Natl. Acad. Sci. Lett.
https://doi.org/10.1007/s40009-020-00998-w

SHORT COMMUNICATION

Image Forgery Detection Using Singular Value Decomposition with Some Attacks

Neeraj Kumar Rathore[1] · **Neelesh Kumar Jain**[2] · **Prashant Kumar Shukla**[3] · **UmaShankar Rawat**[4] · **Rachana Dubey**[5]

Received: 4 September 2017 / Revised: 13 January 2020 / Accepted: 27 June 2020

Abstract To improve the trustworthiness to assess the digital images by identifying authentic images and tampered images, this work is focused on Copy-Move based image Forgery Detection (CMFD) and classification using Improved Relevance Vector Machine (IRVM). In this paper, Biorthogonal Wavelet Transform with Singular Value Decomposition (BWT-SVD)-based feature extraction is applied to find the image forgery. The proposed method begins with dividing the test images into overlapping blocks, and then Biorthogonal Wavelet Transform (BWT) with Singular Value Decomposition (SVD) applies to extract the feature vector from the blocks. After that, the feature vectors are sorts and the duplicate vectors are identified by the similarity between two successive vectors. The occurrences of clone vectors are identified on the basis of Minkowski distance and the threshold value. Then, similarity criteria result in the existence of forgery in images. To classify images into the category of authentic images or forged images, improved version of Relevance Vector Machine (RVM) uses, which leads to efficiency and accuracy of forged image identification process. Performance of proposed scheme tests by performing experiments on CoMoFoD database. The simulation results show that the proposed IRVM scheme attained high performance when compared with existing Copy-Move based image Forgery Detection schemes in MATLAB environment.

Keywords Biorthogonal wavelet transform (BWT) · Copy-move forgery (CMF) · Glowworm swarm optimization (GSO) · Improved relevance vector machine (IRVM) · Minkowski distance · Similarity measure

Introduction

Modernly, in digital publishing and printing fields, image forgery is considered as a major issue. Image forgery is the approach of modification of imaging data from the pictures using image-processing software packages like Photoshop, alternative image editor tools, etc. Various strategies for manipulating the image data like an addition of noise, scaling, blurring, resizing and rotation, adding and removing any object are used for hiding the real information within the image. The forged image leaves some clues which may be wont to find the manipulated regions. The Scale-Invariant Feature Transform (SIFT) feature may be used to find clone areas [1, 2]. For splicing tampered image

✉ Neeraj Kumar Rathore
neerajrathore37@gmail.com

Neelesh Kumar Jain
neeleshdei@gmail.com

Prashant Kumar Shukla
prashantshukla2005@gmail.com

UmaShankar Rawat
umashankar.rawat@jaipur.manipal.edu

Rachana Dubey
rachanamishra812@gmail.com

[1] Shri G. S. Institute of Technology and Science, Indore, M.P., India

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

[3] Department of Computer Science, School of Engineering and Technology, Jagran Lake City University, Bhopal, M.P., India

[4] School of Computing and IT, Manipal University Jaipur, Jaipur, India

[5] Lakshmi Nariman College of Technology, Bhopal, India

Published online: 29 July 2020

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 presented scheme goal is to automatically observe copy-move within a single method without any earlier information concerning the forgery type of the uncertain image. Some existing CMFD schemes are reviewed in the literature of [2–10].

In the field of digital image forensics, the Copy-Move based image Forgery Detection (CMFD) is one of the emerging problems. 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 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 based on biorthogonal wavelet transform (BWT) with singular value decomposition (SVD) and classification scheme improved relevance vector machine (IRVM) has been introduced.

Initially, the input color image has been converted into gray scale. After that, biorthogonal wavelet transform (BWT) is used to reduce noise and extract the feature. To reduce the computation complexity, the singular value decomposition (SVD) has been proposed and it exploits block comparison. Then, 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 HMM + SVM [13] and SVM [16]-based forgery detection method.

In this section, the proposed IRVM-based Copy-Move Forgery Detection (CMFD) algorithm has been discussed. The step by step procedure of proposed scheme has been discussed in given below sub sections.

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

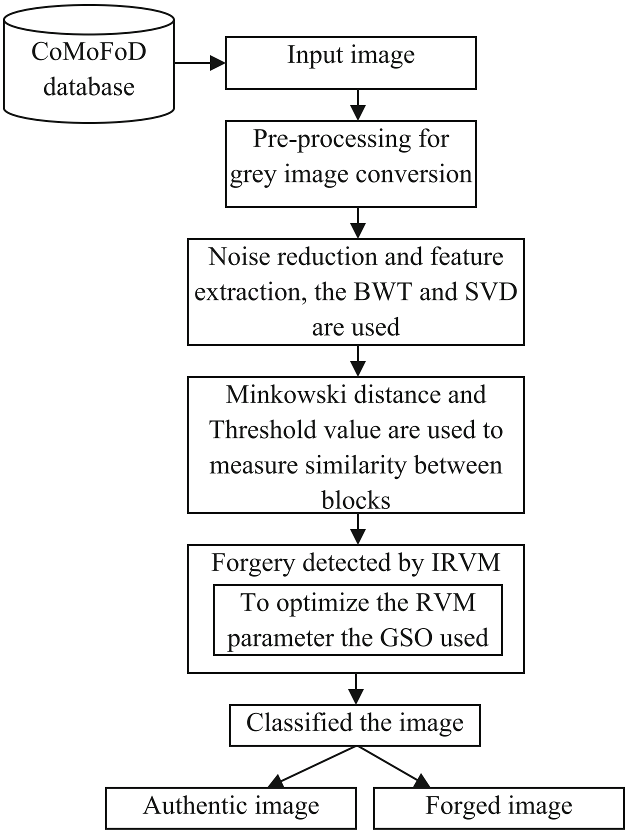

CoMoFoD database
Input image
Pre-processing for grey image conversion
Noise reduction and feature extraction, the BWT and SVD are used
Minkowski distance and Threshold value are used to measure similarity between blocks
Forgery detected by IRVM
To optimize the RVM parameter the GSO used
Classified the image
Authentic image
Forged image

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

Noise reduction and feature extraction: The input dataset has been downloaded from the 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 [19–34], the proposed system has been used a biorthogonal wavelet transform (BWT) and singular value decomposition (SVD) schemes.

Biorthogonal Wavelet Transform (BWT): In biorthogonal wavelet transform, biorthogonal filters are developed for providing symmetric property instead of using two filters. In this proposed scheme, the biorthogonal wavelet transform is used to denoising the image and extract the features from images like variance, mean, skewness, energy, etc.

To solve the problem of phase distortion, the BWT is designed and it contains spline wavelets [18]. Here, Finite Impulse Response filters are used to reconstruct the image. 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

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

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

Singular Value Decomposition (SVD): SVD can preserve the useful features of the original image and use less storage space of memory [17]. 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. Singular values signify maximum energy packing in an image that shows good constancy even when the image endures from minor deformation. Singular value feature vector has following geometric and algebraic invariant properties like scaling property, stability, and rotation invariance. It is also insensitive to noise. The proposed method attains dimensionality reduction of block vectors by using singular value decomposition as well as provides the better feature that is stable.

This forms the basis of using SVD as a dimensionality reduction technique. 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 → orthogonal matrices, $U^T U = I, V^T V = I$, and $S = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_r)$ [14]. 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.

Image forgery detection and classification using Improved Relevance Vector Machine (IRVM): Generally, RVM [11] 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 (GSO) to improve the classification accuracy. 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 the 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 $k(\hat{F}) = [k(F_1, \hat{F})\ldots k(F_n, \hat{F})]^T$, 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 [15], because, to train the model, it can adopt a Bayesian probabilistic framework. Also, it using the key feature of Automatic Relevance Determination (ARD) prior over the weight vector $\boldsymbol{w}$, which is used to separate 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 effectively forced to zero. Accordingly, the corresponding kernel functions can be pruned out in a sparse model result. The inputs F_i equivalent to the remaining nonzero weights is 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

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

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.

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

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.

Glowworm Swarm Optimization (GSO): The GSO [12] is a swarm intelligence based optimization algorithm. 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 probabilistic mechanism moves toward it. The probability of glowworms $p_j(t)$ moving toward a neighbor *nb* is based on Eq. (11) at iteration *t*

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

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

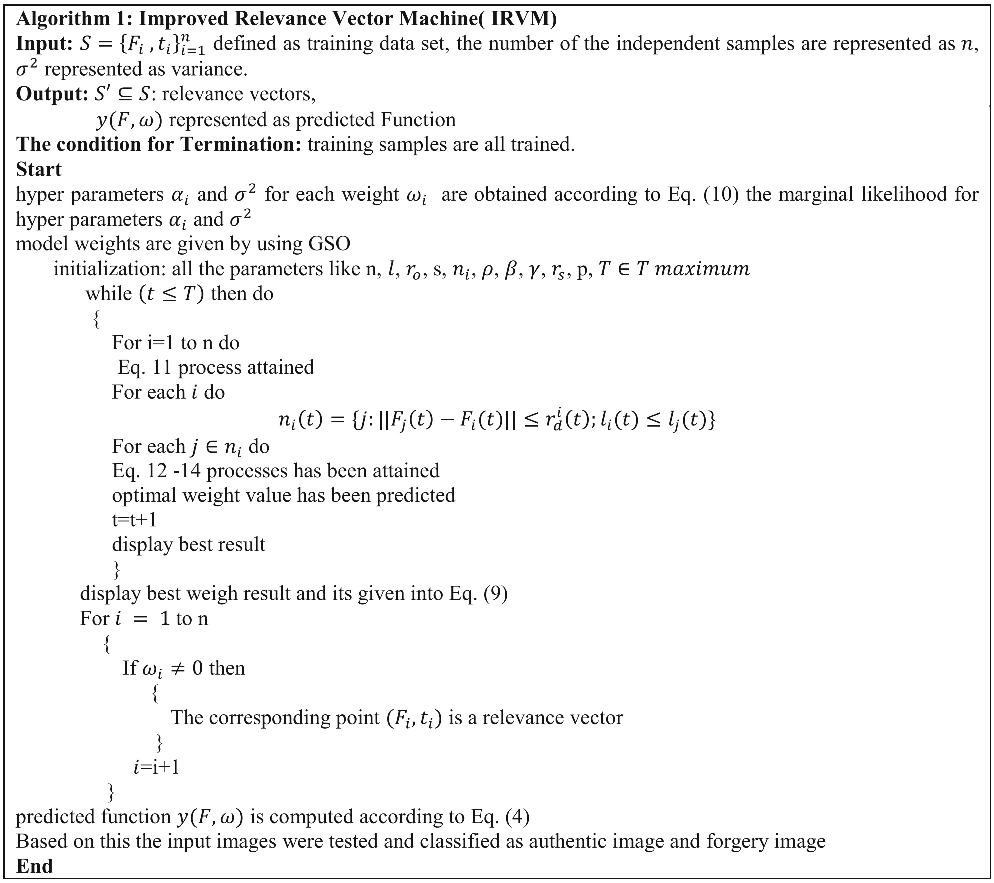
$$F_i(t+1) = F_i(t) + s\left(\frac{F_j(t) - F_i(t)}{F_j(t) - Fx_i(t)}\right) \tag{13}$$

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

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

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

where $r_d^i(t+1)$ is indicating the local-decision domain of glowworm *i* at the *t* + 1 iteration, β represents a constant parameter and changes the rate of altering 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 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 $n$, $\sigma^2$ represented as variance.
Output: $S' \subseteq S$: relevance vectors,
            $y(F,\omega)$ represented as predicted Function
The condition for Termination: training samples are all trained.
Start
hyper parameters $\alpha_i$ and $\sigma^2$ for each weight $\omega_i$ are obtained according to Eq. (10) the marginal likelihood for hyper parameters $\alpha_i$ and $\sigma^2$
model weights are given by using GSO
    initialization: all the parameters like n, $l$, $r_o$, s, $n_i$, $\rho$, $\beta$, $\gamma$, $r_s$, p, $T \in T\ maximum$
        while ($t \le T$) then do
        {
            For i=1 to n do
             Eq. 11 process attained
            For each $i$ do
                        $n_i(t) = \{j: ||F_j(t) - F_i(t)|| \le r_d^i(t); l_i(t) \le l_j(t)\}$
            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 $\omega_i \ne 0$ 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.

IRVM-based Copy-Move Forgery Detection (CMFD) Process:

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 with SVD is applied to each block in each node and the singular values are 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(Minkowski distance with exponent 2) 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,

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

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

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

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. The threshold parameter is calculated by using Minkowski distance of images from the set of authentic dataset. The threshold value is 15 for given experimental setup.

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 are 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 due to the efficient optimization and effective feature extraction process.

Results and Discussion: In this section, the proposed IRVM-based forgery detection performance tests on the basis of various performance measures which further compares with existing SVM-based forgery detection method [13] and HMM-SVM based forgery detection methods [14–34] results. At first, CoMoFoD database [15] images are trained and then tested. In training phase, 250 authentic images and 250 forged images are used for proposed IRVM model. In proposed experimental setup, images divided into 5 set, each set consist 100 images. Each gray-scale image is then tiled into overlapping blocks of size 128 × 128. Every set is undergoing through training procedure and each image from the set is tested with IRVM. The performance tests in terms of Sensitivity, *F*-measure, Specificity, *G*-mean, Precision and Accuracy. The simulation is running in MATLAB.

In this proposed system, evaluates small image size category (512 × 512). It is downloading from http://www.vcl.fer.hr/comofod/download.html

Evolution parameter for measuring forgery: In this paper, appropriate measures are used to tests the IRVM-based copy-move forgery detection performance. The performance measures [20-59] like Sensitivity (i.e., *Sen*), Specificity (i.e., *Spc*), Accuracy (i.e., *Acc*) Precision (*p*), Recall (*r*), *F*-measure, and *G*-mean calculate for set of images. The performance measures like Precision (*p*) and Recall (*r*) calculating for images with varying block sizes. In the experimental setup of the proposed method, T_p shows the value of a true positive rate of images, F_p shows the value of a false positive rate of images, T_n shows the value of a true negative of images and F_n shows the value of a false negative rate of images. These measures compute for query images and test images in the different run, and finally, the average performance of all measures computes.

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

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

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

Precision (*p*) could be a measure of 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 of 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

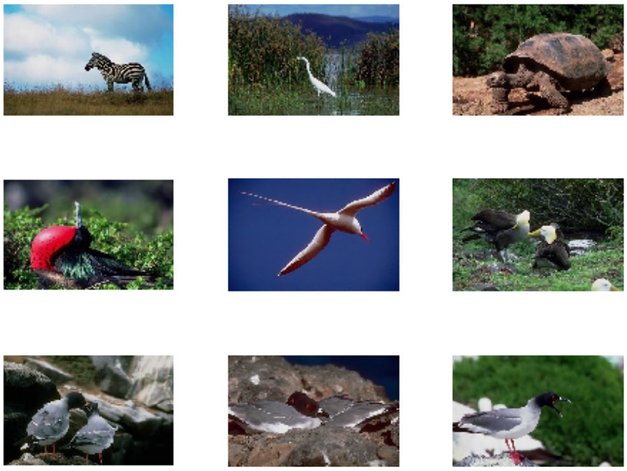


Fig. 2 Images used for testing and correctly detected as authentic

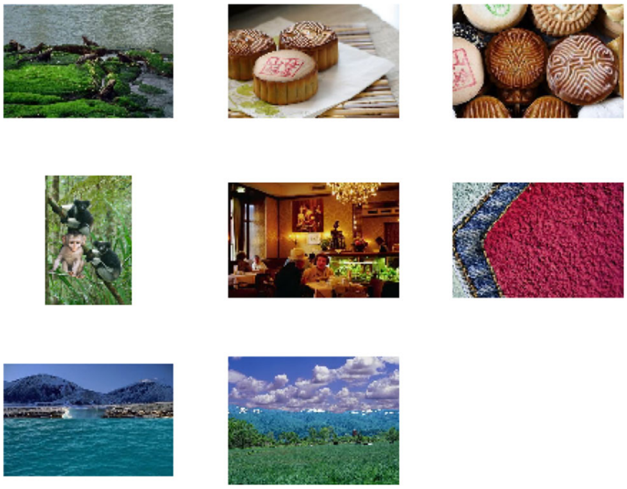


Fig. 3 Images used for testing and correctly detected as tampered

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

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

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

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

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

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

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

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

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

Training and classification procedure and results: In CoMoFoD database, set of images is modeled through estimates the parameters, and supply to IRVM. In training phase, set of authentic images and tampered images use as test data. Next, images are pre-process to extracts 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 show samples of authentic and forged images.

The proposed IRVM system performance is evaluated for all set of images (Set 1 to Set 5) and the numerical values in terms of accuracy, sensitivity, specificity, precision, recall, *F*-measure and *G*-mean are predicted in Table 1. In IRVM, for example, out of 100 images, 92 images are correctly identified the authentic and forgery images due to the efficient feature extraction and improved classifier. It illustrates that the number of images increases means the performance of proposed values also increases.

Table 1 Performance measures value for proposed method

Input	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 2 Evaluation of proposed method parameters numerical results

Input	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 3 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 4 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

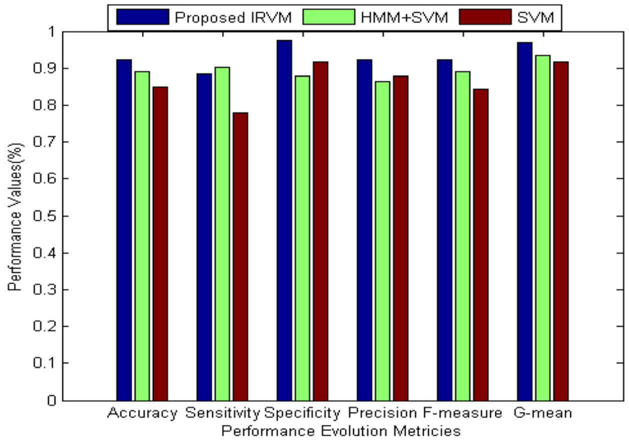


Fig. 4 Overall performance prediction for all classification methods

The set of images were trained and input images are tested in fivefold cross-validation experimental setup. The parameters values for each set are evaluates and their average values also predicted. The parameters values for proposed IRVM are showed in Table 2.

This Table 2 illustrates the proposed IRVM attained best results compared than existing schemes due to efficient feature selection and efficient training process with optimized weights.

The evaluation of other parameters like precision, recall, PPV, NPV, FPR, and FNR are evaluated for all classifiers and their evaluation results are shown in Table 3. It shows the proposed IRVM attained high results compared than existing schemes

Performance evaluation Table 4 shows the performance measures values of proposed IRVM with HMM + SVM, SVM forgery detection schemes in terms of accuracy, sensitivity, specificity, precision, recall, F-measure, and G-mean. Table 4 illustrates the accuracy (92.22%), sensitivity (88.4%), specificity (97.6%), F-measure (92.24%), G-mean (92.31%), precision (96.87%), recall (88.4%) of proposed IRVM is higher due to the optimal weight prediction and SVD-based decomposition. Table 4 illustrate that only the HMM + SVM method has the ability to manage a sensitivity with a 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.

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. 4.

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 on some texture instead of the whole image.

References

1. 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 Trans Inf Forensics Secur 6(3):1099–1110
2. Rathore N, Chana I (2014) Load balancing and job migration techniques in grid: a survey of recent trends. Wirel Pers Commun 79(3):2089–2125
3. Kuznetsov AV, Myasnikov VV (2016) A copy-move detection algorithm based on binary gradient contours. Comput Opt 40:284–293
4. Ranjani MB, Poovendran R (2016) Image duplication copy move forgery detection using discrete cosine transforms method. Int J Appl Eng Res 11(4):2671–2674
5. Ustubioglu B, Ulutas G, Ulutas M, Nabiyev VV (2016) A new copy move forgery detection technique with automatic threshold determination. Int J Electron Commun 70(8):1076–1087
6. Puri M, Chopra V (2016) A survey: copy-move forgery detection methods. Int J Comput Syst 3(9):582–586
7. Rathore NK (2016) Ethical hacking & security against cyber Crime. J Inf Technol 5(1):7–11
8. Ustubioglu B, Ulutas G, Ulutas M, Nabiyev VV (2016) A new copy move forgery detection technique with automatic threshold determination. Int J Electron Commun 70:1076–1087
9. Rathore N, Chana I (2014) Job migration with fault tolerance based QoS scheduling using hash table functionality in social Grid computing. J Intell Fuzzy Syst 27(6):2821–2833
10. Goyal H, Gulati T (2014) Robust copy-move image forgery detection using SIFT. Int J Comput Sci Appl 97:14–19
11. Rathore NK, Chana I (2008) Comparative analysis of checkpointing. In: PIMR 3rd National IT conference, IT enabled practices and emerging management Paradigm book and category is communication technologies and security issues, Topic No/Name-46, Prestige Management and Research, Indore, pp 32–35
12. 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 Trans Forensics Secur 6(3):1099–1110
13. Rathore NK, 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), IEEE proceedings paper, Mumbai, ISBN 978-1-4673-0127-5, December 2011, pp 77–82
14. Zhang G, Wang H (2012) SURF based detection of copy-move forgery in flat region. Int J Adv Comput Technol. https://doi.org/10.4156/ijact
15. Rathore N, Chana I (2015) Variable threshold-based hierarchical load balancing technique in Grid. Eng Comput 31(3):597–615
16. Li L, Li S, Zhu H (2013) An efficient scheme for detecting copy-move forged images by local binary patterns. J Inf Hiding Multimed Signal Process 4:46–56
17. Rathore NK, Chana I (2013) A sender initiate based hierarchical load balancing technique for grid using variable threshold value. In: International conference IEEE-ISPC, ISBN 978-1-4673-6188-0, 26–28 Sept 2013, pp 1–6
18. Ayumi V, Fanany MI (2015) Distribution-sensitive learning on relevance vector machine for pose-based human gesture recognition. Procedia Comput Sci 72:527–534
19. Rathore NK (2015) Map reduce architecture for grid. J Softw Eng 10(1):21–30
20. Zainal N, Zain AM, Radzi NHM, Othman MR (2016) Glowworm swarm optimization (GSO) for optimization of machining parameters. J Intell Manuf 27(4):797–804
21. Rathore NK (2014) Efficient hierarchical load balancing technique based on grid. In: 29th M. P. Young scientist congress, Bhopal, Feb 28, 2014, pp 55
22. Huynh-Kha T, Le-Tien T, Ha-Viet-Uyen S, Huynh-Van K, Luong M (2016) A robust algorithm of forgery detection in copy-move and spliced images. Int J Adv Comput Sci Appl 7(3):1–8
23. Rathore N (2018) Performance of hybrid load balancing algorithm in distributed web server system. Wirel Pers Commun 101(4):1233–1246
24. Tralic D, Zupancic I, Grgic S, Grgic M (2013) CoMoFoD-new database for copy-move forgery detection. In: Proceedings of the 55th international symposium ELMAR-2013, pp 49–54
25. Rathore NK (2015) Efficient agent based priority scheduling and load balancing using fuzzy logic in grid computing. J Comput Sci 3(3):11–22
26. 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 J 42(11):95–120
27. Kaur Savroop, Dadhwal Hartej S (2015) Biorthogonal wavelet transform using bilateral filter and adaptive histogram equalization. Int J Intell Syst Appl 7(3):37
28. Rathore N (2016) Dynamic threshold based load balancing algorithms. Wirel Pers Commun 91(1):151–185
29. Al-Qershi OM, Khoo BE (2013) Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Sci Int 231(1):284–295
30. Rathore N, Rawat U, Kulhari SC (2019) Efficient hybrid load balancing algorithm. Natl Acad Sci Lett. https://doi.org/10.1007/s40009-019-00834-w
31. Jain N, Rathore N, Mishra A (2018) An efficient image forgery detection using biorthogonal wavelet transform and improved relevance vector machine. Wirel Pers Commun 101(4):1983–2008
32. Rathore N, Chana I (2016) Job migration policies for grid environment. Wirel Pers Commun 89(1):241–269
33. Sharma V, Kumar R, Rathore NK (2015) Topological broadcasting using parameter sensitivity based logical proximity graphs in coordinated ground-flying ad hoc networks. J Wirel Mob Netw Ubiquitous Comput Dependable Appl 6(3):54–72
34. Rathore NK, Chana I (2013) Report on hierarchal load balancing technique in grid environment. J Inf Technol 2(4):21–35

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.