Blind Feature-Based Steganalysis with and Without Cross Validation on Calibrated JPEG Images Using Support Vector Machine

Deepa D. Shankar and Adresya Suresh Azhakath

Abstract The paper presents the comparative result analysis of calibrated JPEG images with and without cross-validation technique. Pixel-value differencing, LSB replacement, F5 and LSB Matching are used as steganographic algorithms. 25% of embedding is considered for the analysis. The images are calibrated before they are considered for analysis and relevant features are extracted. The classifier used is SVM with six various kernels and four types of sampling methods. The sampling methods are linear, shuffle, stratified and automatic. Radial, dot, Epanechnikov, multiquadratic, polynomial and ANOVA kernels are taken into consideration in this paper.

Keywords Steganalysis · Cross validation · Sampling · Kernel · Calibration · Feature extraction

1 Introduction

Steganography is the way of furtive communiqué [1]. The paper proposes a comparative analysis of how well the analysis of the presence of a medium is recognized. The payload used is a text message and the medium used are images in JPEG format. The JPEG format was chosen since it is the most preferred medium of Internet transmission [2, 3]. Steganalysis can be commonly allocated into two. Targeted steganalysis is intended for a certain procedure and is, therefore, very tough for that algorithm. On the contrary, blind steganalysis can recognize anonymous stego systems. Since the steganographic algorithms are not known, statistical analysis has been taken into consideration for blind steganalysis. Machine-learning techniques are incorporated and classifiers are used to check whether the given image contains a message or

D. D. Shankar (✉)
Banasthali Vidyapith, Jaipur, Rajasthan, India
e-mail: deepadayashankar@gmail.com

A. S. Azhakath
BITS Pilani, Dubai, UAE
e-mail: sudee99@gmail.com

© Springer Nature Singapore Pte Ltd. 2020

R. Sharma et al. (eds.), *Innovation in Electrical Power Engineering, Communication, and Computing Technology*, Lecture Notes in Electrical Engineering 630,
https://doi.org/10.1007/978-981-15-2305-2_2

not. The use of statistics can give rise to false positives and false negatives. These errors need to be reduced to get a good detection rate. The paper considers four steganographic algorithms. LSB replacement is the simplest steganographic system [4, 5]. The LSB matching algorithm works by modifying the individual coefficients. The modification is done by randomly increasing or decreasing the bits. Due to this arrangement, LSB modification is difficult to detect than LSB replacement. Both LSB modification and LSB replacement embedding are done in spatial domain, whereas pixel-value differencing (PVD) and F5 embedding are done in transform domain [6]. F5 works under the principle of matrix embedding. The matrix embedding lowers the number of changes in embedding, when it is a small payload. This is the reason for F5 to be considered for analysis. PVD [7] works under transform domain and also make use of PRNG to achieve confidentiality just as F5 does. Two domains can be considered for steganalysis—spatial and transform. In spatial domain, the pixel values are considered directly, whereas in transform domain, the pixels undergo a transformation before the values are considered. The frequency of coefficients is used to create a histogram [3]. Different features had been considered in previous research [8–11]. The paper deals with images that are changed to transform domain. The transformation is discrete cosine transform (DCT). The DCT uses the concept of block dependency along with the concept of calibration in images to extract the features [13]. The technique of calibration is shown in Fig. 1. In calibration, the DCT-transformed image is converted into the spatial domain. Four pixels each from both horizontal and vertical side of the image are cropped. This is because the JPEG property states that any changes incorporated in the spatial image of a JPEG image will erase any existing embeddings. The changes can be either cropping, rotating or skewing.

Images that undergo calibration will have the similar features as the cover image. After calibration, the relevant features are mined from both images. Previous literature had discussed several features [8, 9, 11]. For analysis, this paper makes use of an arrangement of initial orders [12] and Markov features [10]. The characteristics are removed and served in a classification method to sense the incidence of a communication. Using the features, the cover and stego images are classified by the classifier. This paper makes use of support vector machine (SVM) as classifier. The consideration was due to the fact that the previous literature stated SVM to be an exceptional tool for presumptions in wide real-life scenarios.SVM is also the most prevalent classifier to decide the existence of payload [13].

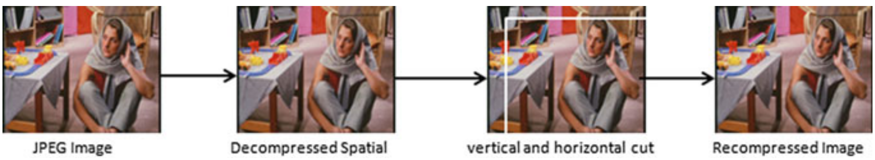

Fig. 1 Technique of calibration

2 Implementation

The work flow for the steganalytic scheme is given in Fig. 2.

2.1 *Extraction of Features*

The objective of the paper is a reasonable work with and without cross validation on calibrated images to achieve a decent classification for image with an embedding percentage of 25. The system emphasize upon removing the relevant features which will reach a totality of 274 features. The original DCT characteristics are 23 functionals [8]. The extraction is carried out and can be symbolized as:

$$F = |f(Si) - f(Ci)| \tag{1}$$

The initial values can be stretched to 193 functionals that are interblock dependencies [10]. The features of Markov are the dependencies of the intra block. The paper, therefore, takes into account the dependencies based on interblock and intrablock, to eliminate the shortcomings triggered by each of them. DCT coefficient array $d_{i(a,\,b)}$ defines a stego image, where i is the block and a and b are coefficients [9]. The dual histogram is signified by

$$g_{ab}^{d} = \sum_{i=1}^{n} x(d, d_{i(a,b)}) \tag{2}$$

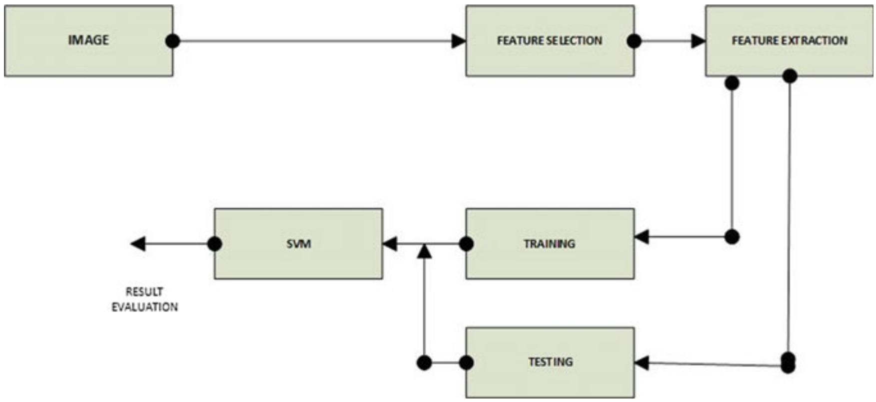

Fig. 2 Workflow diagram of steganalytic system

where g is the maximum block number and d is the value of the coefficient. Variance is epitomized as

$$V = \sum_{a,b=1}^{8} \sum_{i=1}^{|I_{\text{row}}|-1} \left| d_{I_{\text{row}}(i)(a,b)} - d_{I_{\text{row}}(i+1)(a,b)} \right| + \sum_{a,b=1}^{8} \sum_{i=1}^{|I_{\text{col}}|-1} \left| d_{I_{\text{col}}(i)(a,b)} - d_{I_{\text{col}}(i+1)(a,b)} \right| \tag{3}$$

where I_{row} and I_{col} are vectors of block indices [11, 14].

Blockiness is denoted as

$$B_\alpha = \frac{\sum_{a=1}^{|(A-1)/8|} \sum_{b=1}^{B} \left| x_{(8a,b)} - x_{(8a+1,b)} \right|^n + \sum_{a=1}^{|(B-1)/8|} \sum_{b=1}^{A} \sum \left| x_{(8a,b)} - x_{(8a+1,b)} \right|^n}{B[(A-1)/8] + A[(B-1)/8]} \tag{4}$$

where A and B are the image dimensions. The sharing of probabilities of neighbouring DCT coefficient pairs is known as a co-occurrence. It is denoted as

$$C_{st} = \frac{\sum_{i=1}^{|I_{\text{row}}|-1} \sum_{a,b=1}^{8} \delta(s, d_{a,(i)}(i,j)\delta(t, d_{a,(i+1)}(a,b) + \sum_{i=1}^{|I_{\text{col}}|-1} \sum_{a,b=1}^{8} \delta(s, d_{a,(i)}(a,b)\delta(t, d_{a,(i+1)}(a,b)}{|I_{\text{row}}| + |I_{\text{col}}|} \tag{5}$$

The Markov feature has four different arrays in horizontal, vertical and two diagonal directions.

2.2 Cross Validation

Usually, an image server is split into a variety of training and testing. This is achieved by assigning the image at random, thereby eliminating any bias. No rules are in place to verify that the testing and training set have to be identical. Training and testing are executed k times to avoid performance dissimilarity, known as k-fold validation. In this paper, the definition of cross validation is 10 for the value of k [12]. Here, the training and testing are done 10 times. The value of k can be changed.

2.3 SVM Classification

The classification phase is performed after feature extraction. The SVM gives an optimal hyperplane with the training dataset to classify the hyperplane [13] as shown in Fig. 3. This gives the minimum distance to sustain the vector, which is called the margin.

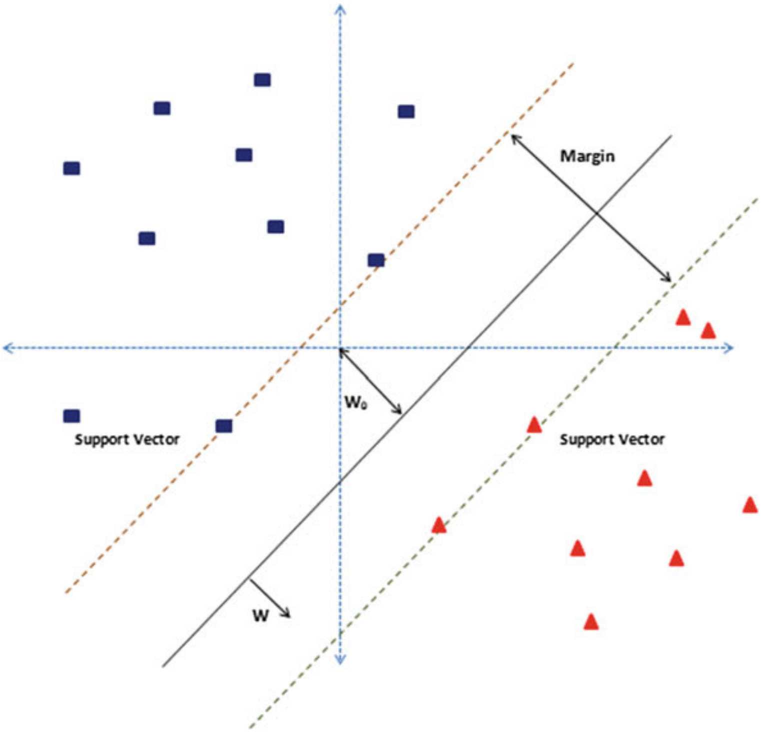

Fig. 3 Classification using support vector machine

The choice of SVM is because of its efficiency to work well with high-dimensional features and the flexibility to choose a greater number of kernels.

The following Eq. (6) characterizes the radial kernel

$$\mathrm{e}^{(-g||a-b||^2)} \tag{6}$$

where g is the gamma parameter. The dot kernel is characterized by

$$k(a, b) = a * b \tag{7}$$

The Eq. (7) represents the polynomial kernel

$$k(a, b) = (a * b + 1)^v \tag{8}$$

v is known as the degree of the kernel.

The ANOVA kernel is said as

$$e^{(-g(a-b))} \tag{9}$$

The Epanechnikov kernel is shown by the function

$$(3/4)(1 - n2) \tag{10}$$

for n between -1 and 1 and zero for n outside that range. Equation (11) describes multiquadratic kernel

$$\sqrt{||a-b||^2 + c^2} \tag{11}$$

3 Experimental Results

The experimental results of the works are explained as below:

3.1 Database of Images

The performance of a research depends on the quality of the database used for it. This paper uses a collection of 2300 images each of JPEG format. The image is compressed to 256×256 in size. UCID standard dataset [15] of 1500 JPEG images is used as the training dataset and the standard INRIA image dataset [16] of 800 images are taken as the test dataset. The images are calibrated and the relevant features are selected and extracted for classification. The selection of features is based on their sensitivity towards embedding changes.

3.2 Feature Extraction

The features adapted in this paper are 274 comprising of first order, second order, extended DCT and Markovian features. All features are normalized before any analysis is done.

3.3 Training Phase

The dataset of 1,500 images each with 274 characteristics is used during the training stage. The characteristics are fed into the classifier after being either marked as stego or cover, thus decreasing the amount of false positives and false negatives.

3.4 Testing Phase

The phase comes after the classifier is trained. 800 images are used for testing and features are extracted. In order to avoid overfitting, it is highly recommended to have the test dataset to be different from training dataset. Moreover, this concept is correct for the scenario because the analysis is always performed with real-time information.

4 Analysis of Results

In this paper, only calibrated images are used for classification. SVMs are generally flexible for various sampling and diverse kernels and, therefore, reflected for classification in this paper.

4.1 Results with No Cross Validation

The results with no cross validation done with four steganographic schemes is as explained below (Tables 1 and 2).

From the above results, multiquadratic kernel, radial kernel and Epanechnikov kernel give lower results than the other mentioned kernels. ANOVA, polynomial and dot kernel offer improved result with stratified sampling.

Table 1 Results on LSB replacement

	Linear	Shuffle	Stratified	Automatic
Dot	55.13	73.29	72.85	72.85
Radial	42.89	42.24	42.7	42.7
Polynomial	56.2	72.3	55.12	55.12
Multiquadratic	42.9	48.16	50	50
Epanechnikov	43.78	44.46	44.79	44.79
ANOVA	57.12	72.52	73.3	73.3

Table 2 Results on LSB matching

	Linear	Shuffle	Stratified	Automatic
Dot	53.4	73.3	72.4	72.4
Radial	44.8	46.03	45.7	45.7
Polynomial	53.07	73.28	72.6	72.6
Multiquadratic	45.91	52.57	53.23	53.23
Epanechnikov	53.11	48.4	48.93	48.93
ANOVA	54.6	59.73	72.45	72.45

From the above results, radial, multiquadratic and Epanechnikov kernels provide a lower result rate than the other kernel functions. The above results give good results with ANOVA, polynomial and dot kernel with stratified sampling (Tables 3 and 4).

The worthy results are obtained with ANOVA, polynomial and dot kernel with stratified sampling.

The above results give good results with ANOVA, polynomial and dot kernel with stratified sampling.

Table 3 Results on pixel-value differencing

	Linear	Shuffle	Stratified	Automatic
Dot	42.78	53.1	51.83	51.83
Radial	42.89	31.73	31.90	31.90
Polynomial	41.98	53.21	51.21	51.21
Multiquadratic	42.67	48.13	50	50
Epanechnikov	42.78	36.33	37.34	37.34
ANOVA	42.89	50.41	51.12	51.12

Table 4 Results on F5

	Linear	Shuffle	Stratified	Automatic
Dot	55.10	75.89	74.83	74.83
Radial	42.67	53.2	53.72	53.72
Polynomial	51.12	72.34	71.82	71.82
Multiquadratic	40.52	48.17	50	50
Epanechnikov	54.24	54.13	56.34	56.34
ANOVA	56.13	76.27	84.78	84.78

4.2 Results with Cross Validation

The results with no cross validation done with four steganographic schemes are as explained below (Table 5):

The above findings indicate that with stratified sampling, the ANOVA gives a better outcome (Table 6).

In the above result, the stratified sampling gives a better result with polynomial kernel (Table 7).

Similar to other kernels, the dot kernel gives a better result with stratified sampling (Table 8).

From the consequence, it can be understood that with stratified sampling, the ANOVA gives the highest outcome.

Table 5 Results on LSB replacement

	Linear	Shuffle	Stratified	Automatic
Dot	69.51	74.66	74.66	74.66
Radial	43.88	56.78	67.95	67.95
Polynomial	71.3	73.62	73.62	73.62
Multiquadratic	43.78	49.73	50.03	50.03
Epanechnikov	43.88	48.2	47.07	47.07
ANOVA	64.98	74.32	74.32	74.32

Table 6 Results on LSB matching

	Linear	Shuffle	Stratified	Automatic
Dot	65.96	73.46	73.49	73.49
Radial	48.38	49.72	50.2	50.2
Polynomial	68.83	72.4	77.58	77.58
Multiquadratic	52.32	52.29	52.29	52.29
Epanechnikov	56.23	48.16	48.14	48.14
ANOVA	61.7	73.27	73.2	73.2

Table 7 Results on F5

	Linear	Shuffle	Stratified	Automatic
Dot	92.74	97.35	97.26	97.26
Radial	50.26	56.12	57.53	57.53
Polynomial	90.35	94.82	94.69	94.69
Multiquadratic	50.02	47.74	49.96	49.96
Epanechnikov	62.26	56.12	57.53	57.53
ANOVA	91.24	93.56	94.65	94.65

Table 8 Results on pixel-value differencing

	Linear	Shuffle	Stratified	Automatic
Dot	5.68	54.31	54.31	54.31
Radial	6.4	40.21	40.78	40.78
Polynomial	43.87	53.82	53.18	53.18
Multiquadratic	49.6	57.63	58.35	58.35
Epanechnikov	52.06	47.31	48.25	48.25
ANOVA	52.94	63.88	71.75	71.75

5 Conclusion

The payload was embedded using four different steganographic algorithms. The embedding rate used here is 25. The dataset used for analysis is calibrated to have an estimate of cover image. SVM is the classifier used for the dataset. The findings were obtained from multiple kernels and sampling techniques. The final review suggests that the cross-validation outcome is better than the result without cross validation. For LSB replacement, the polynomial kernel gives better result with cross validation than without it. In LSB matching, both dot and polynomial give good result with cross validation. PVD gives better result with ANOVA and stratified sampling. F5 gives the best classification rate with ANOVA, cross validation and stratified sampling.

References

1. Kumar BR, Murti PR (2011) Data security and authentication using steganography. Int J Comput Sci Inf Technol 2(4):1453–1456
2. Sherif M, Badr M, Salim I (2014) A review on steganalysis techniques: from image format point of view. Int J Comput Appl 1:0975–8887
3. Shankar DD, Upadhyay P (2016) Performance analysis of various feature sets in calibrated blind steganalysis. Int J Comput Sci Netw Secur 16:29
4. Goljan M, Fridrich J, Soukal T (2003) Higher-order statistical steganalysis of palette images. Proc SPIE 5020:178–190
5. Ker AD (2005) A general framework for the structural analysis of LSB replacement. In: Proceedings of the 7th information hiding workshop, pp 296–311
6. Westfeld A (2001) F5—a steganographic algorithm. In: Information hiding: 4th international workshop, pp 289–302
7. Wu D-C, Tsai W-H (2003) A steganographic method of images by pixel-value differencing. Patt Recogn Lett 24:1613
8. Attaby AA, Alsammak AK, Mursi Ahmed MFM (2018) Data hiding inside JPEG images with high resistance to steganalysis using a novel technique. DCT-M3 Ain Shams Eng J 9(4):46–50
9. Zeng J, Li B, Huang J, Tan S (2017) Large scale JPEG image steganalysis using hybrid deep learning framework. IEEE Trans Inf Forens Secur 1–14:1200
10. Pevny T, Fridrich J, Merging Markov (2007) DCT features for multiclass JPEG steganalysis. In: SPIE proceedings, electronic imaging, security, steganography and watermarking of multimedia contents, vol IX, pp 301–314

11. Ashu A, Chhikara R (2014) Performance evaluation of first and second order features for steganalysis. Int J Comput Appl 92:17–22
12. Kokkinos Y, Margaritis KG (2018) Managing the computational cost of model selection and cross-validation in extreme learning machines via Cholesky, SVD, QR and eigen decompositions. Neurocomputing 21:29–45
13. Liu P, Yang C, Liu F, Song X (2015) Improving steganalysis by fusing SVM classifiers for JPEG images. In: International conference on computer science and mechanical automation (CSMA), pp 185–190
14. Kodovsky J, Fridrich J (2009) Calibrated revisited. In: The workshop in ACM multimedia and security, pp 63–74
15. Schaefer G, Stich M (2004) UCID-an uncompressed colour image database. In: SPIE conference storage and retrieval methods and applications for multimedia
16. Jegouu H, Schmid C (2008) Hamming embedding and weak geometric consistency for large scale image search. In: European conference computer vision