I J C T A, 8(5), 2015, pp. 1927-1938

An Optimized Low Volume Blind Universal Steganalyzer with improved Generalization

S. Arivazhagan[1], W. Sylvia Lilly Jebarani [1], S.T. Veena[1]

Abstract: *Background*: Generic Steganalysis proves to be a boon when there is a suspicion of covert channels with no other information regarding stego images. With the advent of sophisticated steganographic techniques, the process becomes tough as the hidden data is very meager and leaves undecipherable artifacts. A Universal, Blind and Statistical Steganalyzer needs to be more generalized as it encounters unseen stego images created out of any steganographic software working in spatial/transform domain altering any type of feature of the cover image. Also it needs to provide more detection accuracy for the next phase of active steganalysis to proceed successfully. *Objective*: This paper proposes mixed blind generic classification which attempts to improve the generalization of the classifier. The designed Steganalyzer makes use of hybrid composite / concatenated feature set along with a Sequential Minimal Optimisation (SMO) classifier to set aside stego images from that of cover images. Feature selection based on F-Score has been employed for this work to address the dimensionality problem. *Results*: Comparison of the obtained results show the efficiency of our approach over SPAM features, the benchmark standard for Steganalysis. *Conclusion*: Thus a Mixed Blind Universal Steganalyser encompassing a multitude of features with effective feature selection is presented for generalized classification of low volume payloads.

Article history: *Received X X 201XReceived in revised form X X X 201X Accepted X X 201X*

Keywords: *Blind Generic SteganalysisLow Volume PayloadFeature Selection*

1. INTRODUCTION

Steganographers in a desire to totally cover their covert channel, resort to low volume embedding. Also raw / uncompressed cover formats rather than JPEG is the most popular form of image encoding since embedding in JPEG causes a number of coefficients to be modified in embedding a single bit (Lyu and Farid, 2006). Due to these facts, the embedding artifacts become too feeble to be noticed and do not render themselves towards identification of stego images. In addition, LSB embedding and their variations do not alter 50% of the cover data even after embedding of secret message (Ker, 2005). The Embedding Change Rate (ECR) parameter when defined for a JPEG image for the same amount of secret data embedded is far higher compared to a bmp(or any other raw, uncompressed format) image (Fridrich et al., 2001). Given all these conditions to prevail in a steganalytic scenario, the number of commercial steganographic algorithms that are getting released are also on the rise (Ker, 2005). A Universal steganalyzer which has been trained to detect only a handful of steganographic algorithms, once commissioned may have to face stego images created with new, unseen steganographic software. Hence the steganalyzer designed should address all these issues namely; working with raw, uncompressed images that have been embedded with a very minimal payload and to have a training phase with samples from stego images created by a single steganographic algorithm.

1.1. Literature Survey

Steganalytic attempts have been made throughout since the advent of digital steganographic techniques. Avcibaş et al., (2002) used the fact that the binary texture characteristics within the bit planes as well as

[1] Department of Electronics and Communication, MEPCO Schlenk Engineering College, Sivakasi, Tamilnadu, India.

correlation between the bit planes will differ between a stego image and a cover image. They employed seventh and eighth bit planes in an image for the computation of binary similarity measures. Avcibas et al., (2003) also used the hypothesis that steganographic schemes leave statistical evidence and exploited that for stego detection with Image Quality Metrics (IQMs) and multivariate regression analysis. Geetha et al., (2009) refined the process by making the IQMs content independent aiming at maximizing the sensitivity and specificity of the Steganalyzer.

Zhang and Ping, (2003) used the translation coefficients between difference image histograms to discriminate the stego image from the carrier image. Harmsen and Pearlman, (2003) in their work on detecting additive noise modelable information hiding schemes like, LSB, Spread Spectrum and DCT hiding methods have shown that these embedding methods are equivalent to a low pass filtering of histograms that is quantified by a decrease in the Histogram characteristic function Center of mass. Xuan et al., (2005) proposed an image steganalytic scheme based on statistical moments of histogram of multi-level wavelet subbands. Shi et al., (2005) optimized the work and later included prediction for content independency. Dong and Tan, (2008) proposed a blind image steganalyzer where higher order statistics of characteristic functions of three types of run-length histograms are used along with SVM.

Holotyak et al., (2005) estimated stego signal by considering the fact that features employed for Steganalysis must be sensitive to embedding modifications and insensitive to image content. Goljan et al., (2006) used higher order absolute moments of the noise residual calculated in the wavelet domain as features for the blind steganalyser. Zou et al., (2006) thresholded the prediction error images since the larger values represent image content and modeled the prediction error images using Markov chain. An empirical transition matrix calculated after thresholding served as the feature for Steganalysis. Shi et al., (2007) used the same technique to decorrelate the absolute values of Block DCT coefficients along horizontal, vertical and diagonal directions. Gou et al., (2007) employed three sets of statistical features obtained from denoising operations, wavelet analysis and neighborhood prediction for distinguishing digital images from their tampered or stego versions. Pevny et al., (2010) generalized this procedure and referred to it as Subtractive Pixel adjacency Matrix. Cho et al., (2013) differentiated a stego image from its cover image inspecting decomposed image blocks of DCT coefficients by exploiting the homogeneous characteristics of image blocks.

Wen-Nung Lie and Guo-Shiang Lin, (2005) pointed out randomization of LSB plane, gray level changes between groups of pixels and variation of transform domain coefficients as the statistical pointers for detection of hidden messages. The authors used Gradient Energy and Statistical Variance of the Laplacian parameter as features for Steganalysis wherein they emphasized on a combination of features extracted in different domains. Lyu and Farid, (2006) exploited the fact that within multiscale, multiorientation image decompositions, first and higher order magnitude and phase statistics are relatively consistent, but are disturbed by the presence of embedded hidden messages. The authors also declared that the chance of detection falls as the message size becomes smaller i.e., messages utilizing approximately 5% of the cover are unlikely to be detected. Savoldi and Gubian, (2007) presented a multi class steganalytic system based on high-order wavelet statistics and clustering approach. Gul and Kurugollu, (2010) developed a Universal Steganalyzer by modeling linear dependencies of image rows / columns in local neighborhoods using singular value decomposition transform and also enabled content independency by a wiener filtering process. Luo et al., (2011) computed features from wavelet coefficient subbands, the prediction subbands of wavelet coefficients, the prediction error subbands of wavelet coefficients, the wavelet subband coefficients of image noise and the log prediction error subbands of wavelet coefficients. They declared that the CF moments outperform PDF moments except for the features derived from log prediction error subbands of wavelet coefficients. Zong et al., (2012) proposed a blind JPEG steganalytic method based on inter and intra wavelet subband correlations.

Fridrich et al., (2003) developed a blind feature based steganalytic method for JPEG images. She calculated every feature as the L1 norm of the difference between a specific functional of the stego image and its cropped / recompressed version wherein this 'calibration' decreased image-to-image variations. Gul and Kurugollu, (2013) addressed the blind steganalysis by modeling the correlations among the DCT coefficients using k-variate pdf estimates constructed by means of Markov Random Field (MRF) cliques. Holub and Fridrich, (2013) used higher order cooccurrence to detect steganographic changes better as they can capture dependencies across multiple pixels. Also an entire family of noise residuals has been made use of, referred to as rich image representation. Pathak and Selvakumar, (2014) extended the concept of image calibration proposed by Fridrich in a dilation process and employed statistical features from spatial, frequency and wavelet domains for Steganalysis. Goljan et al., (2015) proposed a high dimensional feature model to steganalyse a variety of spatial domain algorithms for colour images.

2. PROPOSED METHODOLOGY

The Steganalyzer is designed to work as Universal (Generic) / Blind / Passive Steganalyser where the given test image is declared to be a cover or stego image. The Steganalyzer is referred to as Universal (Generic) as the process accepts stego images created by any steganographic algorithm and differentiates them from clean, unadulterated images and proceeds no further. The process is blind in the sense that the steganalytic procedure will not require cover images as well as any detail pertaining to steganographic algorithms employed in the generation of stego images. The process is also passive since the extraction of embedded secret is not the scope of this paper. The design of this phase is critical as this saves the time of the Steganalyst in proceeding with active steganalysis in estimating the length of the message embedded, location of the message etc. With this information, the steganalyst can extract the hidden secret message once the tool used to hide the payload is known.

2.1. Mixed Blind Generic steganalysis

Normally, the Generic Steganalysis works by training the cover and stego image of one particular tool and recognizing the cover and stego images of only that tool. Thus a total of *n* steganalysers are needed for detecting stego images from *n* tools. In the proposed approach, which is aimed at improving the generalization of the Generic steganalyzer, a single steganalyzer is trained with cover and stego images created by a single tool but tested with a set framed from cover images and stego images created with all the steganographic tools. Thus the schematic representation of the mixed blind generic steganalyser is shown in Fig. 1.

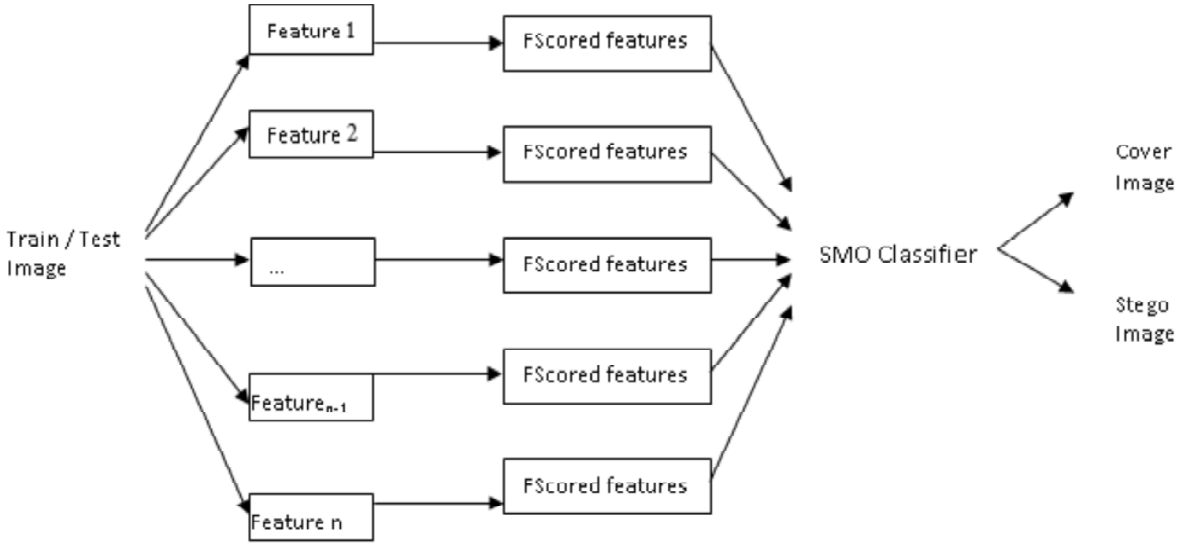


Figure 1: Proposed Mixed Blind Generic Steganalyser

2.2. Feature Selection

F-Score: F-score is a simple technique which measures the discrimination of two sets of real numbers. Given training vectors x_k, $k = 1, \ldots, m$, if the number of positive and negative instances are n_+ and n_-, respectively, then the F-score of the ith feature is defined as in Eqn. 1

$$F(i)=\frac{(\overline{X}_i^{(+)}-\overline{x}_i)^2+(\overline{X}_i^{(-)}-\overline{x}_i)^2}{\frac{1}{(n_+-1)}\sum_{k=1}^{n+}X_{k,i}^{(+)}-\overline{x}_i^{(+)})^2+\frac{1}{(n\_-1)}\sum_{k=1}^{n-}(X_{k,i}^{(-)}-\overline{x}_i^{(-)})^2+} \quad (1)$$

where $\overline{X}_i$, $\overline{X}_{i}^{(+)}$, $\overline{X}_{i}^{(-)}$ are the average of the i^{th} feature of the whole, positive, and negative data sets, respectively; $x_{k,i}^{(+)}$ is the i^{th} feature of the k^{th} positive instance, and $x(-)_{k,i}$ is the i^{th} feature of the k^{th} negative instance. The numerator indicates the discrimination between the positive and negative sets, and the denominator indicates the one within each of the two sets. The larger the F-score is, the more likely this feature is more discriminative. Thus, this score can be used as a feature selection criterion.

Here in the proposed approach, the feature set from different domains as described in section 3 are extracted and F-Score is applied to each one of the set and the features are sorted in the descending order of their F-Score. Then different fraction of features from each feature set are taken by trial and error and concatenated to yield the final feature set.

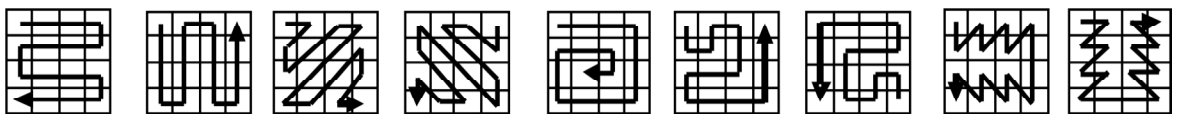
3. FEATURE EXTRACTION

Experimentation with an individual feature has shown that high detection accuracy cannot be achieved for low volume payloads. Hence feature sets computed in the spatial domain and transform domain have been made use of. Also, the feature sets have been framed in such a way that local and global features as well as features from potential hiding locations in an image are considered.

3.1. Spatial Domain Features

Local Scan Path features: Steganographic algorithms often hide data in a scattered fashion than in a concentrated mode. To highlight these imperceptible artifacts dispersed in an image, the image pixels in a sub block are arranged in a specific way termed as a scan path. The scan paths used in this work are shown in Fig. 2. After the pixels are arranged in a particular scan path, adjacent pixel differences are computed and then thresholded. Those differences which fall in the range [-4, 4] are retained and others are made zero since higher differences belong to edges of an image and the lower differences may be due to the embedded data. A co-occurrence matrix is obtained from the thresholded differences whose dimension will be 9×9. All the elements in the 9 transition matrices are used as a feature after concatenation. The transition matrices are computed for every 4×4 block in an image. The scan paths proposed by Zeng et al., (2009) which are used to embed data sequentially have been made use of in detecting hidden data.

Co-Occurrence Features derived from different bit planes of an image: Steganographic algorithms differ in their choice of bit plane to embed data. Most algorithms use the least significant bit plane to hide



(a) (b) (c) (d) (e) (f) (g) (h) (i)

Figure 2: Nine Scan Paths (a) Path S1; (b) Path S2; (c) Path S3; (d) Path S4; (e) Path S5; (f) Path S6; (g) Path S7; (h) Path S8; (i) Path S9;

data so that quality of stego image gets maintained. Other algorithms make use of higher bit planes with the help of compensation procedures. To obtain those artifacts, statistical features like mean, variance, shape distribution features like skewness, kurtosis and entropy and co-occurrence features (Haralick et al., 1973) namely contrast, energy, local homogeneity, cluster shade and cluster prominence are computed from all bit planes.

Net Pixel Change rate (NPCR): NPCR is a quantifier used in cryptography to evaluate the strength of image encryption algorithms (Mastan et al., 2011). It is mostly used to evaluate against differential attacks. It is given by the Eqn. 2 as

$$N(P,C) = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100$$

$$where\ D(i,j = \begin{cases} 0 & if \quad C(i,j) = P(i,j) \\ 1 & if \quad C(i,j) \neq P(i,j) \end{cases} \tag{2}$$

where $P(i, j)$ and $C(i, j)$ are the plain-image and the corresponding encrypted image of size $M \times N$ respectively. A high NPCR means high resistance to differential attacks. And also since this vividly captures the number of pixels changed in an image, this can be used as an efficient feature for steganalysis. As Blind Steganalysis cannot have any information regarding the cover image, to derive the NPCR parameter, the cover image needs to be predicted from the stego image at hand. Prediction can always be done by exploiting the fact that the pixels in neighbourhood have high correlation. The prediction method for a pixel x is adopted from (Shi et al., 2005b) and is given by Fig. 3 and Eqn. 3**.** NPCR feature has been calculated using Eqn. 2 substituting stego image for $C(i, j)$ and predicted image for $P(i, j)$.

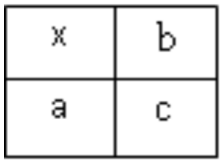


Figure 3: Prediction Context

$$\hat{x} = \begin{cases} \max(a,b) & c \leq \min(a,b) \\ \min(a,b) & c \geq \max(a,b) \\ a + b - c & otherwise \end{cases} \tag{3}$$

where a, b, c are in the context of the pixel x, x is the prediction value of x.

3.2. Transform Domain Features

Moments of Characteristic functions (MCF): Moments of Characteristic Functions (CFs) can reflect the differentiation property of associated histograms and can reflect sensitively changes caused by data hiding (Xuan et al., 2005). The statistical moments of the CFs of both the original image and its wavelet subbands have been used as features for steganalysis and are defined by Eqn.4.

$$M_n = \frac{\sum_{j=1}^{N/2} f_j^n \left| H(f_j) \right|}{\sum_{j=1}^{N/2} \left| H(f_j) \right|} \tag{4}$$

where, $H(f_j)$ is the CF component at frequency f_j and N is the total number of points in the horizontal axis of the histogram. MCF from different multiresolution transforms-Discrete Wavelet Transform, Discrete Wavelet Packet Transform, Dual Tree Discrete Wavelet Transform, Gabor Transform, Rigelet Transform, Curvelet Transform are computed and used as features.

Colour Wavelet based features: Colour wavelet feature vectors are more sensitive to image changes especially that occur in a particular colour channel. As illustrated in Fig. 4, for RGB colour images, the input image is decomposed into three channels and wavelet decomposition is performed in each channel separately.

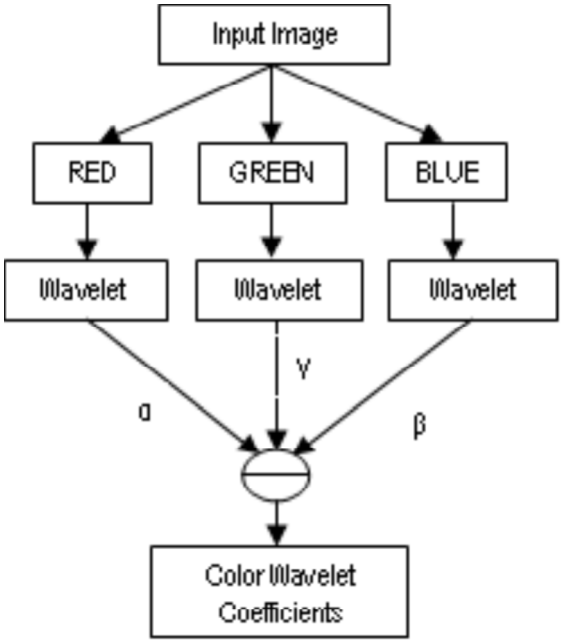


Figure 4: Colour Wavelet Decomposition

After multilevel wavelet decomposition of each colour channel, the fused coefficients are referred to as mixed colour channel wavelet decomposition (Agaian and Cai, 2004). This wavelet decomposition is called colour wavelet decomposition,

$$W = \alpha * C(R) + \beta * C(G) + \gamma * C(B) \quad (5)$$

where α, β and γ are adjust parameters, which will be adjusted according to different applications. The values C(R), C(G) and C(B) are the wavelet coefficients within the red, green and blue channels being analyzed. This implementation has used three levels and has derived features Skewness, Kurtosis, Mean and Standard Deviation from all 12 subbands.

Wavelet based Histogram features: In the embedding process, the texture pattern present in an image may be disturbed and this can be highlighted by using Wavelet features that characterize texture. Feature extraction algorithm proposed by (Hiremath et al., 2006) is made use of for this purpose. The minimum composition rule is applied to the segmented pair of bands to form a normalized cumulative histogram. The features mean, mean deviation and slope of regression line are extracted from the normalized cumulative histogram.

Features from detail subbands: Steganographic algorithms that hide data in the transform domain mostly work on the detail subbands with the horizontal and the diagonal bands being the favourites. Wavelet decomposition is first applied on the image to segregate approximation and detail parts. The approximation coefficients are then made zero and the image is now reconstructed from only the detail subband which

results in an image having only the edge details. From the details image, statistical features Mean, Variance, Co-occurrence features Contrast, Energy, Local Homogeneity, Cluster Shade, Cluster Prominence and Shape Distribution features Skewness, Kurtosis, Entropy are found to be used as a feature vector.

Features from Gradient Points: Some steganographic algorithms hide data in those areas of the image in which the changes caused by the embedding algorithm are not perceptible. Hence to capture those details, only significant edges are retained in the image and that pre-processed image is subjected to wavelet decomposition. Significant edges are those edges whose magnitude is atleast one third of the maximum gradient value in the image. Statistical features like Mean, Variance and Shape Distribution features like Skewness and Kurtosis are derived from all subbands at level 1.

The feature sets that have been derived from RGB are shown in Table. 1. For HSV domain, the feature sets representation has suffix '*H*'.

Table 1
RGB Features Sets exploited

S. No.	*Feature Sets*	*Dimension*
1	Bit Plane Cooccurrence matrix-BPCM	264
2	Colour Wavelet Statistics-CWS	36
3	Features from Gradient Points-FGP	48
4	Features from Details subbands-FID	99
5	Features from Scan Path-FSP	729
6	MCF Features from Curvelet Coefficients-MCFCTC	1746
7	MCF Features from Discrete Packet Wavelet Transform Coefficients (I Level)-MCFDPC	153
8	MCF Features from Discrete Packet Wavelet Transform Coefficients (III Level) MCFDPCIII	576
9	MCF Features from Dual Tree Discrete Wavelet Transform Coefficients-MCFDTC	90
10	MCF Features from Gabor Wavelet Transform Coefficients-MCFGTC	216
11	MCF Features from Rigelet Transform Coefficients-MCFRTC	612
12	MCF Features from Spatial Domain-MCF	9
13	MCF Features from Discrete Wavelet Transform Coefficients MCFWC	108
14	Net Pixel Change Rate-NPCR	3
15	Wavelet Based Histogram Features-WHF	144

4. RESULTS AND DISCUSSIONS

Raw and uncompressed images have been chosen to be the cover media and such images are collected from the web. From the database so formed, 500 images of size greater than size 512 × 512 are set aside to act as cover images and out of the smaller rest, yet another 500 have been used as secret images to be embedded into the larger size covers. Five free steganographic tools have been downloaded namely, Image protector

Table 2
Steganographic Software Details

Steganographic Software	*Carrier/ Stego file*	*Secret file size*	*Compression*
Image Protector (IP)	BMP	Max Size 40KB	No
Invisible Secrets (IS)	JPEG, PNG, BMP, HTML, WAV	Max Size 90KB	Yes
Third Eye (TE)	BMP	Max Size 75KB	No
S-Tools (ST)	BMP & GIF	Max Size 97KB	No
Wb-Stego (WB)	BMP, TXT, HTML, PDF	Max Size 90KB	No

(IP 2008), Invisible Secrets (IS 1997), Third Eye (TE 2010), S-Tools (ST 2010) and Wb-stego (WB 2004). Table 2 portrays the details of the Steganographic tools made use of in the experimentation. The 500 selected cover images have been subjected to the five different steganographic tools yielding 2500 stego images in the database with each cover image embedded with different and varying payloads.

Different secret images of varying sizes have been embedded in the cover image and the payload is specified as percentage of embedding capacity is given in the Table 3. Table 3 also displays the maximum size that can be embedded with different steganographic tools selected. It can be observed from Table 4 that, around 83% of the stego images in the database have a payload of less than 5% of the embedding capacity of the corresponding cover images while around 10% of them have a payload of 10% of the embedding capacity. 4 different bins have been considered based on embedding capacity such as <5%, 5 to 10%, 10 to 25% and 25 to 50% in the formation of database.

As mentioned in the feature extraction section, 30 feature sets have been derived for each and every image in the database and stored in the features Library. 400 cover images and 2000 stego images (400 stego images for each one of the steganographic software 400 5 = 2000) are used for training. The train / test ratio is 80:20 and the train/ test ratio is disjoint and random selection has been employed in fixing the train and test set. During classification, the unseen images have been used for validation of the developed steganalyzer.

Table 3
Secret Images Size as Percentage of Embedding Capacity

S. No.	*Steganographic Algorithm*	*Max Embedding Capacity*	*Size of Embedded Secret Images*				
			<=5%	*5% to 10%*	*10 to 25%*	*25 to 50%*	*Total*
1	Image Protector (IP)	40KB	416	52	27	5	500
2	Invisible Secrets (IS)	90 KB	416	52	27	5	500
3	Third Eye (TE)	75 KB	416	51	28	5	500
4	S-Tools (ST)	97 KB	417	51	27	5	500
5	Wb-Stego (WB)	90 KB	416	52	27	5	500
Total in numbers		2081	258	136	25	2500	
Total in %83.24		10.32	5.44	1	100		

Table 4
Details of Images used for Training & Classification

	No of Images used for Training & Classification							
	<=5%		*5-10%*		*10-25%*		*25-50%*	
Steganographic Software	*#Train Images*	*# Test Images*	*#Train Images*	*# Test Images*	*#Train Images*	*# Test Images*	*# Train Images*	*# Test Images*
IP	344	72	42	10	13	14	0	5
IS	344	72	42	10	13	14	0	5
TE	344	72	42	9	13	15	0	5
ST	345	72	41	10	13	14	0	5
WB	344	72	42	10	13	14	0	5

As the problem involved meager payloads and individual feature sets do not provide good detection accuracy, the proposed approach makes use of a composite feature set. As simple concatenation of the feature sets which are 30 in number will make the dimensionality too large to be handled by a classifier, a composite feature set has been made use of.

Table 5
Results of Single feature set Model

Feature	*Detection Accuracy for each tool in %*					
	IP	*IS*	*TE*	*ST*	*WB*	*Average*
BPCM	61.5	80.5	49.5	50	49.5	58.2
BPCMH	52.5	91.5	56	55	51	61.2
CWS	45	46.5	46.5	47	46	46.2
CWSH	53.5	69.5	58.5	62	60	60.7
FGP	45	45.5	47.5	48	47	46.6
FGPH	51	66	55.5	56.5	55	56.8
FID	44	52.5	48	48.5	47.5	48.1
FIDH	49.5	70.5	57.5	58	59.5	59
FSP	46.5	49	46.5	48.5	47.5	47.6
FSPH	54.5	84	49.5	53	50	58.2
MCFCTC	53	57	47.5	47	49	50.7
MCFDPC	56	61.5	52.5	47	47	52.8
MCFDPCIII	48	44.5	48	53	45.5	47.8
MCFDTC	61	63.5	48.5	51	50.5	54.9
MCFGTC	46.5	47	46.5	47	46.5	46.7
MCFHCTC	45	65.5	50.5	49	51	52.2
MCFHDPC	48.5	82	56.5	53.5	55.5	59.2
MCFHDPCIII	46	74	58	56	47.5	56.3
MCFHDTC	49	81.5	54	56	52	58.5
MCFHGTC	49.5	59	55.5	46.5	53.5	52.8
MCFHRTC	47	60	50	54	56.5	53.5
MCFHSC	48.5	62	47.5	47	55.5	52.1
MCFHWC	51	90	58	57	53.5	61.9
MCFRTC	50	51	48.5	52	49.5	50.2
MCFSC	50	52.5	47	45	50.5	49
MCFWC	55.5	64	49	44.5	50	52.6
NPCR	65.5	61.5	52	53	50.5	56.5
NPCRH	58	89.5	61	60.5	53.5	64.5
WHF	47.5	57.5	50	49.5	47	50.3
WHFH	48	65.5	55	53.5	51	54.6

The composite feature set has been coined after employing a feature selection procedure based on F-score. For every individual feature set, the features are arranged on the basis of their F-scores and a significant share is collected and compiled to form the composite feature set. As the significant share improve, so do the dimensionality of the composite feature set and the detection accuracy. A maximum overall detection accuracy of 80% is achieved with 30% of the significant features from every feature set contributing to the composite feature set of dimensionality 3118 as evident from Table 6. The classifier used is SMO.

To improve the generalization of the classifier, only one algorithm was trained and the rest are tested. The overall detection accuracy when 30% of the features are considered is 88.33% proving the generalization of the Steganalyzer.

Table 6
Results of generic Steganalysis-Hybrid Concatenated F-Scored feature set for different fractions

S. No.	Train Tool	Accuracy For Various Fractions (#)					
		1%(648)	5%(988)	10%(1414)	20%(2267)	30%(3118)	50%(4833)
1	IP	69	70.5	73.5	75	77.5	73.5
2	IS	51.5	54	56.5	57.5	58.5	60.5
3	TE	68.5	76	79.5	82.5	84.5	84
4	ST	69	74	77.5	82	85.5	86
5	WB	80.5	86	91	94	94	93
	Overall Accuracy	67.7	72.1	75.6	78.2	80	79.4

Table 7
Mixed Blind Generic Steganalysis-Hybrid Concatenated F-Scored feature set for different fractions

S. No.	*Train Tool*	*Accuracy For Various Fractions (#)*		
		10%(1414)	*30%(3118)*	*50%(4833)*
1	IP	84.5	87.5	87
2	IS	75.67	79.33	80.17
3	TE	88.5	91.67	91.5
4	ST	86.33	91.17	92
5	WB	88.83	92	91.67
	Overall Accuracy	84.766	88.334	88.468

To demonstrate the competence of the designed Steganalyzer, the obtained results have been compared with SPAM features (Pevny et al., 2010). Table 8 shows the detection accuracy obtained for the same database with SPAM features (2058D) derived from RGB, HSV and also combining the features obtained from both the colour models. Our approach gives a better performance than SPAM features but with a lower dimensionality (3118D).

Table 8 : Comparison with SPAM Feature

S. No.	*Train Tool*	*SPAM(2058)*	*SPAMH(2058)*	*Combined(4116)*
1	IP	75	64	74.5
2	IS	95	98	97
3	TE	56.5	74	72
4	ST	54.5	70.5	69.5
5	WB	60	56.5	58.5
	Overall	68.2	72.6	74.3

5. CONCLUSION

A Universal, blind statistical steganalyzer has been designed to distinguish between clean and stego images. The stego images have very minimal payloads embedded on raw and uncompressed media. The composite feature set gathered after applying feature selection along with the SMO classifier showed greater generalization capabilities, a mandatory feature for Universal steganalysis. The designed steganalyzer has achieved this with less dimensionality compared to the SPAM features. Low volume payloads hidden into raw and uncompressed media posed a tough challenge and this proposed approach has addressed this issue for steganalysts with a hybrid composite feature set framed after meticulous selection of features.

References

[1] Agaian, S., Cai, H., 2004. Color wavelet based universal blind steganalysis, in: The 2004 International Workshop on Spectral Methods and Multirate Signal Processing, SMMSP. Citeseer.

[2] Avcıbaþ, İ., Kharrazib, M., Memonc, N., Sankurd, B., 2002. Image steganalysis with binary similarity measures. IEEE Trans. Image Process 1057–7149.

[3] Avcibas, I., Memon, N., Sankur, B., 2003. Steganalysis using image quality metrics. IEEE Transactions on Image Processing 12, 221–229. doi:10.1109/TIP. 2002.807363

[4] Cho, S., Cha, B.-H., Gawecki, M., Jay Kuo, C.-C., 2013. Block-based image steganalysis: Algorithm and performance evaluation. Journal of Visual Communication and Image Representation 24, 846–856. doi:10.1016/j.jvcir.2013.05.007

[5] Dong, J., Tan, T., 2008. Blind image steganalysis based on run-length histogram analysis., in: ICIP. pp. 2064–2067.

[6] Fridrich, J., Goljan, M., Du, R., 2001. Steganalysis based on JPEG compatibility, in: ITCom 2001: International Symposium on the Convergence of IT and Communications. International Society for Optics and Photonics, pp. 275–280.

[7] Fridrich, J., Goljan, M., Hogea, D., 2003. New methodology for breaking steganographic techniques for JPEGs, in: Electronic Imaging 2003. International Society for Optics and Photonics, pp. 143–155.

[8] Geetha, S., Sivatha Sindhu, S.S., Kamaraj, N., 2009. Blind image steganalysis based on content independent statistical measures maximizing the specificity and sensitivity of the system. Computers & Security 28, 683–697. doi:10.1016/j.cose.2009.03.006

[9] Goljan, M., Fridrich, J., Holotyak, T., 2006. New blind steganalysis and its implications, in: Electronic Imaging 2006. International Society for Optics and Photonics, pp. 607201–607201.

[10] Goljan, M., Fridrich, J., Cogranne, R., others, 2015. Rich model for steganalysis of color images, in: Parallel Computing Technologies (PARCOMPTECH), 2015 National Conference on. IEEE, pp. 185–190.

[11] Gou, H., Swaminathan, A., Wu, M., 2007. Noise features for image tampering detection and steganalysis, in: Image Processing, 2007. ICIP 2007. IEEE International Conference on. IEEE, pp. VI–97.

[12] Gul, G., Kurugollu, F., 2013. JPEG Image Steganalysis Using Multivariate PDF Estimates With MRF Cliques. IEEE Transactions on Information Forensics and Security 8, 578–587. doi:10.1109/TIFS.2013.2247399

[13] Gul, G., Kurugollu, F., 2010. SVD-Based Universal Spatial Domain Image Steganalysis. Information Forensics and Security, IEEE Transactions on 5, 349–353. doi:10.1109/TIFS.2010.2041826

[14] Haralick, R.M., Shanmugam, K., Dinstein, I., 1973. Textural Features for Image Classification. IEEE Transactions on Systems, Man, and Cybernetics 3, 610–621. doi:10.1109/TSMC.1973.4309314

[15] Harmsen, J.J., Pearlman, W.A., 2003. Steganalysis of additive-noise modelable information hiding, in: Electronic Imaging 2003. International Society for Optics and Photonics, pp. 131–142.

[16] Hiremath, P.S., Shivashankar, S., Pujari, J., 2006. Wavelet based features for color texture classification with application to CBIR. International Journal of Computer Science and Network Security 6, 124–133.

[17] Holotyak, T., Fridrich, J., Voloshynovskiy, S., 2005. Blind statistical steganalysis of additive steganography using wavelet higher order statistics, in: Communications and Multimedia Security. pp. 273–274.

[18] Holub, V., Fridrich, J., 2013. Random Projections of Residuals for Digital Image Steganalysis. Information Forensics and Security, IEEE Transactions on 8, 1996–2006. doi:10.1109/TIFS.2013.2286682

[19] Ker, A.D., 2005. Steganalysis of LSB matching in grayscale images. Signal Processing Letters, IEEE 12, 441–444. doi:10.1109/LSP. 2005.847889

[20] Luo, X., Liu, F., Lian, S., Yang, C., Gritzalis, S., 2011. On the Typical Statistic Features for Image Blind Steganalysis. IEEE Journal on Selected Areas in Communications 29, 1404–1422. doi:10.1109/JSAC.2011.110807

[21] Lyu, S., Farid, H., 2006. Steganalysis Using Higher-Order Image Statistics. IEEE Transactions on Information Forensics and Security 1, 111–119. doi:10.1109/TIFS.2005.863485

[22] Mastan, J.M.K., Sathishkumar, G.A., Bagan, K.B., 2011. A Color Image Encryption Technique Based on a Substitution-Permutation Network, in: Abraham, A., Mauri, J.L., Buford, J.F., Suzuki, J., Thampi, S.M. (Eds.), Advances in Computing and Communications, Communications in Computer and Information Science. Springer Berlin Heidelberg, pp. 524–533.

[23] Pathak, P., Selvakumar, S., 2014. Blind Image Steganalysis of JPEG images using feature extraction through the process of dilation. Digital Investigation 11, 67–77. doi:10.1016/j.diin.2013.12.002

[24] Pevny, T., Bas, P., Fridrich, J., 2010. Steganalysis by Subtractive Pixel Adjacency Matrix. Information Forensics and Security, IEEE Transactions on 5, 215–224. doi:10.1109/TIFS.2010.2045842

[25] Savoldi, A., Gubian, P., 2007. Blind multi-class steganalysis system using wavelet statistics, in: Iih-Msp. IEEE, pp. 93–96.

[26] Shi, Y.Q., Chen, C., Chen, W., 2007. A Markov process based approach to effective attacking JPEG steganography, in: Information Hiding. Springer, pp. 249–264.

[27] Shi, Y.Q., Xuan, G., Yang, C., Gao, J., Zhang, Z., Chai, P., Zou, D., Chen, C., Chen, W., 2005a. Effective steganalysis based on statistical moments of wavelet characteristic function, in: Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on. IEEE, pp. 768–773.

[28] Shi, Y.Q., Zou, D., Chen, W., Chen, C., others, 2005b. Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network, in: 2005 IEEE International Conference on Multimedia and Expo. IEEE, p. 4.

[29] Wen-Nung Lie, Guo-Shiang Lin, 2005. A feature-based classification technique for blind image steganalysis. IEEE Transactions on Multimedia 7, 1007–1020. doi:10.1109/TMM.2005.858377

[30] Xuan, G., Gao, J., Shi, Y.Q., Zou, D., 2005. Image Steganalysis Based on Statistical Moments of Wavelet Subband Histograms in DFT Domain, in: 2005 IEEE 7th Workshop on Multimedia Signal Processing. Presented at the 2005 IEEE 7th Workshop on Multimedia Signal Processing, pp. 1–4. doi:10.1109/MMSP. 2005.248584

[31] Zeng, X., Ping, L., Li, Z., 2009. Lossless data hiding scheme using adjacent pixel difference based on scan path. Journal of Multimedia 4, 145–152.

[32] Zhang, T., Ping, X., 2003. Reliable detection of LSB steganography based on the difference image histogram, in: Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on. IEEE, pp. 545 – 548.

[33] Zong, H., Liu, F., Luo, X., 2012. Blind image steganalysis based on wavelet coefficient correlation. Digital Investigation 9, 58–68. doi:10.1016/j.diin.2012.02.003

[34] Zou, D., Shi, Y.Q., Su, W., Xuan, G., 2006. Steganalysis based on Markov model of thresholded prediction-error image, in: Multimedia and Expo, 2006 IEEE International Conference on. IEEE, pp. 1365–1368.

[35] ID Image Protector 1.2. Available from: < www.sharesoftware24.com/free-downloads/windows/security-privacy/encryption-tools/info/id-image-protector-2232.html> [25 April 2008].

[36] Invisible Secrets 4. Available from: < www.invisiblesecrets.com > [11 January 1997].

[37] Third Eye. Available from: < www.securekit.net/index.html > [1 June 2010].

[38] S Tools. Available at: http://www.spychecker.com/download/download-stools.html [1 February 2010].

[39] Wb Stego 4. Available from: < http://wbstego.wbailer.com > [1 March 2004].