Low Dimensional Multi Class Steganalysis of Spatial LSB based Stego Images Using Textural Features

Veena Sivasamy Thanasekaran
Department of Computer Science and Engineeirng
Mepco Schlenk Engineering College, India
veena_st@mepcoeng.ac.in

Arivazhagan Selvaraj
Department of Electronics and Communication Engineering
Mepco Schlenk Engineering College, India
sarivu@mepcoeng.ac.in

Abstract: *Image steganalysis ranges from detecting the presence of covert information in an image (passive steganalysis) to extraction of the information from the stego image (active steganalysis). One of the steps in active steganalysis is determining the stego algorithm used to produce the stego image. In this paper, a low dimensional combination of textural features is adapted for steganalysis. Also a novel blind statistical steganalyser to determine the spatial domain Least Significant Bit (LSB) based algorithms using one against one multi class classification is proposed. The proposed steganalyser is a multiclass ensemble Fisher Linear Discriminant (FLD) classifier that uses novel low dimensional textural features for steganalysis. The performed experiments on the Bossbase database for 5 different LSB based algorithms for 8 different payloads show that the results are much better than the state of art steganalyser.*

Keywords: *Active steganalysis, blind steganalysis, statistical steganalysis, multi class classifier, spatial domain algorithms, ensemble classifier.*

Received May 3, 2022; accepted May 8, 2023
https://doi.org/10.34028/iajit/21/2/6

1. Introduction

Steganalysis is the process of detecting the presence of covert information in a medium. If the medium is an image, then it is called image steganalysis. Detecting the mere presence of hidden information in the image is termed as passive image steganalysis. Finding out more details of the concealed information in the stego image like length, location and extraction of the secret information is named as active image steganalysis [2, 30]. Algorithm determination is the first step of active steganalysis needed to extract the secret. Here the information about which algorithm has been employed to create the stego image is identified. It is done using multi class classification.

Steganalysis is more promising in case of pre compressed JPEG images or colour images [21], since the embedding process leaves a heavy trail in those images, that can be detected, even for meagre payload secrets. And thus most of the literature concentrates on binary classification or multi class classification of algorithms in JPEG images [6, 13, 19, 23, 24, 34] but a few are reported for multi class classification of grayscale images in spatial domain [1, 18].

The existing binary classification feature models [9, 11], that work on large number of spatial domain steganographic algorithms have practical difficulty in acquiring features and extending them to multi classification because of their high dimensionality and complex nature. Also recently deep neural network is drawing attention to steganalysis like other field [1, 22, 33, 36].

But they require high computational machines or GPUs for processing. Also there exists a research about the choice of well-defined handcrafted features and those of deep learning [4, 7, 26, 35]. Hence, in condense, our aim is to find a low dimensional hand crafted feature for identifying the most popularly used Least Significant Bit based steganographic algorithms in spatial domain of grayscale images. Here the main algorithms considered are Least Significant Bit Replacement (LSBR), Least Significant Bit Matching (LSBM), Least Significant Bit Matching Revisited (LSBMR), Two LSB bit embedding (LSBR2) and Modular Five (LSBRmod5) embedding. They are the variants of LSB embedding or LSB based steganographic algorithms. The classification is based on textural features.

It is a well-established fact that features for textural classification has equally been powerful for passive steganalysis in spatial domain Co-occurrence matrix [32], Local Binary Pattern (LBP) [28], Local Texture Pattern (LTP) [5] and hidden markov model [10]. In this paper a combination of textural features-Markov, LDP and Local Filter Pattern (LFP) is proposed for identifying the spatial domain LSB based algorithms. Local Derivative Pattern LDP is used for various applications like Image tampering detection, Camera model identification, Texture Classification. And Local Filter Pattern (LFP) is proposed as a modification of LDP. The authors have

undertaken another step of active steganalysis in finding the estimate of the payload using this feature and have found it useful [30]. The novelty lies in adapting those features to active steganalysis of algorithm detection. The multi class classification is done by combining the binary ensemble FLD classifiers in one against one ensemble fashion. Thus an ensemble of ensemble binary classifiers is proposed as multi class classifier. The highlights of the paper are:

1) Low dimensional combination of groups of features effective for active steganalysis.
2) Study of the proposed simplified, less complex ensemble classifier with various parameter adjustments in stego algorithm identification.

The rest of the paper is organised as follows. Section 2 sketches the basics of the LSB algorithms used, section 3 illustrates the features to be used for classification and the following section 4 explains the multi class classifier model, while section 5 presents the work done and the inferences drawn. Section 6 concludes the paper with scope for future direction.

2. LSB Algorithms

The popular steganographic LSB algorithms frequently employed for embedding and hence for steganalysis are LSBR [14], LSBM [27], LSBMR [20], LSBR2 [15] and LSBRmod5 [18]. The secret data decomposed to bits, occupy the least significant bit of every cover pixel to yield a LSBR stego image, while two bits from the secret payload occupies two least significant bits of a cover pixel to create a LSBR2 stego image. Least Significant Bit(s) substitution algorithms (LSBR and LSBR2), though simple in implementation, suffers from an inherent asymmetry i.e., even pixel values are either unaffected or increased by 1 while the odd pixel values are either unaltered or decreased by 1. To overcome this limitation, LSBM popularly known as ± 1 embedding, randomly either subtracts or adds 1 to the pixel value, if the secret data bit is not the same as that of the LSB of cover image pixel to be embedded. Enhancing this idea, LSBMR performs hiding two bits in a pair of cover pixels as one embedding unit so that pixel change rate is lowered than in case of LSBM. LSBRmod5 embeds in a fashion that when the stego pixel is divided by 5, the remainder will yield the secret digit. The models of the steganographic algorithms considered in this steganalytic work are characterized by Equation (1).

$$\begin{aligned} LSBR(X) &= 2\times\lfloor X/2\rfloor + M \\ LSBM(X) &= 2\times\lfloor X/2\rfloor \pm M \\ LSBMR(X) &= LSBR(f(p,q)) \\ LSBR2(X) &= 4\times\lfloor X/2\rfloor + M \\ LSBR\bmod 5(X) &= \arg\min_{Y \bmod 5 - M} |X - Y| \end{aligned} \tag{1}$$

where X, Y, are pixels ∈ {0,1, ..., 255}, M is the secret message in bits and $f(A,B)$ is the function on pixel pairs A,B. All the LSB based algorithms embed the secret at random location based on key.

3. Features Extracted

Except the block based Steganalytic schemes, almost all others extract features from cover and stego images considering them as whole, the technique being labeled as global feature extraction. This will characterize the embedding distortions on a larger scale. But embedding distortions that occur due to minute payloads need to be searched for, in confined image locations, much smaller than the entire image. This technique is referred to as local feature extraction. This paper proceeds to extract the synergy of both local and global features as a refined tool for active steganalysis.

3.1. Co-occurrence Features from Markov Process

Least significant bits of cover image pixels change their value based on either the value of the secret bit to be embedded or the rule of the embedding algorithm. Such random changes can be effectively captured by a Markov process as it is inherently a probabilistic model which characterizes rule dependent transitions. In this work, a Markov model is employed to model the subtle embedding distortions present in a stego image on a global perspective. Derivatives have been deployed to identify the variations among pixel neighbours. The first order derivative has been observed in eight different directions-two horizontal, two vertical, two major diagonal and two minor diagonal directions. For example, the vertical first order derivatives (top to bottom) of Image, and (bottom to top) are depicted by Equation (2).

$$\begin{aligned} I^{vtb}_{i,j} &= I_{i,j} - I_{i+1,j} \\ I^{vbt}_{i,j} &= I_{i+1,j} - I_{i,j} \end{aligned} \tag{2}$$

The derivatives represent a high pass filtered result which are subsequently thresholded. These thresholded derivatives highlight the embedding distortions caused by LSB embedding algorithms. Equation (3) presents the thresholded first order derivative in the vertical direction from top to bottom. The threshold (T) is considered to be 3 as experimented by Pevny *et al*. [25] for this work. As per the example shown in Equation (3), derivative along the other seven directions have also been obtained.

$$I^{vtb}_{p,q} = \begin{cases} I^{vtb}_{p,q} \; if \; -T \le I^{vtb}_{p,q} \le T \\ 0 \qquad otherwise \end{cases} \tag{3}$$

Co-occurrence matrix characterizes co-occurring values as a probability distribution. Co-occurrence features subjected to a Markov process can identify changes in the textures [25] and can be employed readily for steganalysis as a feature set. The second order Markov

process on the first order vertical thresholded derivative (top to bottom) of the image is given by Equation (4).

$$M^{vtb}_{x,y,z} = \Pr(I^{vtb}_{i+2,j} = x \mid I^{vtb}_{i+1,j} = y \mid I^{vtb}_{i,j} = x) \quad (4)$$

Considering image symmetry and dimensionality reduction, the mean vector of all the eight co-occurrence matrices is computed which forms the first 343D (D stands for dimensionality) features of the proposed feature set F_1 for this work. The mean vector is also computed on co-occurrence matrices of the second order Markov process on the second order derivative and they form the first 343D features of the second feature F_2. Both F_1 and F_2 help to highlight the minute embedding distortions present in the stego images since second order Markov process captures the minor variations that are caused in adjacent pixels by the embedding process.

3.2. Local Derivative Pattern

Inspired by LBP, the able local discriminator, LDP has been employed in this work. LBP limits itself to only first order spatial variations between pixel neighbours. LDP extends to n^{th} order derivative for the local region considered. After computing the n^{th} order derivative for the 3×3 subimage, the center pixel, X_c is set by comparing with the eight neighbours as in Equation (5), the product of the center pixel. If the product is less than 0, then a directional difference is said to exist and the pixel position is represented by a '1', otherwise it is encoded as '0' and the encoding is converted to decimal notation.

$$LDP_B(X'_C) = \sum_{i=1}^{B} f(X'_i) \times 2^{i-1}$$
$$f(X'_i) = \begin{cases} 1 & if \quad X'_i \times X'_C < 0 \\ 0 & otherwise \end{cases} \quad (5)$$

where B=number of neighbours and X' is the nth derivative of pixel X. LDP values lie in the range 0-255 and hence the LDP features are from the 256 bin histogram of the LDP values. As this depends on the ordering of spatial neighbours, rotation invariant LDP has been considered. Solving the dependency on the ordering, this further limits rotation invariant LDPs to have only 36 unique patterns. Grouping them according to the pattern results in a 36D rotation invariant LDP feature. This outperforms LBP in local edge detection [5]. In this work, rotation invariant LDP has been derived from the second order derivative of the stego image.

3.3. Local Filter Pattern

LFP is a simple modification done on LDP by replacing the derivative high pass filters with the custom high pass filters [29, 31]. The motivation behind the work is to employ the soul of steganalysis (i.e.,) custom high pass filter in the mission. The custom high pass filter used in this work is given in Figure 1-a). It is a second order derivative 2D filter. This helps in bringing out the hidden data into view by removing the image content and the process is defined by Equation (6).

$$LFP_B(X''_C) = \sum_{i=1}^{B} f(X''_i) \times 2^{i-1}$$
$$f(X''_i) = \begin{cases} 1 & if \quad X''_i \times X''_C < 0 \\ 0 & otherwise \end{cases} \quad (6)$$

where X'' is the high pass filter output of image X, X''_c is the centre pixel of the local 3×3 window, B=number of neighbours and is 8 if local window of 3×3 is considered and denotes the local neighbours in that window. X''_i denotes the product of $X''_i \cdot X''_c$. An example of LFP is illustrated in Figure 1.

The high pass filter kernel chosen for LFP to steganalysis various LSB based algorithms is depicted in Figure 1-a), the sample subimage X in.

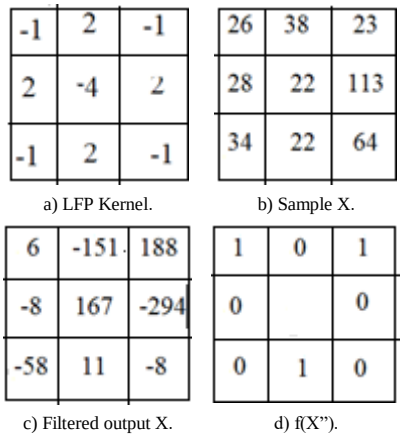


Figure 1. Example to illustrate LFP calculation.

Figure 1-b), the high pass filtered output using kernel is in Figure 1-c) and the encoding f in Figure 1-d). The encoding is explained as below. The first row left element X_1'' '6' is encoded as 0 since X''_c =167 and $X''_i \cdot X''_c$>0 therefore $f(X_1'')$ = 0 and first row second left element X_2'' is '-151' is encoded as 1 since $X''_i \cdot X''_c < 0$. Thus, encoding is done for all neighbours on the local window of high pass filtered output of image X. These are then converted into LFP values using Equation (6).

LFP possesses characteristics common to the LBP and LDP like multi scale and multi resolution exploration as well as uniform, rotation invariant mapping. This work uses only rotation invariant LFP and employs 36D LFP features for the proposed steganalytic mission. The feature sets F_1 and F_2 have been proposed for the steganographic algorithm detection posed as a multiclass classification problem. F_1 and F_2 have been framed by concatenating Markov co-occurrence matrices of first and second order thresholded derivatives with concatenated LDP and LFP features, respectively. As the 36D features of LDP and LFP each add to the Markov features of 343D, the dimensionality for F_1 and F_2 is 415D (= length of Markov (343)+length of rotation invariant LDP (36)+length of rotation invariant LFP (36)).

4. Classifier Model

The multi class classifier is derived from the ensemble FLD classifier proposed by Kodovsky *et al*. [16]. This ensemble FLD classifier is used for binary classification and is shown in Figure 2. The base learners are FLD classifiers. Instead of operating on the whole domain of the feature set, a subspace less than the original is chosen at random. This bootstrap sampling property makes it applicable for even higher dimension feature set without curse of dimensionality. Finally, majority voting of the base learners produce the desired result. Thus, the ensemble FLD binary classifier is a simplified, less complex ensemble classifier which relatively performs as efficient as Support Vector Machine (SVM), yet supports features of high dimension.

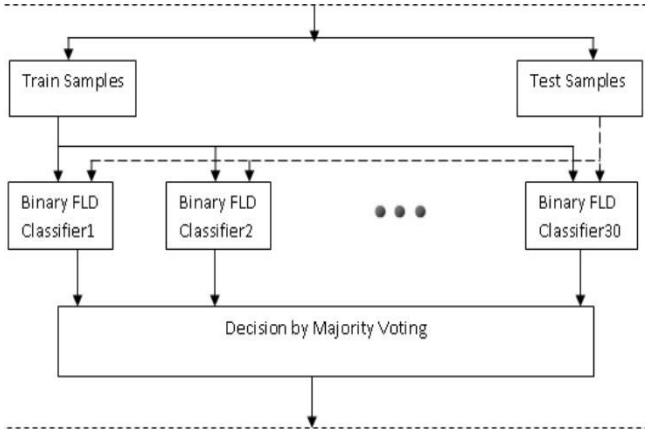


Figure 2. Block diagram of basic ensemble FLD binary classifier.

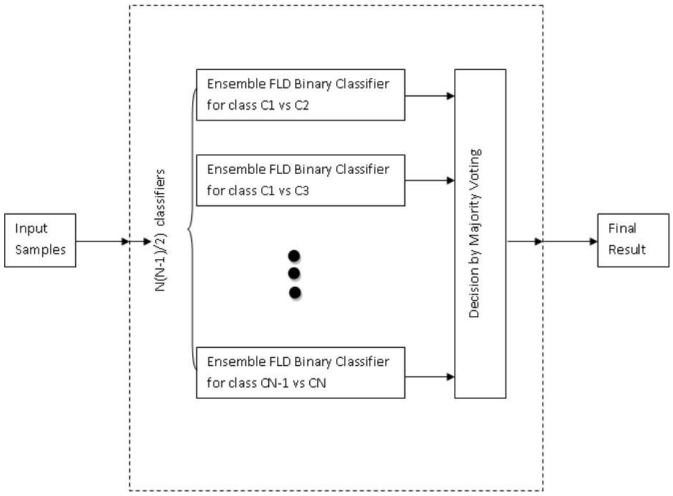


Figure 3. Block diagram of proposed Multi class classifier one against one approach.

In our paper, basic ensemble FLD binary classifier is extended for multi class classification by following the principle of one against one strategy as shown in Figure 3. Let N be the total number of classes and each class be denoted by the label C_i where $i=1,...,N$. Then for each pair of classes, a binary ensemble FLD classifier is constructed, thus yielding a total of $k=N\times(N-1)/2$ ensemble FLD binary classifiers. Let f_k be the decision of k^{th} ensemble FLD binary classifier and $S_i(x)$ be the sum of ensemble FLD binary classifiers that vote x to be of C_i^{th} class. Then the final decision of the one against one ensemble multi class classifier for sample x, $D(x)$, is given by Equation (7).

$$D(x) = \underset{i=1,2,..N}{\arg\max} \; S_i(x)$$
$$S_i(x) = \#\{k \mid f_k(x) = C_i\} \tag{7}$$

The bootstrapping of the sample is left out, since our feature set is relatively low dimensional and number of base learners is limited to 30. This is because classification accuracy saturates with number of base learners [16], further increase does not improve accuracy while at the same time increases the run time of the task. Thus, a fast efficient multi class ensemble of ensemble classifier is constructed.

5. Experimental Results and Discussions

The main goal of the work is to present a low complex steganalysis feature for active steganalysis of commonly used (LSB based) steganography in spatial domain of grayscale images. To enrich the study, LSB based spatial domain algorithms LSBR, LSBM, LSBMR, LSBR2, and LSBRmod5 embedding with eight different payloads 0.1-0.4 bpp(bits per pixel) in steps of 0.1 bpp and 0.25-1.0 bpp in steps of 0.25 bpp are chosen. Since LSBR2 and LSBRmod5 have different embedding capacity than that of other LSB algorithms, a uniform embedding change rate is chosen. Thus the corresponding embedding changes for payload of 1.0 bpp are 100% for first three algorithms and 50% for LSBR2 and 43% for LSBRmod5 algorithms respectively.

A well-established cover database for steganalysis-Bossbase version 1.01 [3] is chosen. Out of the 10,000 grayscale images, for simplicity only first 1000 images are chosen for building the steganographic database. These 1000 images form the cover images. Then 1000 stego images are formed for each algorithm and each payload using these cover images. Thus a total of (1000 x 8 payloads) 8000 stego images are formed for each of the stego algorithm using random data of required payloads. Thus, total stego images created are 40,000 images (1000 x 8 payloads x 5 algorithms). The train test ratio for the experimentation is fixed as 50%, i.e. Random 500 images of each cover and stego images of each payload (total 500 cover and 2500 (500x5 algorithms) stego images) are trained using the proposed ensemble multi class classifier and the remaining unseen images are tested. The statistics for all the experiments are collected after 10 fold cross validation. A model that exhibits small variance and high bias will underfit the target, while a model with high variance and little bias will overfit the target. There is a bias-variance trade-off associated with the choice of k in k-fold cross validation. Typically, given these considerations, one performs k-fold cross-validation using k=5 or k=10, as these values have been

shown empirically to yield test error rate estimates that suffer neither from excessively high bias nor from very high variance [12]. This is because as *k* becomes larger, the difference in size between the training set and the resampling subsets gets smaller. As this difference decreases, the bias of the technique becomes smaller [17]. Therefore to get a better model, *k*=10 is chosen. To compare the proposed steganalyser, comparison is done here in two ways. First the proposed features are tested against the State of Art LSB steganalysis feature set SPAM. This is done by running their code available on the database and classification by our ensemble classifier. The dimensionality of extracted SPAM features is 686D [25]. Second the proposed method is compared against different classifiers and feature sets as existing in literature.

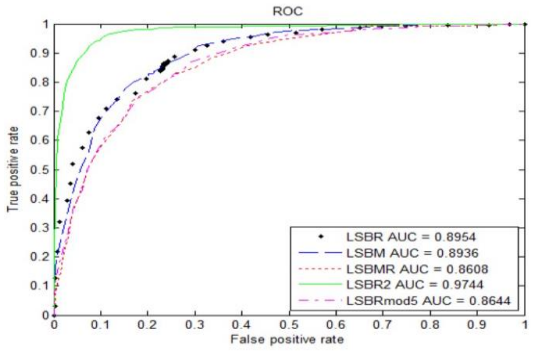
5.1. Analysis of Performance in Binary Classification

The effectiveness of the proposed features are proved by testing their efficiency in binary classification (Cover vs Stego). The results are shown by the Receiver Operator Characteristics (ROC) plot for the payload of 0.1 bpp in Figure 4 The accuracy P_A of the binary ensemble FLD is calculated as in Equation (8).

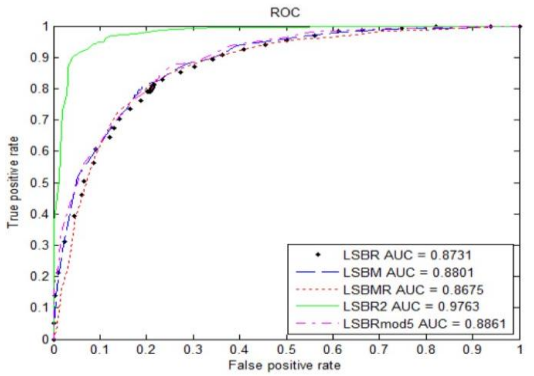
$$P_A = 1 - P_E$$
$$P_E = \min\left(\frac{1}{2} P_{FA} + P_{MD}(P_{FA})\right) \quad (8)$$

where P_E is the error probability, P_{FA} is the false alarm probability and P_{MD} is missed detection probability.

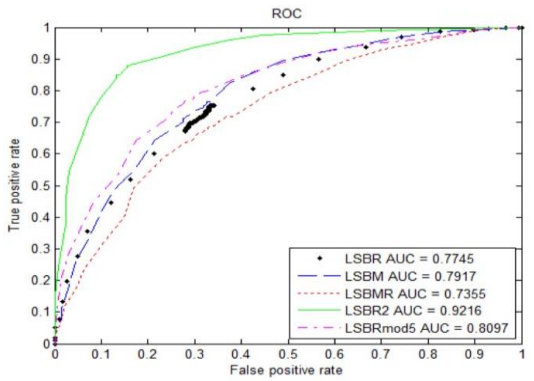
It can be clearly noted that our proposed features are a way better than SPAM features in detecting the algorithms in terms of accuracy and dimensionality. This is because of the proposed local features. The local features suppress the image content while at the same time, the payload embedded values (differences) are brought out by local pattern formed. Also, between our features F_1 and F_2, it can be noted though they perform equally, F_2 features performs better than F_1 for LSBMR and LSBmod5 embedding and F_1 performs better for LSBR and LSBM at low payload.



a) Proposed feature set F_1.



b) Proposed feature set F2.



c) SPAM.

Figure 4. ROC Curve of binary classification of various LSB based Algorithms using different feature sets.

5.2. Analysis of Performance in Multi Class Classification

The work of multi class classification is divided into three. The first work experiments the discrimination power of the proposed features sets F_1 and F_2 in multi class classification for a fixed payload. The second work continues the process for a variable payload and various groupings of LSB algorithms. Finally, the efficiency of the classifier is tested against other multi class classifier.

1) Analysis of Performance for Fixed Payload

Here cover and stego images from all the five above said algorithms are considered and the payload is fixed as 1.0 bpp. The confusion matrices for the multi class classification are given through Tables 1, 2, and 3.

Table 1. Confusion Matrix for LSB based algorithms for 1 bpp payload using feature set F_1.

Embedding Algorithm	Classified as					
	Cover	LSBR	LSBM	LSBMR	LSBR2	LSBRmod5
Cover	475	1	0	24	0	0
LSBR	1	491	6	2	0	0
LSBM	7	3	458	31	0	1
LSBMR	2	9	41	447	0	1
LSBR2	0	0	1	0	497	2
LSBRmod5	0	0	0	1	1	498

Table 2. Confusion Matrix for LSB based algorithms for 1 bpp payload using feature set F_2.

Embedding Algorithm	Classified as					
	Cover	LSBR	LSBM	LSBMR	LSBR2	LSBRmod5
Cover	476	1	0	22	0	1
LSBR	0	486	10	1	0	2
LSBM	2	4	443	39	2	10
LSBMR	6	4	48	435	0	7
LSBR2	0	0	1	0	497	2
LSBRmod5	6	1	8	13	2	470

Table 3. Confusion Matrix for LSB based algorithms for 1 bpp payload using SPAM.

Embedding Algorithm	Classified as					
	Cover	LSBR	LSBM	LSBMR	LSBR2	LSBRmod5
Cover	452	2	7	36	3	0
LSBR	2	489	0	3	6	0
LSBM	13	0	426	57	4	0
LSBMR	30	5	63	398	4	0
LSBR2	1	1	1	1	496	0
LSBRmod5	1	0	0	0	0	499

Table 1 signifies that out of the 500 cover images and 2500 stego images (500 stego images for each algorithm) considered for testing, first row signifies 475 out of the 500 cover images are correctly identified as cover (1 is identified as LSBR stego image and 24 as LSBMR stego images - misclassification). In second row 1 out of 500 LSBR stego images tested is misclassified as cover, 491 are correctly classified as LSBR stego images and so on.

A LSBR stego image *(S)* is created by adding noise *(P)* (payload) to the cover image *(C)* i.e., $S=C+P$. Say our pixel is 30 then the LSB is 0, and if and only if payload is 1, the bit is altered otherwise the pixel remains unchanged though a payload (0 bit) of 1 bit has been embedded. In an image after embedding 100% payload on average only 50% of the pixel will be altered. And if payload is low, then more pixels remain unaltered (resembling cover). This is the reason for a stego LSB image to be classified as cover image.

Similarly, in LSBR image say a pixel of intensity 30 is either converted to 31 or stays at 30 (+1 noise addition) while in LSBMR it is ± 1 which means it can be 29, 30, or 31. The choice to add or subtract is purely random and if by random choice there are more +1s then LSBMR image resembles LSBR image. Therefore, it is likely possible to have a LSBR image sometimes recognised as LSBMR image. Also, LSBR2 is two bit version of LSBR therefore it is common to have same LSB resulting in misclassification. Similar explanation can be provided for other rows and tables. It can be noted that for high payloads, F_1 features are better in discriminating algorithms LSBR, LSBR2, LSBRmod5 and F_2 features perform moderately compared to F_1. Payload in LSB Steganography is in a way additive noise and for steganalysis, the payload detection must be devoid of image content including edges. F_1 is better in discriminating because it is built using first order differences. And first order differences are sensitive to noises and therefore capture LSB embeddings (payload) in spite of image content. Therefore, F_1 features are more discriminating. The second order differences capture the edges (image content rather than hidden payload) Therefore F_2 is less discriminating than F_1. Also, the embedding pattern (capacity) of LSBR2, LSBRmod5 are different while that of LSBR, LSBM and LSBMR are same. It is also the reason why those algorithms are more discriminative. However, SPAM features are the best for LSBR2 and LSBRmod5 algorithms because of the global nature of capturing major pixel variations.

2) Analysis of Performance in Different Groups and Payloads

In this section, Multi classification is done by grouping stego images of different algorithms for all payloads. Various groups are considered for the sake of comparison with the existing methods. The three different groups are considered - First group, G_1 consists of the cover, stego images from LSBR, LSBM and LSBMR algorithms, the second group G_2 covers the cover and LSBR, LSBM, LSBR2 and LSBmod5 stego images and the last group G_3 consists of images from all the above said algorithms. G_1 consists of algorithms which are widely used in steganography, G_2 is considered for comparison with one existing literature and G_3 is the sum total of all algorithms considered. The results are tabulated as in Table 4.

It can be seen that irrespective of the payload, G_1 is difficult to detect while second group, G_2 is the easiest to detect. Thus, embedding in the second LSB paves way for easier detection, even for the same payload. Also, it can be seen that the discriminating nature of the algorithms helps in multi class classification accuracy, while similar algorithms produce results with less accuracy.

Table 4. Multi class Detection Accuracy for LSB based algorithms for different groups and payloads in percentage.

Payload (bpp)	Proposed Feature Set F_1			Proposed Feature Set F_2			SPAM		
	G_1	G_2	G_3	G_1	G_2	G_3	G_1	G_2	G_3
0.1	51.69	61.34	54.44	53.32	64.4	57.69	44.89	54.98	49.05
0.2	68.68	77.54	70.49	69.26	78.91	72.25	61.2	71.23	63.92
0.25	73.37	81.86	75.25	73.89	83.19	76.5	66.2	76.4	68.98
0.3	76.81	84.74	78.39	77.24	85.73	80.01	69.43	80.02	72.5
0.4	81.05	89.72	83.29	81.31	89.37	83.71	74.9	85.5	78.35
0.5	84.7	92.69	87.19	84.54	91.82	86.80	78.42	82.86	86.24
0.75	90.09	97.06	92.71	89.73	94.77	90.79	85.13	94.94	89.36
1	93.2	98.34	95.08	92.29	96.36	93.14	88.56	96.94	91.85

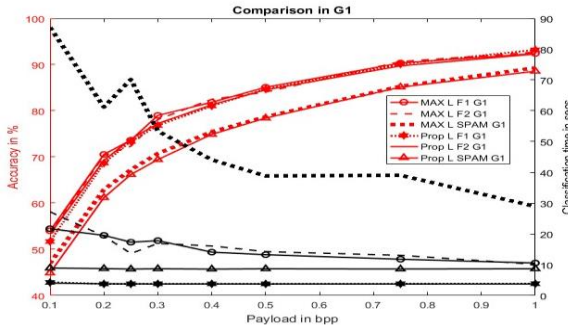
For the proposed feature sets, it can be seen that second feature set F_2 is better for low volume payloads,

while the first set F_1 is better for higher payload. Clearly both methods are a way ahead of SPAM in accuracy and dimensionality.

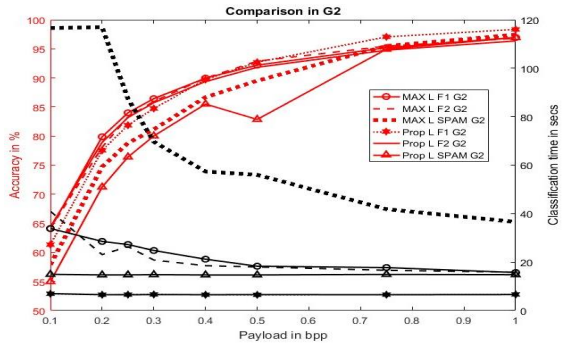
3) Effect of Parameters on the Performance

This section tries to study the effect of number of base learners parameter (L) on the performance. The experiment is conducted for various L values and the minimum out-of-bag estimate is obtained [16]. And maximum L reported in multi classification is reported as Max L method. This method is compared against the proposed method with fixed (30) base learners (Prop L) and the result for different groups and payloads are reported in Figure 5.

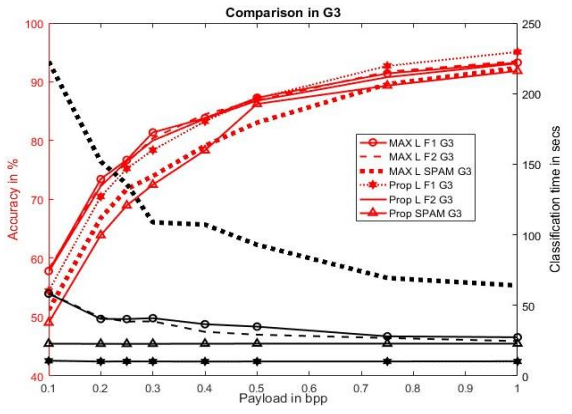
Figure 5 depict the plots between accuracy, classification time against payload for both Max L and Prop L for groups G_1, G_2 and G_3 using all three feature sets F_1, F_2 and SPAM.



a) Group G1.



b) Group G2.



c) Group G3.

Figure 5. Comparison Plot depicting the variation of Accuracy (primary Y axis) and Time taken for classification (secondary Y axis) with various payloads.

Considering the performance of proposed feature sets in G_1 (Figure 5-a), very little difference in accuracy (red ones) is detected using the both Max L and Prop L methods. However, in terms of time in secondary y axis (black ones), Prop L takes nearly 3 to 6 times lesser time than the Max L method. The same effect can be seen in other groups also (Figure 5-b and Figure 5-c). This justifies the fact that accuracy saturates with increasing L and increased L leads to additional cost of time and complexity. On comparison with SPAM clearly in group G_1, the proposed features excel them for all payloads and in G_2 and G_3 for low payloads. An equivalent performance of SPAM is seen in G_2 *and* G_3 for payload greater than 0.5 yet, the best accuracy and time is obtained by the proposed feature F_1 in Prop L method.

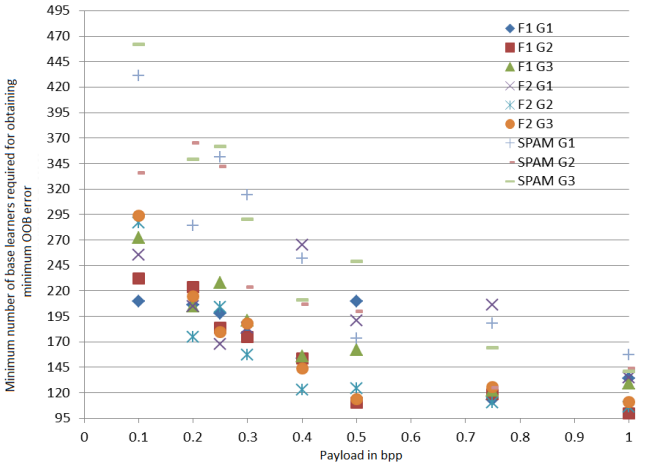


Figure 6. Scatter Plot depicting the maximum number of base learners used for each multi classification using different feature sets, groups and payloads in Max L method.

Another feature notable in time, payload plot (black ones) is that Max L method takes more time for classifying low payloads and drastically decreases for high payload, while the classification time in Prop L method is nearly linear in all groups and feature sets. The maximum number of base learners used for each one against one classification is given as a scatter plot in Figure 6. The figure clearly demonstrates the optimacy of the proposed parameter L. Thus, the proposed method with fixed number of learners (Prop L) using proposed features proves to be an efficient low dimensional multi class steganalysis.

4) Analysis of Performance against other Existing Works

To compare our proposed steganalyser, two methods are considered. One is the existing method proposed by Lubenko and ker [18] (results reported as in paper; version of database and number of images vary) which employs a standard feature set with their Logistic regression classifier. The paper compares both linear and kernelised version of classifier of various classifiers like SVM Smooth SVM and Logistic Regression (LR) in Bossbase and the results reported for multi class classification are taken as such for comparison. Since the

paper reports results only for 0.5 bpp payload, also 0.5 bpp is the mid payload, therefore the results are reported for the same to have an equivalent comparison. The other is the multi class classifier from WEKA [8]. In case of Weka, the multi class classifier is a one against all concept-oriented classifier. The results are taken by conducting the experiments for the same database with our proposed feature sets with Weka v3.7. The parameter for the multi class classifier is set as to default. The comparison results of the proposed method against WEKA for other payloads is given by Figure 7.

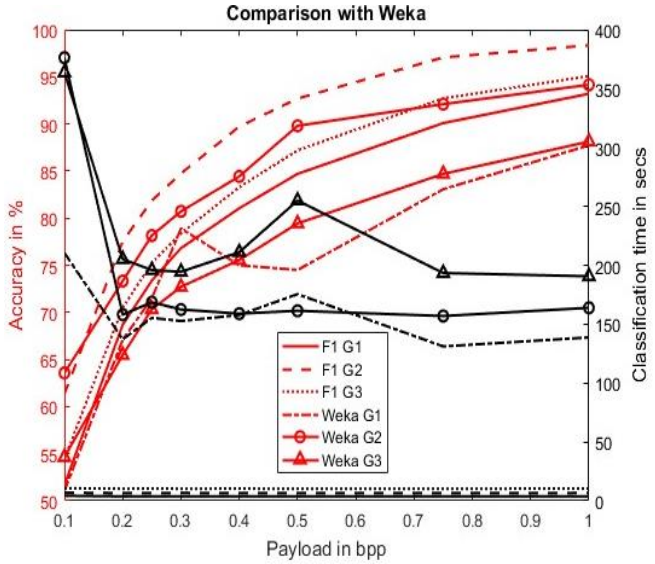


Figure 7. Comparison Plot against weka depicting the variation of Accuracy (primary Y axis) and Time taken for classification (secondary Y axis) with various payloads.

Table 5. Comparison Table for accuracy and time with different classifiers for payload of 0.5 bpp.

Classifier	Class group	Accuracy (percentage)	Time (sec)
Proposed Ensemble Multi class classifier	G_1	84.7	6.78
Lubenko Kernelised LR	G_1	-NA-	-NA-
Weka	G_1	82.75	179.38
Proposed Ensemble Multi class classifier	G_2	92.69	11.54
Lubenko Kernelised LR	G_2	82.3	23446
Weka	G_2	89.8	237.99
Proposed Ensemble Multi class classifier	G_3	87.19	17.86
Lubenko Kernelised LR	G_3	-NA-	-NA-
Weka	G_3	84.43	435.86

As seen from Table 5 and Figure 7 the proposed ensemble Multi class classifier is better than existing ones in terms of time and accuracy.

6. Conclusions

With performed experiments, it can be concluded that the proposed low dimensional feature sets for detecting the LSB steganographic algorithms is novel and effective compared to SPAM. They are composed of both global and local features which effectively discriminates the LSB based algorithms used. Also, the proposed steganalyser using an ensemble (one against one) approach of ensemble binary FLD classifiers is effective for the multi class classification of LSB based algorithms in spatial domain. The determination of other effective textural features for adaptive steganographic scheme also is the scope for future research work.

References

[1] Arivazhagan S., Amrutha E., Jebarani W., and Veena S., "Hybrid Convolutional Neural Network Architecture Driven by Residual Features for Steganalysis of Spatial Steganographic Algorithms," *Neural Computing and Applications*, vol. 33, no. 17, pp. 11465-11485, 2021. https://doi.org/10.1007/s00521-021-05837-7

[2] Arivazhagan S., Jebarani W., Veena S., and Amrutha E., "Extraction of Secrets from LSB Stego Images Using Various Denoising Methods," *The International Journal of Information Technology*, vol. 15, pp. 2107-2121, 2023. https://doi.org/10.1007/s41870-023-01265-z

[3] Bas P., Filler T., and Pevný T., "Break our Steganographic System": The Ins and Outs of Organizing BOSS," *in Proceedings of the Information Hiding 13th International Conference*, Prague, pp. 59-70, 2011. https://doi.org/10.1007/978-3-642-24178-9_5

[4] Bogacsovics G., Toth J., Hajdu A., and Harangi B., "Enhancing CNNs through the Use of Hand-Crafted Features in Automated Fundus Image Classification," *Biomedical Signal Processing and Control*, vol. 76, pp. 103685, 2022. https://doi.org/10.1016/j.bspc.2022.103685

[5] Chen J., Lu W., Fang Y., Liu X., and Yeung Y., "Binary Image Steganalysis Based on Local Texture Pattern," *Journal of Visual Communication and Image Representation*, vol. 55, pp. 149-56, 2018. https://doi.org/10.1016/j.jvcir.2018.06.004

[6] Feng G., Zhang X., Ren Y., Qian Z., and Li S., "Diversity-Based Cascade Filters for JPEG Steganalysis," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 2, pp. 376-86, 2020. doi: 10.1109/TCSVT.2019.2891778

[7] Figueroa A., "Refining Fine-Tuned Transformers with Hand-Crafted Features for Gender Screening on Question-Answering Communities," *Information Fusion*, vol. 92, pp. 256-67, 2023. https://doi.org/10.1016/j.inffus.2022.12.003

[8] Frank E., Hall M., and Witten I., *The WEKA Workbench Online Appendix for Data Mining Practical Machine Learning Tools and Techniques*, Morgan Kaufman, 2016. https://www.cs.waikato.ac.nz/ml/weka/Witten_et_al_2016_appendix.pdf

[9] Fridrich J. and Kodovsky J., "Rich Models for Steganalysis of Digital Images," *IEEE Transactions on Information Forensics and*

Security, vol. 7, no. 3, pp. 868-882, 2012. doi: 10.1109/TIFS.2012.2190402

[10] Gul G. and Kurugollu F., "JPEG Image Steganalysis Using Multivariate PDF Estimates with MRF Cliques," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 578-87, 2013. doi:10.1109/TIFS.2013.2247399

[11] Holub V., Fridrich J., and Denemark T., "Random Projections of Residuals as an Alternative to Co-Occurrences in Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1996, 2013. DOI:10.1109/TIFS.2013.2286682

[12] James G., Witten D., Hastie T., and Tibshirani R., *An Introduction to Statistical Learning with Applications*, Springer New York, 2021. https://link.springer.com/book/10.1007/978-1-4614-7138-7

[13] Jin Z., Feng G., Ren Y., and Zhang X., "Feature Extraction Optimization of JPEG Steganalysis Based on Residual Images," *Signal Processing*, vol. 170, pp. 107455, 2020. https://doi.org/10.1016/j.sigpro.2020.107455Get righ

[14] Johnson N. and Jajodia S., "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, pp. 26-34, 1998. doi: 10.1109/MC.1998.4655281

[15] Ker A., "Steganalysis of Embedding in Two Least-Significant Bits," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 46-54, 2007. DOI:10.1109/TIFS.2006.890519

[16] Kodovsky J., Fridrich J., and Holub V., "Ensemble Classifiers for Steganalysis of Digital Media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432-44, 2012. doi:10.1109/TIFS.2011.2175919

[17] Kuhn M. and Johnson K., "Over-Fitting and Model Tuning," *Applied Predictive Modeling*, Springer, 2013. https://doi.org/10.1007/978-1-4614-6849-3_4

[18] Lubenko I. and Ker A., "Steganalysis Using Logistic Regression," *Media Watermarking Security and Forensics III*, vol. 7880, pp. 193-203 2011. https://doi.org/10.1117/12.872245

[19] Luo W., Dang J., Wang W., and Zhai F., "Low-Complexity JPEG Steganalysis Via Filters Optimation from Symmetric Property," *Multimedia Systems*, vol. 27, no. 3, pp. 371-377, 2021. https://doi.org/10.1007/s00530-021-00780-y

[20] Mielikainen J., "LSB Matching Revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006. doi: 10.1109/LSP.2006.870357

[21] Muralidharan T., Cohen A., Cohen A., and Nissim N., "The Infinite Race between Steganography and Steganalysis in Images," *Signal Processing*, vol. 201, pp. 108711, 2022. https://doi.org/10.1016/j.sigpro.2022.108711

[22] Nouisser A., Zouari R., and Kherallah M., "Deep Learning Based MobileNet and Multi-Head Attention Model for Facial Expression Recognition," *The International Arab Journal of Information Technology*, vol. 20, no. 3A, 2023. https://doi.org/10.34028/iajit/20/3A/6

[23] Pevny T., Bas P., and Fridrich J., "Steganalysis by Subtractive Pixel Adjacency Matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215-224, 2010. doi:10.1109/TIFS.2010.2045842

[24] Pevný T. and Fridrich J., "Towards Multi-Class Blind Steganalyzer for JPEG Images," *The International workshop on Digital Watermarking*, vol. 3710, pp. 39-53, 2005. https://doi.org/10.1007/11551492_4

[25] Pevný T. and Fridrich J., "Multi-Class Blind Steganalysis for JPEG Images," *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072. pp. 257-269, 2006. https://doi.org/10.1117/12.640943

[26] Priyadharshini R., Arivazhagan S., and Arun M., "Crack Recognition on Concrete Structures Based on Machine Crafted and Hand Crafted Features," *Expert Systems with Applications*, vol. 228, pp. 120447, 2023. https://doi.org/10.1016/j.eswa.2023.120447

[27] Sharp T., "An Implementation of Key-Based Digital Signal Steganography," *The International Workshop on Information Hiding*. pp. 13-26, 2001. DOI:10.1007/3-540-45496-9_2

[28] Shi Y., Sutthiwan P., and Chen L., "Textural Features for Steganalysis," *Information Hiding, 14th International Conference*, Berkeley, pp. 63-77, 2013. https://doi.org/10.1007/978-3-642-36373-3_5

[29] Veena T. and Arivazhagan S., "Universal Secret Payload Location Identification in Spatial LSB Stego Images," *Annals of Telecommunications*, vol. 74, no. 5, pp. 273-286, 2019. https://doi.org/10.1007/s12243-018-0676-x

[30] Veena T. and Arivazhagan S., "Quantitative Steganalysis of Spatial LSB Based Stego Images Using Reduced Instances and Features," *Pattern Recognition Letters*, vol. 105, pp. 39-49, 2018. https://doi.org/10.1016/j.patrec.2017.08.016

[31] Veena T. and Selvaraj A., "Local Descriptor Based Steganalysis of Spatial LSB Variant Stego Images," *in Proceedings of the International Conference on Computation*, Karaikudi, 2016. https://www.researchgate.net/publication/311927921_Local_descriptor_based_

[32] Wang L., Xu Y., Zhai L., Ren Y., and Du B., "A Posterior Evaluation Algorithm of Steganalysis Accuracy Inspired by Residual Co-Occurrence Probability," *Pattern Recognition*, vol. 87, pp. 106-17, 2019. https://doi.org/10.1016/j.patcog.2018.10.003

[33] Xie G., Ren J., Marshall S., Zhao H., and Li R., "Self-Attention Enhanced Deep Residual Network

for Spatial Image Steganalysis," *Digital Signal Processing*, vol. 139, pp. 104063, 2023. https://doi.org/10.1016/j.dsp.2023.104063

[34] Yang L., Men M., Xue Y., Wen J., and Zhong P., "Transfer Subspace Learning Based on Structure Preservation for JPEG Image Mismatched Steganalysis," *Signal Processing: Image Communication*, vol. 90, pp. 116052, 2021. https://doi.org/10.1016/j.image.2020.116052

[35] Yelchuri R., Dash J., Singh P., Mahapatro A., and Panigrahi S., "Exploiting Deep and Hand-Crafted Features for Texture Image Retrieval Using Class Membership," *Pattern Recognition Letters*, vol. 160, pp. 163-71, 2022. https://doi.org/10.1016/j.patrec.2022.06.017

[36] Zavalsız M., Alhajj S., Sailunaz K., Ozyer T., and Alhajj R., "A Comparative Study of Different Pre-Trained Deep Learning Models and Custom CNN for Pancreatic Tumor Detection," *The International Arab Journal of Information Technology*, vol. 20, no. 3A, 2023. https://doi.org/10.34028/iajit/20/3A/9

Veena Sivasamy Thanasekaran received her B.Sc degree in Computer Science from Madurai Kamaraj University in 1995, her M.C.A degree in Computer Applications from Alagappa University in 2001, her M.E degree in Computer Science and Engineering from Anna University in 2010 and her Ph.D in Information and Communication Engineering. Her interests include Steganalysis, Digital Image Processing, Steganography, Visual Cryptography, Pattern Recognition. She is a member in IETE.

Arivazhagan Selvaraj is currently a professor in the ECE Department and Principal of Mepco Schlenk Engineering College, Sivakasi. He has 38 years of teaching and research experience. He has been awarded Young Scientist Fellowship by TNSCST, Chennai in 1999. He has published more than 250 technical papers in international/national journals and conferences. Also, he has completed 15 Research and Development Projects, funded by various organizations. His current research interests include Machine Learning, Biometric System, Digital Image Processing, Steganography, Steganalysis, and Digital Electronics.