multimedia segmentation and image databases summarization. Another possible future direction is to evaluate other relevant local and may be global visual features and descriptors to select the most suitable ones in order to improve the expected results. Finally, we plan to consider other interesting bench marked datasets such as (FRITH) [49] to evaluate both the current and further works.

References

[1] A. Almomani, M. Alauthman, F. AlBalas, O.M. Dorgham, A. Obeidat, An online intrusion detection system to cloud computing based on neucube algorithms, IJCAC 8 (2018) 96–112.

[2] H. Vahdat-Nejad, S.O. Eilaki, S. Izadpanah, Towards a better understanding of ubiquitous cloud computing, Int. J. Cloud Appl. Comput. 8 (2018) 1–20.

[3] O. Dorgham, A. Almomani, M. Alauthman, F. Albalas, A. Obeidat, An online intrusion detection system to cloud computing based on neucube algorithms, Int. J. Cloud Appl. Comput. 8 (2018) 96–112.

[4] A. Criminisi, P. Pérez, K. Toyama, Region filling and object removal by exemplar-based image inpainting, IEEE Trans. Image Processing 13 (2004) 1200–1212.

[5] J. Wu, Q. Ruan, Object removal by cross isophotes exemplar-based inpainting, in: 18th International Conference on Pattern Recognition, Hong Kong, China, 2006, pp. 810–813.

[6] A. Wong, J. Orchard, A nonlocal-means approach to exemplar-based inpainting, in: Proceedings of the International Conference on Image Processing, San Diego, California, USA, 2006, pp. 2600–2603.

[7] B. Marcelo, S. Guillermo, C. Vincent, B. Coloma, Image inpainting, in: Proceedings of the 27th Annual Conference on Computer Graphics and Interactive Techniques SIGGRAPH, 2000, pp. 417–424.

[8] G.K. Birajdar, V.H. Mankar, Digital image forgery detection using passive techniques: a survey, Digital Investigation 10 (2013) 226–245.

[9] E. Silva, T.J. de Carvalho, A. Ferreira, A. Rocha, Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes, J. Visual Commun. Image Represent. 29 (2015) 16–32.

[10] C. Lu, H.M. Liao, Structural digital signature for image authentication: an incidental distortion resistant scheme, IEEE Trans. Multimedia 5 (2003) 161–173.

[11] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting traces of resampling, IEEE Trans. Signal Processing 53 (2005) 758–767.

[12] C.S. Prakash, A. Kumar, S. Maheshkar, V. Maheshkar, An integrated method of copy-move and splicing for image forgery detection, Multimedia Tools Appl. 77 (2018) 26939–26963.

[13] H. Wang, H. Wang, X. Sun, Q. Qian, A passive authentication scheme for copy-move forgery based on package clustering algorithm, Multimedia Tools Appl. 76 (2017) 12627–12644.

[14] A.J. Fridrich, B.D. Soukal, A.J. Lukas, Detection of copy-move forgery in digital images, in: Proceedings of Digital Forensic Research Workshop, 2003.

[15] G. Li, Q. Wu, D. Tu, S. Sun, A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. in: Proceedings of the 2007 IEEE International Conference on Multimedia and Expo, ICME 2007, July 2–5, 2007, Beijing, China, pp. 1750–1753.

[16] S. Ryu, M. Lee, H. Lee, Detection of copy-rotate-move forgery using zernike moments, in: Information Hiding - 12th International Conference, IH 2010, Calgary, AB, Canada, June 28–30, 2010, Revised Selected Papers, pp. 51–65.

[17] M.K. Johnson, H. Farid, Exposing digital forgeries in complex lighting environments, IEEE Trans. Inf. Forensics Security 2 (2007) 450–461.

[18] J. Lukás, J.J. Fridrich, M. Goljan, Digital camera identification from sensor pattern noise, IEEE Trans. Information Forensics Security 1 (2006) 205–214.

[19] I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo, G. Serra, A sift-based forensic method for copy-move attack detection and transformation recovery, IEEE Trans. Inf. Forensics Security 6 (2011) 1099–1110.

[20] X. Pan, S. Lyu, Region duplication detection using image feature matching, IEEE Trans. Inf. Forensics Security 5 (2010) 857–867.

[21] S. Bourouis, M.A. Mashrgy, N. Bouguila, Bayesian learning of finite generalized inverted dirichlet mixtures: application to object classification and forgery detection, Expert Syst. Appl. 41 (2014) 2329–2336.

[22] M. Zandi, A.M. Aznaveh, A. Talebpour, Iterative copy-move forgery detection based on a new interest point detector, IEEE Trans. Inf. Forensics Security 11 (2016) 2499–2512.

[23] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Trans. Inf. Forensics Security 10 (2015) 507–518.

[24] C. Pun, X. Yuan, X. Bi, Image forgery detection using adaptive oversegmentation and feature point matching, IEEE Trans. Inf. Forensics Security 10 (2015) 1705–1716.

[25] G. McLachlan, D. Peel, Finite mixture models, Wiley and Sons, New York, 2000.

[26] I. Channoufi, S. Bourouis, N. Bouguila, K. Hamrouni, A flexible statistical model for image denoising, in: Image Analysis and Recognition – 15th International Conference, ICIAR 2018, Póvoa de Varzim, Portugal, June 27–29, 2018, Proceedings, pp. 30–38.

[27] F. Najar, S. Bourouis, N. Bouguila, S. Belghith, A fixed-point estimation algorithm for learning the multivariate GGMM: application to human action recognition, in: 2018 IEEE Canadian Conference on Electrical & Computer Engineering, CCECE 2018, Quebec, QC, Canada, May 13–16, 2018, pp. 1–4.

[28] I. Channoufi, S. Bourouis, N. Bouguila, K. Hamrouni, Color image segmentation with bounded generalized gaussian mixture model and feature selection, in: 4th International Conference on Advanced Technologies for Signal and Image Processing, ATSIP 2018, Sousse, Tunisia, March, 2018, pp. 21–24, pp. 1–6.

[29] F. Najar, S. Bourouis, A. Zaguia, N. Bouguila, S. Belghith, Unsupervised human action categorization using a riemannian averaged fixed-point learning of multivariate GGMM, in: Image Analysis and Recognition – 15th International Conference, ICIAR 2018, Póvoa de Varzim, Portugal, June 27–29, 2018, Proceedings, pp. 408–415.

[30] S. Bourouis, F.R. Al-Osaimi, N. Bouguila, H. Sallay, F.M. Aldosari, M.A. Mashrgy, Bayesian inference by reversible jump MCMC for clustering based on finite generalized inverted dirichlet mixtures, Soft Comput. 23 (2019) 5799–5813.

[31] T.M. Nguyen, Q.J. Wu, H. Zhang, Bounded generalized gaussian mixture model, Pattern Recogn. 47 (2014) 3132–3142.

[32] I. Channoufi, S. Bourouis, N. Bouguila, K. Hamrouni, Spatially constrained mixture model with feature selection for image and video segmentation, in: Image and Signal Processing – 8th International Conference, ICISP 2018, Cherbourg, France, July 2–4, 2018, Proceedings, pp. 36–44.

[33] V.N. Vapnik, V. Vapnik, Statistical learning theory, vol. 1, Wiley, New York, 1998.

[34] C.M. Bishop, Pattern recognition and machine learning, Springer, 2006.

[35] H. Sallay, S. Bourouis, Intrusion detection alert management for high-speed networks: current researches and applications, Security Commun. Networks 8 (2015) 4362–4372.

[36] V. Vapnik, The nature of statistical learning theory, Springer Science & Business Media (2013).

[37] T.S. Jaakkola, D. Haussler, Exploiting generative models in discriminative classifiers, in: Advances in Neural Information Processing Systems 11, [NIPS Conference, Denver, Colorado, USA, November 30 – December 5, 1998], pp. 487–493.

[38] P.J. Moreno, P.P. Ho, N. Vasconcelos, A kullback-leibler divergence based kernel for svm classification in multimedia applications, in: Advances in neural information processing systems, 2004, pp. 1385–1392.

[39] C.H. You, K. Lee, H. Li, GMM-SVM kernel with a bhattacharyya-based distance for speaker recognition, IEEE Trans. Audio Speech Language Process. 18 (2010) 1300–1312.

[40] X. Yang, S.M. Krishnan, Image segmentation using finite mixtures and spatial information, Image Vision Comput. 22 (2004) 735–745.

[41] M.S. Allili, N. Bouguila, D. Ziou, Finite general gaussian mixture modeling and application to image and video foreground segmentation, J. Electronic Imaging 17 (2008) 013005.

[42] H. Bay, A. Ess, T. Tuytelaars, L.V. Gool, Speeded-up robust features (surf), Comput. Vis. Image Underst. 110 (2008) 346–359.

[43] N. Bouguila, Deriving kernels from generalized dirichlet mixture models and applications, Inf. Process. Manage. 49 (2013) 123–137.

[44] A.B. Chan, N. Vasconcelos, P.J. Moreno, A family of probabilistic kernels based on information divergence, Univ. California, San Diego, CA, Tech. Rep. SVCL-TR-2004-1, 2004.

[45] T. Jebara, R. Kondor, Bhattacharyya and expected likelihood kernels, in: Learning Theory and Kernel Machines: in Proc. of the 16th Annual Conference on Learning Theory (COLT), Springer, 2003, pp. 57–71.

[46] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, An evaluation of popular copy-move forgery detection approaches, IEEE Trans. Inf. Forensics Security 7 (2012) 1841–1854.

[47] Y. Li, J. Zhou, A. Cheng, X. Liu, Y.Y. Tang, SIFT keypoint removal and injection via convex relaxation, IEEE Trans. Inf. Forensics Security 11 (2016) 1722–1735.

[48] D. Cozzolino, G. Poggi, L. Verdoliva, Efficient dense-field copy-move forgery detection, IEEE Trans. Inf. Forensics Security 10 (2015) 2284–2297.

[49] P. Rosin, FRITH Dataset, accessed December 1, 2019.

Corresponding author
Abdullah Alharbi can be contacted at: amharbi@tu.edu.sa