Wireless Pers Commun (2018) 101:1983–2008
https://doi.org/10.1007/s11277-018-5802-6

An Efficient Image Forgery Detection Using Biorthogonal Wavelet Transform and Improved Relevance Vector Machine

Neelesh Kumar Jain[1] · **Neeraj Kumar Rathore**[1] · **Amit Mishra**[2]

Published online: 10 May 2018

Abstract Nowadays, the development of refined image processing and software editing tools has finish the exploitation of digital images easily and invisible the image to the normal eyes and this process known as image fakery. Image security is one of the key issues in any field that makes use of digital images. Copy-move forgery (CMF) is the most effective and simple scheme to create forged digital images. In general, the methodologies based on Scale Invariant Feature Transform (SIFT) are widely used to detect CMF. Unfortunately, the detection performance of all SIFT based CMF detection approaches are extremely dependent on the selection of feature vectors. The values of these parameters are often determined through experience or some experiments on a number of forgery images. However, these experience parameter values are not applicable to every image thereby offers a limited usefulness. This paper deals the CMF problem using improved Relevance Vector Machine technique. The key idea of the IVRM is to apply Biorthogonal Wavelet Transform based scheme on image for feature extraction. The feature vectors are then stored lexicographically and similarity of vectors is decided using Minkowski distance and threshold value. The simulation results of proposed technique show a significant improvement in accuracy, sensitivity, and specificity rates over others existing schemes.

Keywords Image forgery · Copy-move forgery (CMF) · Biorthogonal Wavelet Transform (BWT) · Minkowski distance · Improved Relevance Vector Machine (IRVM) · Glowworm Swarm Optimization (GSO) · Similarity measure

✉ Neeraj Kumar Rathore
neerajrathore37@gmail.com

Neelesh Kumar Jain
neeleash.jain@juet.ac.in

Amit Mishra
amitutk@gmail.com

[1] Jaypee University of Engineering and Technology, Guna, M.P., India

[2] Thapar University, Patiala, Punjab, India

1 Introduction

Nowadays, in digital publishing and printing fields, image forgery is considered as a major issue. Accepting the legitimacy of pictures is kind of tough as most of the digitally printed images are forged before publication. For example in political rallies typically numbers of listeners are digitally modified to point out several attendees. Thus image forensic with forger detection has become a serious challenge. Image conferred as digital evidence can be forged and thus is hard for being considered as valid. There are some previous works in the direction that depends upon detection copy paste forgery only. Image forgery is that the approach of modification the imaging data from the pictures using image-processing software packages like Photoshop, alternative image editor tools. It's also strategies for manipulating the initial data by using varied transformation techniques like addition of noise, scaling, blurring, resizing and rotation, adding and removing any object and applying numerous alternative types of manipulation for hiding the real information within the image to produce a digital image as evidence proof for any criminal case, there's a demand of the identification of the genuineness of the image. Image tampering will be divided into as a copy move forgery and as a non copy move forgery. During a copy move forgery, some portion of the image is derived and further in any other place of the image so that there are no modifications like resizing, blurring etc.

Altering digital pictures via intuitive software is an operation of simpleness with terribly low cost in today's image forgery. Therefore each individual will synthesize a pretend image. For the wide accessible web, the false data disseminates extremely quick. As a consequence, the facts are also distorted and the public opinion is also affected, yielding negative social influence. It will be even worse within the justice once pictures are conferred as proof. Therefore, there's a strong demand need for valid and robust authentication methodology to distinguish whether or not an image is original or not.

Generally, two schemes are used to form a forgery like 1. Copy-Move technique and 2. Splicing Scheme. Within the former case, a region of an image is duplicated then glued onto alternative regions to hide any unwanted portion inside an equivalent picture [1]. Within the latter case, tampered image consists of 2 sources and retains the majority of one image for detail [1]. Earlier, some scientists and researchers have introduced several strategies [2] to reveal such meant manipulations. Passive forensic methods fulfill the task without extra data aside from the image itself, therefore showing benefits over active algorithms like watermarking and alternative signature schemas. Therefore, most analysis work is absorbed in developing blind authentication strategies.

The forged image leaves some clues which may be wont to find the manipulated regions. In that situation, copy-move operation is followed due to the pasted space, although it may probably be altered geometrically, shares some similar features with the original region that is duplicated; finding out analogous features abstracted from local area is a potential solution. SIFT feature may be used to find clone areas [3, 4]. For splicing tampered image detection, considering that there are some discrepancies between the host image and also the spliced region makes an attempt to search out the distinction to reveal that forgeries make sense. The proposed scheme goal is to automatically observe copy-move within a single method without any earlier information concerning the forgery type of the uncertain image. In this paper, IRVM based forgery detection has been proposed with Biorthogonal Wavelet Transform based Singular Value Decomposition (BWT-SVD). Initially, the input color image has been converted into grey scale. After that, BWT is used to reduce noise and extract the feature. Then, the, the feature vectors are sorted in lexicographically and the duplicate vectors are identified by similarity between two successive

vectors. To decide the similarity of vectors, Minkowski distance and Threshold value is used. Finally, the Improved RVM has been carried out with GSO algorithm to detect the forgery and classified as authentic image and forged image. Experimental results show the effectiveness of the proposed work in terms of accuracy, sensitivity, specificity, precision, recall, f-measure and g-mean compared than existing SVM forgery detection method. The remainder sections of this paper are organized as: copy-move image forgery detection based existing scheme has been reviewed in Sect. 2, Sect. 3 explained the proposed methodology, Sect. 4 shows the evaluation results and Sect. 5 concludes this work and provides future enhancement.

2 Related Work

In this section, copy-move image forgery detection based existing scheme has been reviewed. In 2016, Chauhana et al. [5] surveyed on key-point based forgery detection schemes on the basis of various parameters. Various copy move detection methods has been studied and concluded that the Scale Invariant Feature Transform (SIFT) was efficient scheme and it was detected forgery within a single or multiple regions of an image. The SIFT results demonstrate that it was effective for both geometric transformation and plain copy-move forgery. The geometric transformation functions are rotation, scaling and transformation. It has high computation efficient, But, low accuracy.

In 2016, Malviya et al. [6] presented efficient feature extraction based copy move detection for forgery detection. Three types of feature extraction algorithm have been introduced like color moment, HSV histogram, and auto color Correlogram for forgery detection. The simulation results show that the proposed feature extractions have been accurately detected the forged region and effective in some attacks like rotation and scaling. But, it has computation time complexity.

In 2016, Al-Qershi et al. [7] proposed a k-means clustering based new matching scheme for reduced the detection time and increased the detection accuracy. Initially, the image blocks are clustered and then Locality Sensitive Hashing (LSH) was used for matched the blocks based Zernike moments. The simulation results demonstrate that the proposed scheme reduced the 10% of processing rime and enhanced detection accuracy.

In 2016, Ustubioglu et al. [8] proposed a copy-move forgery detection method that can calculate threshold automatically. To limit the range of the feature vector elements, the Discrete Cosine Transform (DCT) has been introduced. Also, to establish the compression history of the image under test, Benford's generalized law has been used. Element-by-element equality was introduced between the feature vectors for find similarity between blocks. It uses compression history to establish the threshold value for the current test image automatically. The simulation results show that the proposed scheme was very efficient to detect copied regions under various scenarios and attained high accuracy. It's not suitable for real time data.

In 2015, Kaushik et al. [9] presented a statistical moments and 2D-Discrete Cosine Transform (DCT) based approach for detecting copy-move forgery in digital images. First, slide a window centered on every pixel of the suspicious image, and then to attain the quantized coefficient matrix, each window was passed through 2D–DCT. Obtained the low dimensional statistical feature vector of each quantized coefficient matrix and then arranged in a feature matrix. Four types were extracted in this scheme. After that, the adjacent pairs of feature vectors are used for detect the copy-move forgery. The simulation

results show that this scheme attained low computational complexity and lower dimension feature vector. But, the system reliability was not good.

In 2015, Isaac et al. [10] proposed a Support Vector Machine (SVM) based image forgery detection scheme for copy-move forgery detection by taking texture information of the image. The texture information was extracted by using Gabor wavelets (GW) and Local Phase Quantization (LPQ). These extracted features are transferred to SVM as an input and it classifies the forgery image and non-forgery image. The simulation results show that this scheme attained high accuracy on both CASIA v1 and the DVMM color dataset. But, the SVM training time was high.

In 2015, Pun et al. [11] presented feature point matching and adaptive over-segmentation based approach for detecting copy-move forgery detection. It has been used both keypoint-based forgery and block-based detection methods. Initially, the input image was segmented irregular blocks and non-overlapping adaptively. After that, extracted the feature points from each block, and then extracted features are matched between one another to locate the labeled feature points. The simulation results show that this scheme attained much better detection results under various scenarios compared than existing scheme. But, it has computational complexity.

In 2015, Ardizzone et al. [12] presented a hybrid of block and point based scheme for detection of copy-move forgery. Initially, extracted the Interest points from image and modeled the objects as a set of attached triangles built onto these points. After that, according to content color information, shapes inner angles and local feature the triangles are matched and compared with point based scheme. As well as the keypoint based approaches used to hide object in a scene. The simulation results show that this hybrid scheme attained better performance compared than existing algorithms. The accuracy and system reliability was not good.

In 2014, Anand et al. [13] presented a comparative study based on three copy-move detection methods such as Dyadic Wavelet Transform (DyWT), discrete wavelet Transform (DWT) and DyWT with SIFT.DyWT (b).DWT and SIFT (c). DyWT and SIFT. The DWT couldn't shift variant but DyWT can be done, therefore DyWT was attained more accurate detection result in analysis of data. To extract more numbers of key points, the DyWT was combined with SIFT and produced more accurate results. The simulation results show that this scheme attained high accuracy compared than other scheme. It has high computation cost and time complexity.

In 2013, Amerini et al. [14] proposed a J-Linkage algorithm based new scheme for localization detection of copy-move forgery. In the space of the geometric transformation, the clustering has been done and it increased the accuracy, reliability and precision of the system. The experimental result shows that it has high performance compared than other algorithms. It has computational complexity. In 2013, Hashmi et al. [15] proposed a hybrid approach based on DWT and SIFT for detection of copy-move image forgery. The experimental results show that it attained good results and has high reliability. But, the system accuracy was not good. In 2013, Al-Qershi et al. [16] presented a survey of passive detection of copy-move forgery in digital images. It has discussed various detection methods and provides key idea for developing robust passive detection scheme for copy-move forgery.

In 2012, Christlein, et al. [17] compared and evaluated the various features results for copy-move detection. Here, 15 most prominent feature sets are examined and analyzed the detection performance on a per-pixel basis and on a per-image basis. The simulation results demonstrate that the keypoint-based features are sensitive to repetitive image content and

low-contrast regions and block-based methods only improved the detection results. It has computational time complexity.

In 2011, Amerini et al. [18] proposed Scale Invariant Features Transform (SIFT) based novel methodology for forgery detection. This method was identified if copy-move attacks has occurred as well as perform cloning to recover the geometric transformation. The simulation results show that this scheme attained high reliability. It has high computation cost and time complexity.

In 2011, Muhammad et al. [19] proposed a dyadic DyWT based blind and robust technique for forgery detection. This scheme has good results compared than DWT. Initially, the input image was decomposed into approximation and detail subbands. After that, these subbands are splitting into overlapping blocks and measure the similarity between blocks. The similarity between the copied and moved blocks are measured by using thresholding, and then matched pair's obtained from the sorted list as copied and moved blocks. The simulation results show that this scheme attained high reliability and high accuracy. It has high computation cost and time complexity.

3 Proposed Methodology

In this section, the proposed IRVM based Copy-Move Forgery Detection (CMFD) algorithm has been discussed. In the field of digital image forensics, the CMFD is one of the emerging problems [20–23]. Earlier, to address this problem, many techniques have been proposed. These methods can be able to identify the duplicated image regions, but the image was affected by the common image processing operations like noise addition, compression and rotation. So, it's considered as a one of the main issues of these techniques as well as the computational time was considered as another challenge, which attained high time when considering the large databases. So, to solve the above problems, the efficient feature extraction and classification scheme have been introduced in this system. The step by step procedure of proposed scheme has been discussed in given below sub sections.

3.1 System Overview

The proposed system accumulates various processes to implement. The Fig. 1 shows the overall architecture of proposed Copy-Move Forgery Detection (CMFD) using IRVM with BWT-SVD.

It illustrates the phases of proposed scheme such as preprocess, feature extraction and detection. Initially, if the input image is color, then it converted to grey image and this converted into various overlapping sub-blocks of fixed sizes. At that point, the BWT is used to every block and extracted a feature vector having unique singular values for every image sub-block. Utilizing these feature vectors, they discovered the blocks which are matching Minkowski distance and Threshold value [24–30]. They utilized a threshold value in order to increase the sturdiness and as well wipe out pseudo matching. Finally, the IRVM used for detection of forgery and classification of images like authentic image and forged image. In IRVM, the RVM parameters are optimized by Glowworm Swarm Optimization (GSO) to improve the prediction accuracy.

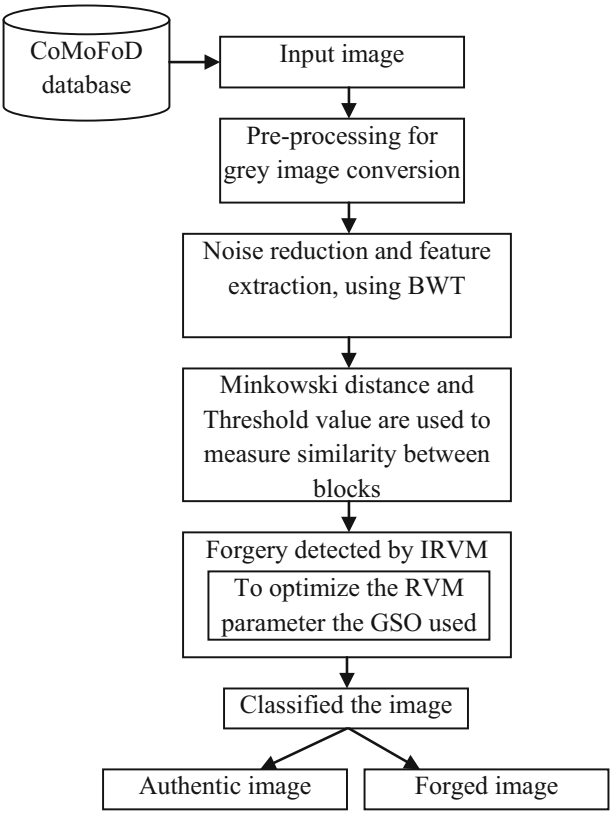

Fig. 1 Overall architecture of proposed CMFD using IRVM with BWT

3.1.1 Symbols Used in Proposed System

Mathematical model of proposed system have various symbolic notations. Table 1 depicted all symbols used in proposed system with their meaning.

3.2 Noise Reduction and Feature Extraction

The input dataset has been downloaded from website. So, it contains some unwanted data's and some noises. To reduce the noise and remove unwanted data, as well as, efficient feature extraction [31–36], the proposed system has been used BWT.

3.2.1 Biorthogonal Wavelet Transform (BWT)

To improve the image quality and extract the features from images like variance, mean, skewness, energy etc. generally, in BWT, biorthogonal filters are developed for providing symmetric property instead of using two filters. In this proposed scheme, The BWT is used to denoising the image and extract [37–39] the features and it has the property of linear phase. To solve the problem of phase distortion the BWT is designed and it contains spline wavelets [40]. Here, Finite Impulse Response filters are used to reconstruct the image.

Table 1 Symbols used in proposed system

Symbol	Meaning	Symbol	Meaning
I1(x, y), $I2(x, y)$	Input images	μ	Fusion rule
U and V	Orthogonal matrices	A	Real matrix
S	Singular values of A	r	The rank of matrix A
$\{F_i, t_i\}_{i=1}^{n}$	Training inputs	n	Number of features
$\hat{F}$	New input features	K	Kernel function vector of $k(\hat{F}) = \left[k(F_1, \hat{F}) \ldots k(F_n, \hat{F})\right]^T$
w	Weight vector of $(\omega_1 \ldots)^T$	α_i	Hyper parameter
$\sigma(.)$	Logistic sigmoid function	r^2	Scale factor
ω_i	Weight Parameter	σ_i^2	Variance
F and z	D-dimension feature vectors	ρ	Luciferin decay constant
$j_i(t)$-	Objective function value at glowworm *i*' s location	$p_j(t)$	Probability of glowworms
t	Time	$l_i(t)$	Luciferin value of glowworm*i*
γ	Luciferin enhancement constant	$\hat{F}$	New input features
$d(i, j)$	Euclidian distance between glowworms i and j	$r_d^i(t+1)$	Local-decision domain of glowworm i at the t + 1 iteration
s	Step-size	β.	Constant parameter
n_t	Threshold	$d(m, n)$	Distance
m and n	n-Dimensional singular value feature vector of blocks b_i and b_j	F_p	False positive rate of images
T_p	True positive rate of images	T_n	True negative of images
F_n	False negative rate of images	Sen	Sensitivity
Spc	Specificity	Acc	Accuracy
p	Precision	r	Recall
PPV	Positive predictive value	NPV	Negative predictive value
FPR	False positive rate	FNR	False negative rate

Wavelet transform fusion is predicted via considering the wavelet transforms *wt* of two registered input images I1(x, y) and $I2(x, y)$ with μ-fusion rule. The fused image reconstruction is defined as

$$\mathrm{I(x,y)} = \mathrm{w} - 1(\mu(\mathrm{wt(I1(x,y))}, \quad \mathrm{wt(I2(x,y))})) \tag{1}$$

After that, the fused image is passed by bilateral filter. It defined as a non-linear, smoothing filter, edge preserving and adaptive histogram equalization. To enhance the contrast in the image, this filter is used and produced a good quality [41–44]. The final fused image is splitting into overlapping blocks.

3.2.2 Singular Value Decomposition (SVD)

SVD can preserve the useful features of the original image and use less storage space of memory [45]. In SVD, each singular value indicates the luminance of an image layer while the corresponding pair of singular vectors denotes the geometry of the image. In SVD, every real matrix A can be decomposed into a product of 3 matrices defined as:

$$A = USV^T \tag{2}$$

where U *and* $V \rightarrow$ orthogonal matrices, $U^TU = I$, $V^TV = I$, and $S = diag(\lambda_1, \lambda_2, \ldots \lambda_r)$ [45]. The diagonal entries of S are defined as the singular values of A, the right singular vectors of A is defined as the columns of V, and the columns of U are defined the left singular vectors of A. This decomposition is called as the Singular Value Decomposition (SVD) of A, and it defined as

$$A = \lambda_1 U_1 V_1^T, \lambda_2 U_2 V_2^T, \ldots \lambda_r U_r V_r^T \tag{3}$$

where $r \rightarrow$ the rank of matrix A.

3.3 Image Forgery Detection and Classification Using Improved Relevance Vector Machine (IRVM)

Generally, RVM [46] has been used for decision making purpose. In this proposed system, it is used for forgery detection and classification process. In RVM, the weight parameter is optimized by using Glowworm Swarm Optimization, and it will improve the RVM performance. Therefore, this combined algorithm named as Improved RVM (i.e. IRVM). The extracted features are given as input in RVM training process. The training inputs denoted as $\{F_i, t_i\}_{i=1}^n$, $F_i \in R^n, t_i \in \{0, 1\}$ and n-defines the number of features. For new inputs $\hat{F}$, RVM makes prediction based on SVM function. RVM takes a linear combination of basic kernel functions remodeled by a logistic sigmoid function

$$y(\hat{F}, w) = \sigma\left(\sum_{i=1}^{n} \omega_i k(F_i, \hat{F})\right) = \sigma(w^T K) \tag{4}$$

where K is defined as the kernel function vector of $k(\hat{F}) = \left[k(F_1, \hat{F}) \ldots k(F_n, \hat{F})\right]^T$, w indicates the weight vector of $(\omega_1 \ldots \omega_n)^T$, and $\sigma(.)$ represented logistic sigmoid function and is given below (Eq. 5),

$$\sigma(a) = \frac{1}{1 + \exp(-a)} \tag{5}$$

The logistic sigmoid function satisfies the symmetry property and is given below

$$\sigma(-a) = 1 - \sigma(a) \tag{6}$$

So, RVM can be used as the posterior probability. For the input feature $\hat{F}$, the posterior probability of class c_1 can be defined as

$$p(t = 1|\hat{F}) = y(\hat{F}, w) \tag{7}$$

Correspondingly, the posterior probability of class c_2 can be defined as

$$p(t = 0|\hat{F}) = 1 - y(\hat{F}, w) \tag{8}$$

RVM can be treated as the posterior probability, because, to train the model, it can be adopts a Bayesian probabilistic framework. Also, it using the key feature of Automatic Relevance Determination (ARD) prior over the weight vector w, which is used to separated the hyper parameter α_i for each weight ω_i parameter. During the deduction process, a lot of

the hyper parameters are driven to large values, therefore that equivalent weights are efficiently forced to zero. Accordingly, the corresponding kernel functions can be pruned out in a sparse model result [47–50]. The inputs F_i equivalent to the remaining nonzero weights are known as relevance vectors.

The RVM decision model for an input vector $\hat{F}$, based on the w_{MP} and RVS vectors Eq. (4) can be rewritten as

$$y\left(\hat{F}, w_{MP}\right) = \sigma\left(\sum_{F_i \in RVS} \omega_i k\left(F_i, \hat{F}\right) + \omega_0\right) \tag{9}$$

In the RVM decision model, kernel function plays a significant role. In this improved RVM, the Elliptical Radial Basis Function (ERBF) can be used for kernel function.

$$(F, z) = exp\left(-\sum_{i=1}^{D} (F_i - z_i)^2 / \left(\sigma_i^2 . r^2\right)\right) \tag{10}$$

where $x = (x_1, \ldots, x_D)^T$ and $z(z_1, \ldots, z_D)^T)$ are defined as the D-dimension feature vectors, r represented as scale factor and σ_i^2 defined variance. To improve the detection accuracy, the hyper parameter of weight can be optimized by Glowworm Swarm Optimization (GSO) approach.

3.3.1 Glowworm Swarm Optimization (GSO)

The GSO [51] is a swarm intelligence based optimization algorithm [52–55]. It is works based on the behavior of glowworm. Basically, it has four steps like deployment, luciferin-update, movement and local-decision domain update. In deployment step, to allow the glowworms to be scattered in the entire objective space as well as each and every glowworm contain identical quantity and sensor range of luciferin. In luciferin-update step, according to the objective function, glowworm changes luciferin location value and the luciferin update rule is defined as

$$l_i(t+1) = (1-\rho) l_i(t) + \gamma j_i(t+1) \tag{11}$$

where $\rho(0 < \rho < 1)$ is defined as the luciferin decay constant, $j_i(t)$ indicates the objective function value at glowworm i' s location at time t and γ is represented as the luciferin enhancement constant.

In Movement step, each and every glowworm chooses a neighbor, which has higher luciferin value and then using a probabilistic mechanism moves toward it. The probability of glowworms $p_j(t)$ moving towards a neighbor nb is based on the Eq. (11) at iteration t

$$p_j(t) = \frac{\left(l_j(t) - l_i(t)\right)}{\sum_{k \epsilon n_i(T)} (l_k(t) - l_i(t))} \tag{12}$$

where $l_i(t)$ defined as the luciferin value of glowworm i, $d(i, j)$ represents the Euclidian distance between glowworms i and j. The glowworms i movement is defined as

$$F_i(t+1) = F_i(t) + s\left(\frac{F_j(t) - F_i(t)}{\left\|F_j(t) - Fx_i(t)\right\|}\right) \tag{13}$$

where s is indicates the step-size. F-is the input of glowworm.

In Local-decision domain update step, if the number of neighbor modifies, then at each of iteration, local-decision domain needs updating and is defined as

$$r_d^i(t+1) = min\{r_s, max\{0, r_d^i(t) + \beta(n_t - |N_i(t)|)\}\} \tag{14}$$

where $r_d^i(t+1)$ is indicates the local-decision domain of glowworm i at the t + 1 iteration, β is represent a constant parameter and changes the rate of alter of the neighbor domain, n_t is indicates a threshold and is used to manage the number of neighbors. Based on these four steps, the fitness value has been estimated. Based on these steps, the hyper parameter of optimized [35–39] weight value has been predicted and is used in RVM and improved the forgery detection accuracy. Pseudo-code of the IRVM is given in Algorithm 1.

Algorithm 1:Improved Relevance Vector Machine(IRVM)
Input: $S = \{F_i, t_i\}_{i=1}^n$ defined as training data set, the number of the independent samples are represented as n, σ^2 represented as variance.
Output: $S' \subseteq S$: relevance vectors,
$y(F, \omega)$ represented as predicted Function
Condition for Termination: training samples are all trained.
Start
hyper parameters α_i and σ^2 for each weight ω_i are obtained according to Eq. (10) the marginal likelihood for hyper parameters α_i and σ^2
model weights are given by using GSO
initialization: all the parameters like n, l, r_o, s, n_i, ρ, β, γ, r_s, p, $T \in T$ $maximum$
while $(t \leq T)$ then do
{
For i=1 to n do
Eq. 11 process attained
For each i do
$$n_i(t) = \{j: ||F_j(t) - F_i(t)|| \leq r_d^i(t); l_i(t) \leq l_j(t)\}$$
For each $j \in n_i$ do
Eq. 12 -14 processes has been attained
optimal weight value has been predicted
t=t+1
display best result
}
display best weigh result and its given into Eq. (9)
For i = 1 to n
{
If $\omega_i \neq 0$ then
{
The corresponding point (F_i, t_i) is a relevance vector
}
i=i+1
}
predicted function $y(F, \omega)$ is computed according to Eq. (4)
Based on this the input images were tested and classified as authentic image and forgery image
End

The proposed IRVM based CMFD step by step process has been given below.

Copy-Move Forgery Detection (CMFD) Process:

The general process of a CMFD system consists of the following steps.

Step 1 Pre-processing—if the input image is a color image (RGB), it is converted to gray-scale image based on the RGB to gray-scale conversion technique. The gray scale image is then tiled into overlapping blocks of fixed size

Step 2 Feature Extraction—in this step, BWT is applied to each block in each node and the average value of each block is used as the feature vector for block comparison and matching

Step 3 Produce feature vectors from blocks

Step 4 Sort the feature vectors in lexicographically

Step 5 Find duplicated vectors—Image Block Similarity Matching—based on the singular value feature vectors obtained in step 5, the Euclidean distance measure is computed between each block in each node. The minimum d measure corresponds to maximum match. Let m and n corresponds to n-dimensional singular value feature vector of blocks b_i and b_j respectively,

$$m = (m_1, m_2, \ldots, m_n)^T \tag{15}$$

$$n = (n_1, n_2, \ldots, n_3)^T \tag{16}$$

$$sim = \left((m-n)^T(m-n)\right)^{(1/2)} = \sum_{i=1}^{k}(m_i - n_i)^2 \tag{17}$$

If d (m, n) is greater than a threshold parameter then, such block pairs are discarded as they non-matching. The remaining block pairs can be candidates of suspected blocks.

Step 6 Consider the block matching

Step 7 Detect the forgery and classified the image by using IRVM

The proposed system classifies CMFD algorithms in groups based on the variation of different techniques used in different steps.

- With and without transformations (Step 2).
- The main differences in algorithms are the way to create feature vectors which is from Step 1 to Step 3.
- The method to compare vectors and look for the block matching at Step 5 and Step 6, respectively.

The proposed IRVM detected forgery with high accuracy [21–26] due to the efficient optimization and effective feature extraction process. The performance is evaluated in Sect. 4.

4 Results and Discussion

In this section, the proposed IRVM based forgery detection performance has been evaluated and compared with existing SVM [10] and HMM-SVM [56]. At first, CoMoFoD database images are trained and then tested. In training process, 250 authentic images and 250 forged images are used for proposed IRVM model and the images are selected as randomly. In testing, the whole 500 images are divided into 5 sets of images and each set consists of 100 images. Each and every set is trained and tested with IRVM. The performance is evaluated in terms of sensitivity, F-measure, specificity, G-mean, precision and accuracy. The simulation results are evaluated by using MATLAB.

4.1 Input Database: CoMoFoD

CoMoFoD database [57] has 260 image sets, 200 images in small image category size of 512 × 512, and 60 images in large image category size of 3000 × 2000. In CoMoFoD database images, the given below transformations are applied to check the image quality.

- In translation, without performing any transformation, a copied region is only transformed to the new location,
- In rotation, rotated a copied region and transformed to the new location,
- In scaling, scaled a copied region and transformed to the new location,
- In distortion, distorted a copied region and transformed to the new location,
- In combination, applied a two or more transformation on a copied region before moving it to the new location.

In this proposed system, small image category (512 × 512) has been used for evaluation. It is downloading from http://www.vcl.fer.hr/comofod/download.html

4.2 Evolution Parameter for Measuring Forgery

In this paper, some appropriate measures are used to evaluate the performance of the IRVM based copy-move detection method. The measures [58] like sensitivity (i.e. *Sen*), specificity (i.e. *Spc*), accuracy (i.e. *Acc*) and precision (p), recall (r), f-measure and g-mean are used. The p and r are checked for varying block sizes. At the whole image level, let T_p indicates the value of true positive rate of images, F_p mentions the value of false positive rate of images, T_n indicates the value of true negative of images and F_n mentions the value of false negative rate of images. These measures are computed individually for every image and on average for the all test images

$$Sen = T_p/(T_p + F_n) \tag{18}$$

$$Spc = T_n/(T_n + F_p) \tag{19}$$

$$Acc = (T_p + T_n)/(T_p + F_n + T_n + F_p) \tag{20}$$

Precision (p) could be a measure for the likelihood that a detected forgery is really a forgery. It denotes the accuracy of the strategy.

$$p = T_p/(T_p + F_p) \tag{21}$$

Recall (r) is a measure for the probability that the forged image is detected. It denotes the completeness of the method.

$$r = T_p/(T_p + F_n) \tag{22}$$

F-Measure is calculated based on the given formula

$$F = 2 \cdot \frac{p.r}{p + r} \tag{23}$$

Positive Predictive Value (i.e. PPV) is calculated based on the given formula

$$PPV = T_p/\left(T_p + F_p\right) \tag{24}$$

Negative Predictive Value (i.e. NPV) is calculated based on the given formula

$$NPV = T_N/(T_N + F_N) \tag{25}$$

False Positive Rate (i.e. FPR) is calculated based on the given formula

$$FPR = 1 - specificity \tag{26}$$

False Negative Rate (i.e. FNR) is calculated based on the given formula

$$FNR = 1 - sensitivity \tag{27}$$

4.3 Training and Classification Procedure and Result

In CoMoFoD database, all Images is modeled through estimate the parameters of the images for IRVM. During training process, a set of images are used and it contains authentic and tampered images. Initially, the image is process and extracted the feature vectors. The features are given as input into IRVM. It processed the inputs based sigmoid kernel function and then selected the best weight values from GSO process. Based on this weight value the training values are predicted efficiently. Based on these training values, the test images are tested and classified as authentic image and forgery images. RVM is machine learning algorithms that use a high dimensional feature space and estimate differences among classes (i.e. authentic class and forgery class) of given data to generalize unseen data. In this system, 500 images are trained and tested. Figures 2 and 3 shows samples of authentic and forged images.

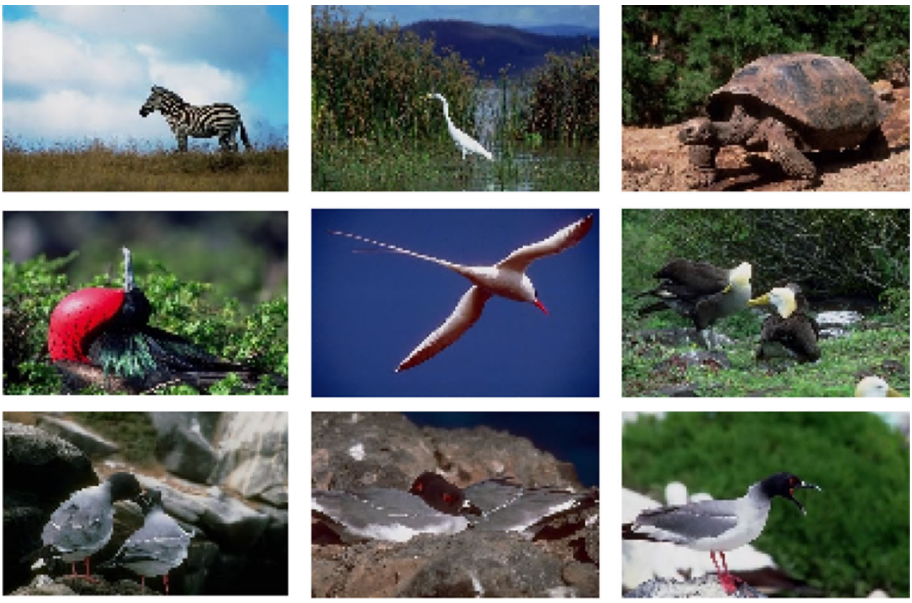

Fig. 2 Images used for testing and correctly detected as authentic

The proposed system performance is evaluated for all set of images (Set 1 to Set 5) and the numerical values are predicted in Table 2. It illustrates that, the number of images increases means the performance of proposed values also increases.

The set of images were tested and trained and their parameters values are predicted and their average values also predicted and is shown in Table 3, 4 and 5.

From the Table 3, 4 and 5 shows the evaluation of parameters numerical results for proposed IRVM and existing HMM + SVM and SVM methods. These tables illustrate the proposed IRVM attained best results compared than existing schemes due to efficient feature selection and efficient training process with optimized weights.

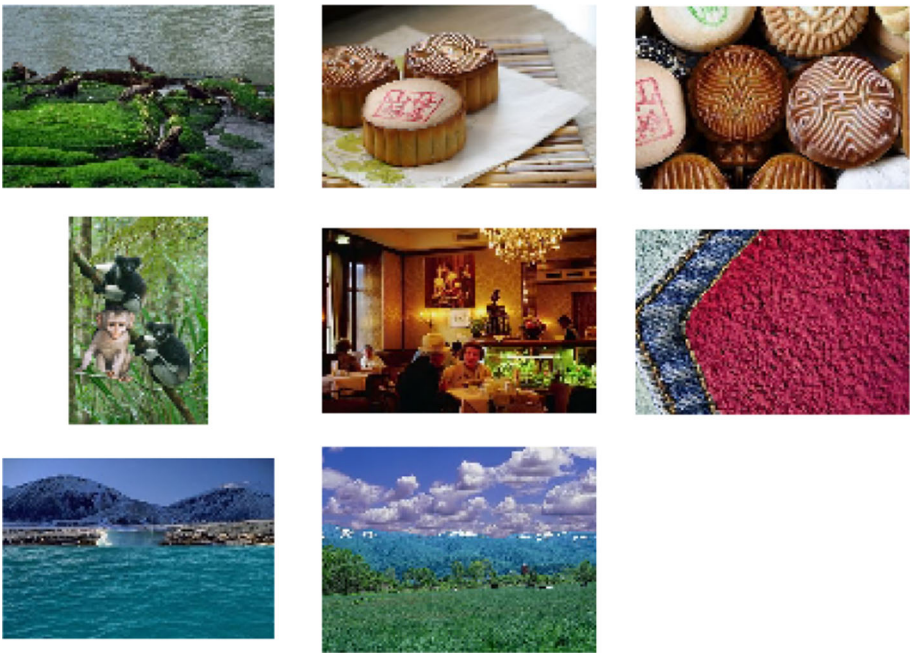

Fig. 3 Images used for testing and detected correctly as tampered

Table 2 Performance measures value for proposed method

Inputs	Sensitivity (%)	Specificity (%)	Accuracy (%)	F-measure (%)	G-mean (%)	Precision (%)	Recall (%)
Set-1	0.8400	1	0.9200	0.9130	0.9165	1	0.8400
Set-2	0.8400	1	0.9210	0.9130	0.9165	1	0.8400
Set-3	0.8600	1	0.9300	0.9247	0.9274	1	0.8600
Set-4	0.9400	0.9400	0.9400	0.9400	0.9400	0.9400	0.9400
Set-5	0.9400	0.9000	0.9000	0.9216	0.9198	0.9038	0.9400
Average	0.884	0.976	0.9222	0.9224	0.9231	0.968	0.884

Table 3 Evaluation of proposed method parameters numerical results

Input set	Number of authentic images	Number of forged images	T_p	T_n	F_p	F_n	Sensitivity (%)	Specificity (%)	Accuracy (%)	F-measure (%)	G-mean (%)
Set-1	50	50	42	50	0	8	0.8400	1	0.9200	0.9130	0.9165
Set-2	50	50	42	50	0	8	0.8400	1	0.9210	0.9130	0.9165
Set-3	50	50	43	50	0	7	0.8600	1	0.9300	0.9247	0.9274
Set-4	50	50	47	43	5	3	0.9400	0.9400	0.9400	0.9400	0.9400
Set-5	50	50	47	45	7	3	0.9400	0.9012	0.9000	0.9216	0.9198
Total	250	250	221	238	12	29	0.884	0.976	0.9222	0.9224	0.9231

Table 4 Evaluation of existing HMM + SVM method parameters numerical results

Input set	Number of authentic images	Number of forged images	T_p	T_n	F_p	F_n	Sensitivity (%)	Specificity (%)	Accuracy (%)	F-measure	G-mean
Set-1	50	50	44	42	9	7	0.8800	0.8403	0.86	0.868	0.8595
Set-2	50	50	43	45	6	7	0.8600	1	0.87	0.8865	0.8698
Set-3	50	50	47	45	3	3	0.9400	1	0.89	0.9145	0.9298
Set-4	50	50	44	43	7	5	0.9000	0.9400	0.93	0.9414	0.9889
Set-5	50	50	47	44	7	3	0.9200	0.9000	0.90	0.9254	0.8895
Total	250	250	224	219	32	25	0.9000	0.936	0.89	0.8654	0.8898

Table 5 Evaluation of existing SVM method parameters numerical results

Input set	Number of authentic images	Number of forged images	T_p	T_n	F_p	F_n	Sensitivity (%)	Specificity (%)	Accuracy (%)	F-measure	G-mean
Set-1	50	50	40	45	5	10	0.8000	0.9000	0.8500	0.8421	0.8485
Set-2	50	50	38	45	5	12	0.7600	0.9000	0.8300	0.8172	0.8270
Set-3	50	50	40	42	8	10	0.8000	0.8400	0.8200	0.8163	0.8198
Set-4	50	50	40	50	0	10	0.8000	1	0.9000	0.8889	0.8944
Set-5	50	50	37	47	3	13	0.7400	0.9400	0.8400	0.8222	0.8340
Total	250	250	195	229	21	55	0.78	0.916	0.848	0.8374	0.8441

4.4 Performance Evaluation

Figures 4, 5, 6, 7, 8, 9, 10 and 11 shows that the overall performance [20, 36, 47, 54] of proposed IRVM and existing HMM + SVM, SVM forgery detection schemes for CoMoFoD database. The figures illustrate the performance of accuracy value is high in proposed IRVM due to the optimal weight prediction and BWT based decomposition. This reduce noise of image in proposed scheme. So, it increased the performance of proposed scheme. So, it increased the performance of the proposed scheme. The sensitivity, specificity values are high in proposed scheme, when increase the number of image, the performance also increased. The proposed system ha low false positive rate and low positive negative rate, and

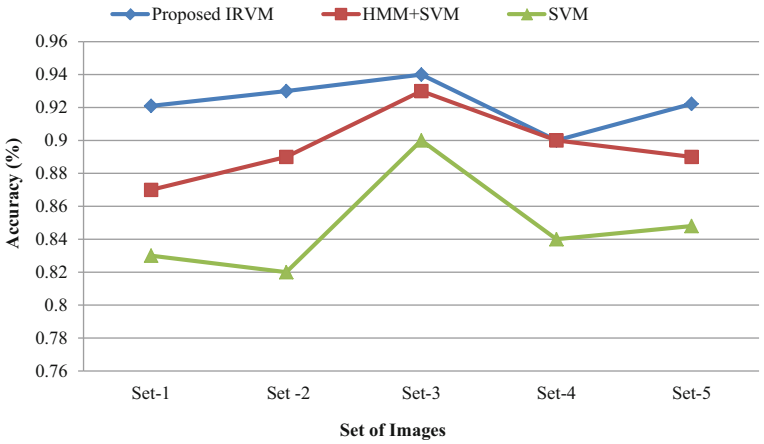

Fig. 4 Accuracy comparison

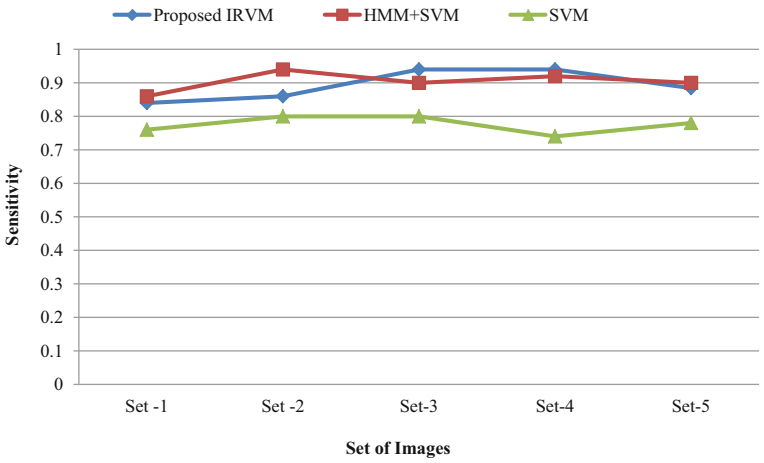

Fig. 5 Sensitivity comparison

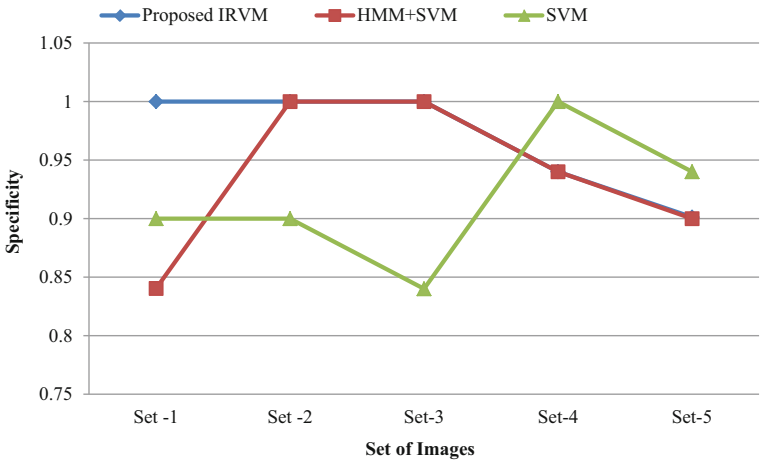

Fig. 6 Specificity comparison

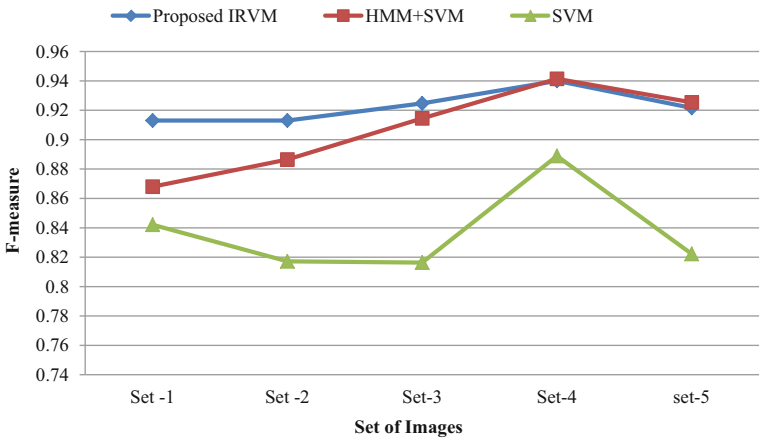

Fig. 7 F-measure comparison

these measures are predicted from precision and recall values. The f-measure and Geometrical means (G-mean) measures also have high value in proposed IRVM compared than existing HMM + SVM and SVM methods.

The evaluation of other parameters like precision, recall, PPV, NPV, FPR and FNR are evaluated for all classifiers and their evaluation results are showed in Table 6. It shows the proposed IRVM attained high results compared than existing schemes.

From the Table 7, only the HMM + SVM method has ability to manage a sensitivity with rate of 90% but it has attained low specificity compared than proposed scheme due to the high training time of SVM. The SVM also has attained less accuracy compared than proposed scheme due to the computational complexity.

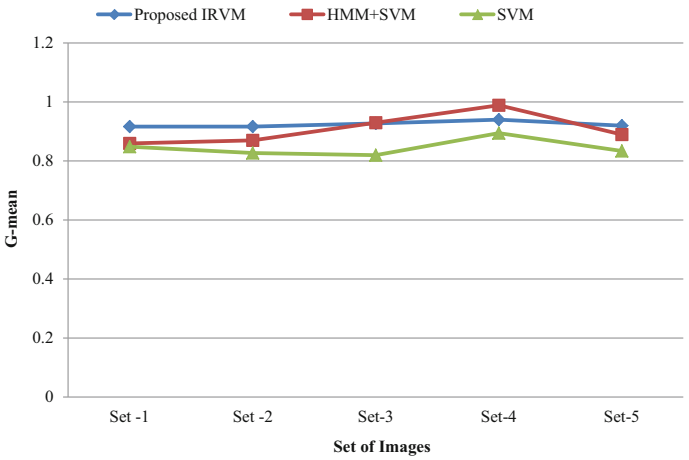

Fig. 8 G-mean comparison

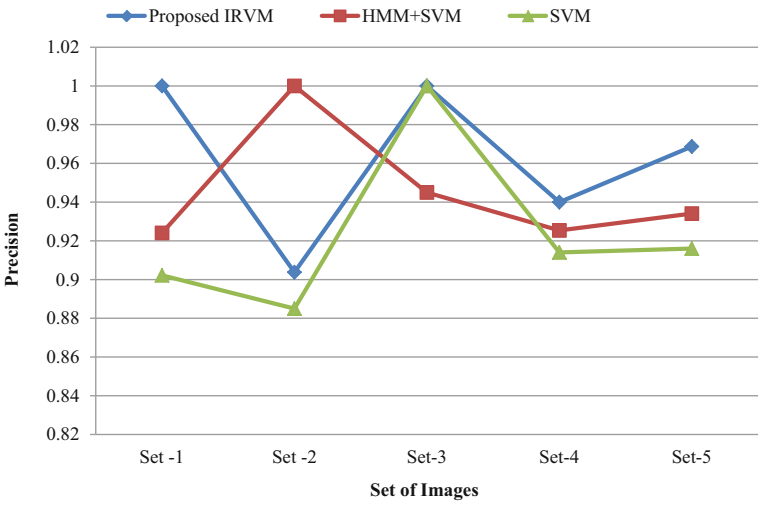

Fig. 9 Precision comparison

As well as, the proposed IRVM scheme attained high performance with high accuracy rate of 92.22%, sensitivity rate of 88.4%, specificity rate of 97.6%, F-measure rate of 92.24%, G-mean rate of 92.31%, precision rate of 96.87% and recall rate of 88.4% compared than existing scheme and their comparative Bar-chart is shown in Fig. 11.

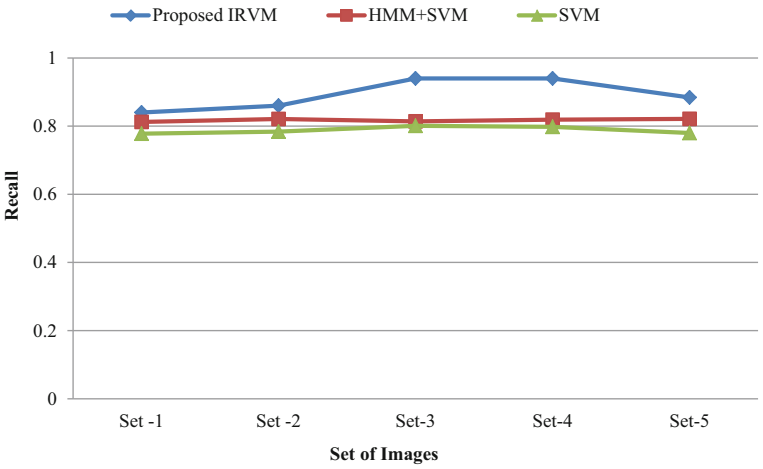

Fig. 10 Recall comparison

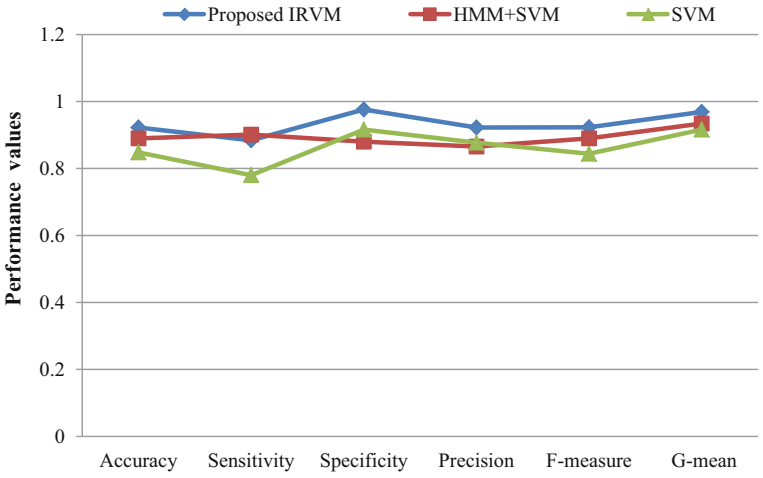

Fig. 11 Overall performance prediction for all classification methods

Table 6 Evaluation of other parameters numerical results for all classifiers

Methods	Precisions (%)	Recall (%)	PPV (%)	NPV (%)	FPR (%)	FNR (%)
SVM	0.9160	0.78	0.8178	0.8182	0.2040	0.1920
HMM + SVM	0.9341	0.8214	0.8822	0.8979	0.1200	0.1000
Proposed IRVM	0.9687	0.884	0.9221	0.9124	0.1600	0.0962

Table 7 Overall performance numerical values of forgery detection methods

Performance matrices	Proposed IRVM	HMM + SVM	SVM
Accuracy	0.9222	0.89	0.848
Sensitivity	0.884	0.9000	0.78
Specificity	0.976	0.88	0.916
F-measure	0.9224	0.8654	0.8772
G-mean	0.9231	0.8898	0.8441
Precision	0.9687	0.9341	0.9160
Recall	0.884	0.8214	0.78

5 Conclusion

In this paper, IRVM based copy-move forgery detection has been proposed with BWT. The main contribution of this work is that it carries out copy-move detection in image bocks, which significantly narrows comparison of the similar blocks, thus reducing the computational complexity. Initially, the input color image has been converted into grey scale. After that, the Biorthogonal Wavelet Transform (BWT) is used to reduce noise and extract the feature. Then, the, the feature vectors are sorted in lexicographically and the duplicate vectors are identified by similarity between two successive vectors. To decide the similarity of vectors, Minkowski distance and Threshold value is used. Finally, the Improved RVM has been carried out with GSO algorithm to detect the forgery. Experimental results show the effectiveness of the proposed IRVM scheme attained high performance with high accuracy rate of 92.22%, sensitivity rate of 88.4%, specificity rate of 97.6%, F-measure rate of 92.24%, G-mean rate of 92.31%, precision rate of 96.87% and recall rate of 88.4% compared than existing, also its robustness against after-copying operations, and detection of multiple copy-move forgery. In future, some other machine learning or neural network based forgery detection will focus with same texture instead of the whole image.

References

1. Elwin, J. G. R., Aditya, T. S., & Madhu Shankar, S. (2010). Survey on passive methods of image tampering detection. In *Proceedings of the international conference on communication and computational intelligence (INCOCCI'10)* (pp. 431–436).
2. Redi, J. A., Taktak, W., & Dugelay, J.-L. (2011). Digital image forensics: A booklet for beginners. *Multimedia Tools and Applications, 51*(1), 133–162.
3. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security, 6*(3), 1099–1110.
4. Pan, X., & Lyu, S. (2010). Detecting image region duplication using sift features. In: *Proceedings of the IEEE international conference on acoustics, speech, and signal processing (ICASSP'10)* (pp.1706–1709).
5. Chauhana, D., Kasatb, D., Jainc, S., Thakared, V. (2016) Survey on keypoint based copy-move forgery detection methods on image. In *Elsevier—International Conference on Computational Modeling and Security (CMS 2016)* (pp. 206–212).
6. Malviya, A., & Ladhake, S. (2016). An image forensic technique for detection of copy-move forgery in digital image. In *International symposium on security in computing and communication* (pp. 328–335). Springer Singapore.

7. Al-Qershi, O. M., & Khoo, B. E. (2016). Copy-move forgery detection using on locality sensitive hashing and k-means clustering. In *Information science and applications (ICISA)* 2016 (pp. 663–672). Springer Singapore.
8. Ustubioglu, B., Ulutas, G., Ulutas, M., & Nabiyev, V. V. (2016). A new copy move forgery detection technique with automatic threshold determination. *International Journal of Electronics and Communications, 70*(8), 1076–1087.
9. Kaushik, R., Bajaj, R. K., & Mathew, J. (2015). On image forgery detection using two dimensional discrete cosine transform and statistical moments. *Procedia Computer Science, 70,* 130–136.
10. Isaac, M. M., & Wilscy, M. (2015). Image forgery detection based on Gabor Wavelets and Local Phase Quantization. *Procedia Computer Science, Elsevier, 58,* 76–83.
11. Pun, C.-M., Yuanand, X.-C., & Bi, X.-L. (2015). Image forgery detection using adaptive over-segmentation and feature point matching. *IEEE Transactions on Information Forensics and Security, 10*(8), 1705–1716.
12. Ardizzone, E., Bruno, A., & Mazzola, G. (2015). Copy-move forgery detection by matching triangles of keypoints. *IEEE Transactions on Information Forensisics and Security, 10*(10), 2084–2094.
13. Anand, V., Hashmi, M. F. & Keskar, A. G. (2014). A copy move forgery detection to overcome sustained attacks using dyadic wavelet transform and SIFT methods. In *Proceedings of the 6th Asian conference on intelligent information and database systems (ACIIDS 2014)*. Springer International Publishing, pp. 530–542.
14. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013). Copy-move forgery detection and localization by means of robust clustering with J-linkage. *Signal Processing: Image Communication, 28*(6), 659–669.
15. Hashmi, M. F., A. R. Hambarde, & A. G. Keskar (2013). Copy move forgery detection using DWT and SIFT features. In *Proceedings of 13th IEEE international conference on intelligent systems design and applications (ISDA-2013)* (pp. 188–193).
16. Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International, 231*(1), 284–295.
17. Christlein, V., & Jordan, J. (2012). An evaluation of popular copy-move forgery detection approaches. In *IEEE transactions on information forensics and security* (pp. 1–26).
18. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transaction on Information Forensics and Security, 6*(3), 1099–1110.
19. Muhammad, G., Hussain, M., Khawaji, K., & Bebis, G. (2011). Blind copy move image forgery detection using dyadic undecimated wavelet transform. In: *Proceedings of IEEE 17th international conference on digital signal processing (DSP-2011)* (pp. 1–6).
20. Rathore, N. (2018). Performance of hybrid load balancing algorithm in distributed web server system. *Wireless Personal Communication*. https://doi.org/10.1007/s11277-018-5758-6.
21. Jain, N., Rathore, N., & Mishra, A. (2017). An efficient image forgery detection using biorthogonal wavelet transform and improved relevance vector machine with some attacks. *Interciencia Journal*, *42*(11), 95–120.
22. Rathore, N. (2016). Dynamic threshold based load balancing algorithms. *Wireless Personal Communications*, *91*(1), 151–185.
23. Rathore, N., & Chana, I. (2015). Variable threshold-based hierarchical load balancing technique in Grid. *Engineering with Computers*, *31*(3), 597–615.
24. Sharma, V., Kumar, R., & Rathore, N. (2015). Topological broadcasting using parameter sensitivity based logical proximity graphs in coordinated ground-flying ad hoc networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 6*(3), 54–72.
25. Rathore, N., & Chana, I. (2014). Load balancing and job migration techniques in grid: A survey of recent trends. *Wireless Personal Communications*, *79*(3), 2089–2125.
26. Rathore, N., & Chana, I. (2014). Job migration with fault tolerance based QoS scheduling using hash table functionality in social Grid computing. *Journal of Intelligent & Fuzzy Systems*, *27*(6), 2821–2833.
27. Rathore, N., & Singh, P. K. (2017). Comparative analysis of fuzzy based load balancing algorithms. *i-manager's Journal on Computer Science*, *5*(2), 23.
28. Rathore, N. K., & Singh, H. (2017). Analysis of grid simulators architecture. *i-manager's Journal on Mobile Applications and Technologies*, *4*(2), 32.
29. Rathore, N. K. (2016). Checkpointing: Fault tolerance mechanism. *Journal on Cloud Computing (JCC)*, *3*(4), 27–34.
30. Rathore, N. (2017). A review towards: Load balancing techniques. *i-manager's Journal on Power Systems Engineering*, *4*(4):47.

31. Rathore, N. K. (2016). Faults in grid. *International Journal of Software and Computer Science Engineering*, *1*(1), 1–19.
32. Rathore, N. K. (2016). Installation of Alchemi.NET in Computational Grid. *Journal on Computer Science (JCOM)*, *4*(2), 1–5.
33. Rathore, N. K. (2016). Ethical hacking & security against cyber crime. *Journal on Information Technology (JIT)*, *5*(1), 7–11.
34. Rathore, N. K. (2015). Efficient agent based priority scheduling and load balancing using fuzzy logic in grid computing. *Journal on Computer Science (JCOM)*, *3*(3), 11–22.
35. Rathore, N. K. (2015). Map reduce architecture for grid. *Journal on Software Engineering (JSE)*, *10*(1), 21–30.
36. Rathore, N. K. (2015). GridSim installation and implementation process. *Journal on Cloud Computing (JCC)*, *2*(4), 29–40.
37. Rathore, N. K., & Chana, I. (2013). Report on hierarchal load balancing technique in grid environment. *Journal on Information Technology (JIT)*, *2*(4), 21–35.
38. Rathore, N. K., & Chana, I. (2010). Checkpointing algorithm in alchemi.NET. *Pragyaan: Journal of Information Technology*, *8*(1), 32–38.
39. Rathore, N. K., & Chana, I. (2013). A sender initiate based hierarchical load balancing technique for grid using variable threshold value. In *International conference IEEE-ISPC* (pp. 1–6).
40. Prakash, O., Srivastava, R., Khare, A. (2013). Biorthogonal wavelet transform based image fusion using absolute maximum fusion rule. In *Proceedings of IEEE conference on information and communication technologies (ICT 2013)*.
41. Rathore, N. K., & Chana, I. (2011). A cognitative analysis of load balancing technique with job migration in grid environment. In *World congress on information and communication technology (WICT), Mumbai, IEEE proceedings paper* (pp. 77–82).
42. Rathore, N. K. (2015). Efficient load balancing algorithm in grid. In *30th M.P. Young Scientist congress, Bhopal, M.P.* (pp. 56).
43. Rathore, N., & Chana, I. (2015). Variable threshold-based hierarchical load balancing technique in Grid. *Engineering with Computers*, *31*(3), 597–615.
44. Chouhan, R., & Rathore, N. K. (2012). Comparision of load balancing technique in grid. In *17th annual conference of Gwalior academy of mathematical science and national symposium on computational mathamatics & information technology*, *JUET, Guna, M.P.* (pp. 7–9).
45. Kaur, S., & Dadhwal, H. S. (2015). Biorthogonal wavelet transform using bilateral filter and adaptive histogram equalization. *International Journal of Intelligent Systems and Applications, 7*(3), 37.
46. Li, N., Liu, C., He, C., Li, Y., & Zha, X. F. (2011). Gear fault detection based on adaptive wavelet packet feature extraction and relevance vector machine. *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science, 225*(11), 2727–2738.
47. Rathore, N. K., & Chana, I. (2010). Fault tolerance algorithm in Alchemi.NET Middleware. In *National conference on education & research (ConFR10), third CSI national conference of CSI division V, Bhopal Chapter, IEEE Bombay, and MPCST Bhopal, organized by JUIT, India*, 6–7th Mar 2010.
48. Rathore, N. K., & Chana, I. (2009). Checkpointing algorithm in Alchemi.NET. In *Annual conference of Vijnana Parishad of India and national symposium recent development in applied mathematics & information technology, JUET, Guna, M.P.*
49. Rathore, N. K., & Chana, I. (2008). Comparative analysis of Checkpointing. In *PIMR third national IT conference, IT enabled practices and emerging management paradigm book and category is communication technologies and security issues* (pp. 32–35) Topic No/Name-46, Prestige Management and Research, Indore, (MP) India.
50. Rathore, N. K., & Chana, I. (2018). An efficient load balancing technique for grid. In *Scholar's press, Mauritius*.
51. He, L., Tong, X., & Huang, S. (2012). A glowworm swarm optimization algorithm with improved movement rule." In *2012 fifth international conference on intelligent networks and intelligent systems (ICINIS)* (pp. 109–112). IEEE.
52. Rathore, N. K., & Singh, P. (2016). An efficient load balancing algorithm in distributed networks, Lambert Academic Publication House (LBA), Germany.
53. Rathore, N. K., & Chana, I. (2016). An enhancement of gridsim architecture with load balancing. In *Scholar's press*.
54. Rathore, N. K., & Sharma, A. (2015). Efficient dynamic distributed load balancing technique. In *Lambert Academic Publication House, Germany*.
55. Rathore, N. K., & Chana, I. (2010). Checkpointing Algorithm in Alchemi.NET. In *Lambert Academic Publication House (LBA), Germany*.

56. Hashmi, M. F., & Keskar, A. G. (2015). Image forgery authentication and classification using hybridization of HMM and SVM classifier. *International Journal of Security & Its Applications, 9,* 125–140.
57. Tralic, D., Zupancic, I., Grgic, S., & Grgic, M. (2013). CoMoFoD—New database for copy-move forgery detection. In *Proceedings of 55th international symposium ELMAR-2013* (pp. 49–54).
58. Cozzolino, D., Gargiulo, F., Sansone, C., & Verdoliva, L. (2013). Multiple classifier systems for image forgery detection. In *Proceedings of the image analysis and processing (ICIAP).*
59. Rathore, N. (2016). Efficient load balancing algorithm. *Wireless Personal Communication.* https://doi.org/10.1007/s11277-016-3452-0.
60. Rathore, N., & Chana, I. (2016). Job migration policies for grid environment. *Wireless Personal Communication, 89*(1), 241–269.

Publisher's Note

Neelesh Kumar Jain joined Computer Science and Engineering Department of Jaypee University, Guna, M.P., India, in 2011 and is presently serving as Assistant Professor in the department. He has over 10 years experience of teaching and research. He is perusing Ph.D. form Jaypee University of Engineering and Technology, Guna (MP). Received the degree of B.E. (Information Technology), M.E. (System Engineering) from Dr. B.R.A.University, Agra (UP), and Dayalbagh Educational Institute (DEI), Agra, His current interest includes Image Forensics, design and Analysis of Algorithm, Optimization Techniques.

Dr. Neeraj Kumar Rathore joined Computer Science and Engineering Department of Jaypee University, Guna, M.P., India, in 2010 and is presently serving as Assistant Professor in the department. He has over 10 years experience of teaching, research as well as industrial experience of IT Industry (Computer Sciences Corporation) with the role of Software Engineer. He is Ph.D. in Computer Science with specialization in Grid Computing (2014) and M.E. in Computer Engineering (2008) from Thapar University and B.E. in Computer Science and Engineering (2006). His areas of interests include Parallel and Distributed Computing, Grid Computing, DBMS and Data structure. He has over 50 publications in International Journals and Conferences and books of repute. Under his supervision, seven Master's thesis has been awarded and one MTech and Ph.D. is on-going.

Dr. Amit Mishra Assistant Professor, Department of Electronics and Communication Engineering, Thapar University, Patiala, Punjab, since July 24, 2015. He has over 15 years experience of teaching, research. Received the degree of B.E. (Electronics Engineering), M.E. (System Engineering) and Ph.D. (Soft computing) from Marathwada University, Aurangabad, Dayalbagh Educational Institute (DEI), Agra, and Jamia Millia Islamia (Central University), Delhi, India respectively. His current interest includes design of neural network architecture and its applications, Image processing, Blind deconvolution and adaptive filter design.