Steganographic Tool Detection using Specific Composite Feature Set and Weighted Decision Function

S. Arivazhagan, W. Sylvia Lilly Jebarani, S.T.Veena

ABSTRACT--- Steganographic tools available in the internet and other commercial steganographic tools are preferred than customized steganographic tools developed from scratch by unlawful groups. Hence a clue regarding the steganographic tool deployed in the covert communication process can save time for the steganalyst in the crucial active steganalysis phase. Signature analysis can lead to success in targeted steganalysis but tool detection needs to be taken forward from a point with a suspicious stego image in hand with no additional details available. In such scenarios, statistical steganalysis comes to rescue but with issues to be addressed like huge dimensionality of feature sets and complex ensemble classifiers. This work accomplishes tool detection with a specific composite feature set identified to distinguish one stego tool from the others with a weighted decision function to enhance the role of the specific feature set when it votes for a particular class. A tool detection accuracy of 85.25% has been achieved simultaneously addressing feature set dimensionality and complexity of ensemble classifiers and a comparison with a benchmark procedure has been made.

Keywords—Steganographic tool detection, specific composite feature set, weighted decision function, ensemble classification; feature/colour model/domain/significant function selection.

Keywords— Steganographic tool detection, specific composite feature set, weighted decision function, ensemble classification; feature/colour model/domain/significant function selection.

I. INTRODUCTION

Steganography meaning covered writing as derived from the word's Greek origin serves as a powerful supplement / alternative to Cryptography. Steganography differs from Cryptography as the communication channel itself goes unnoticed, giving no room for the intruder to launch the attacks. Steganalysis includes all tasks and attempts made towards unearthing and extracting the intelligence out of a secret message transaction. Steganalysis can spoil malicious intentions if deadly plots are exposed and can thus serve human society. Embedding very minimal payloads have become the norm of people who want to establish covert channels since such payloads can easily evade Steganalysis. As the detection rate of hidden communication is directly proportional to amount of hidden data, secret communications are made with vanishingly small amount of information. Such minuscule stealthy communications can easily escape the Steganalysis process as the embedding signatures are hardly visible to be noticed. Steganalysis needs to be rigorous to highlight the delicate artifacts created in the embedding process. With all these issues to be addressed, even if Generic Steganalysis succeeds, that always doesn't lead to extraction of embedded secret. Blind steganalysis [1] comes handy for practical situations. Most of the covert channels prefer creation of stego images with the help of commercial steganographic software rather than customized steganographic algorithms. A clue regarding the steganographic technique used to embed data will aid for a faster extraction of secret. Thus, Steganographic tool detection [2] can be thought of as the first step in Active Steganalysis that follows generic detection.

II. LITERATURE SURVEY

Literature advises to approach the tough task of steganalysis using a pattern recognition perception which immediately opens up an avenue of possibilities which include the identification of apt feature set to characterize the steganographic process and the right form of a classifier. From the viewpoint of Fridrich et al. [3], steganalysis may be completely infeasible or extremely time consuming if the stego technique and the stego and cipher keys are not known. Lu et al. [4] considered the fact that class variance can be exploited to distinguish features based on their class separability. Fisher score modified with Euclidean distance was calculated to reorder the features based on this criterion. And then starting with feature of 1 dimension, the features with maximum score are combined. The score is recalculated for each new combined feature[17, 18]. The Process continues adding a maximum score feature each time until there is no further improvement in the score of combined features which gives the optimal dimensionality. Hou et al. [5] adds to the fact that the major defect in steganalysis exists as treating all images as equals, thus ignoring the statistical variability that would normally exist among them as a major blunder. To overcome this, the authors proposed a clustering strategy of grouping images based on their texture complexity. Wenhao Chen et al. [6] developed algorithms based on signature detection and machine learning methods to identify stego images created by Android mobile apps. They have manually analysed stego app binaries to gain the ground truth of the apps' embedding process. This will modify the app's embedding

Revised Manuscript Received on July 10, 2019.

S. Arivazhagan, Department of Electronics and Communication Engineering MEPCO Schlenk Engineering College Sivakasi – 626005 Tamilnadu, India (sarivu@mepcoeng.ac.in)

W. Sylvia Lilly Jebarani, Department of Electronics and Communication Engineering MEPCO Schlenk Engineering College Sivakasi – 626005 Tamilnadu, India (wsylvia@mepcoeng.ac.in)

S.T.Veena, Department of Electronics and Communication Engineering MEPCO Schlenk Engineering College Sivakasi – 626005 Tamilnadu, India (veena_st@yahoo.com)

function so that it accepts "empty payloads," in which case the produced stego image is equivalent to the cover image, or add a new function to the stego app that can take the pre-embedding clean image data as input, and produce an image that has the same encoding or compression format as the stego image. Ben Li et al [7] developed steganalytic co-occurrence features using an operator called thresholded local binary pattern. Their proposed TLBP features achieve good steganalytic performance under various conditions.

This work attempts Steganographic tool detection with the help of varied feature sets computed from different colour models and domains on a demanding database of stego images which hide meagre payloads. The tool detection process will be very difficult always as the meagre payloads vanish in a frame of pixels. With the proposed frame work, decent tool detection accuracy has been achieved to surpass SPAM features, a benchmark feature set in the steganalysis arena[16].

III. PROPOSED TOOL DETECTION STEGANALYTIC SYSTEM

The proposed steganographic tool detection system follows the Generic Steganalysis phase, an important process in active steganalysis which determines the success of subsequent processes like embedding location and data estimation which will lead to extraction of secret. The tool detector performs feature selection, colour model selection and domain selection for extraction of features and frames a composite feature set. The composite feature set is optimized by fixing the size of the fraction to be extracted from the entire feature space. The WEKA data mining tool has been used for classification of the steganographic tools. The WEKA SMO classifier is by default a binary classifier and many instances of such classifiers with every instance trained with one tool have been combined together in one against one fashion to realize a multi class classifier. This SMO multi class classifier in ensemble form has been employed to differentiate among the eight steganographic tools which have made use of in the creation of database. A weighted decision function combines the results of individual classifiers and declares the tool employed in the steganographic process.

Fig. 1 shows the different processes involved in the proposed steganalytic system. From the database created, 80% of stego images created using different tools have been used for training the Steganalyzer to perform tool detection. The images are subjected to feature extraction. Feature sets are used individually first and then combined as a composite feature set for improvement in classification rate. Feature sets thus framed are stored in the Features Library which completes the learning phase. In the testing phase, the remaining 20% unseen data are subjected to the same set and sequence of processes. The features extracted from the test data are compared with the features stored in the Features Library for a decision. The SMO multi-class classifier has been made use of for all the tool detection approaches in one against one fashion. As the final approach involved specific feature sets and a weighted decision function which magnified the complexity of the process, the 'Multi Classifier', a multi class classifier of WEKA has been used with its default settings of ensemble configuration, one against all approach and classification by logistic regression. The algorithm used for the detection of the employed Steganographic tools is discussed in the following section.

A. Algorithm for Steganographic Tool detection – Training Phase

Experimentation has been carried out with feature sets individually employed as well as a composite / specific feature set with WEKA classifiers. The following algorithm has been implemented to identify the tools and the algorithm consists of two common phases, training phase and testing phase.

The steps involved in Training phase are as follows:

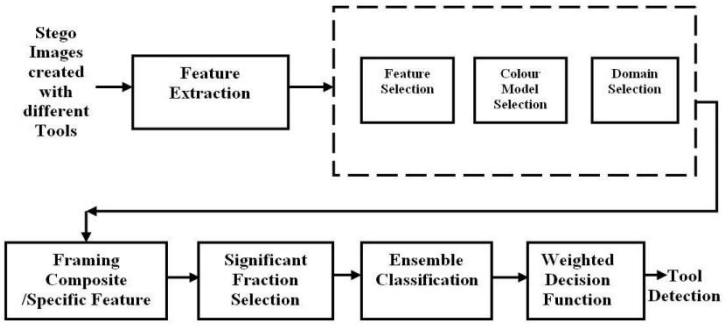
- Read random pairs of stego images created with two different tools at one instance.
- Represent them with eight different colour models like Gray, RGB , HSV, YCbCr, CMY, YIQ, I1-I2-I3, L*a*b*.
- Select the best colour models, features and the domain of extraction.
- Extract the selected features from selected colour models in the selected domain.
- Select the optimum dimensionality for the feature set.
- Frame the composite / specific feature set.
- Store them in a feature library.
- Repeat steps (i) – (vi) for all tools / possible combinations of tool pairs.
- Train SMO multi class classifier / 'Multi classifier' with the relevant feature set.

Save the trained model.

B. Algorithm for Steganographic Tool detection – Testing Phase

- Read unseen stego images.
- Represent them with selected colour models.
- Extract the same feature set used in training.
- Test the features against the trained model.
- Classify the result as one of the tools used in creating the stego image.

Fig.1. Block diagram of proposed tool detection steganalyzer



IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

Phase two of the Steganalysis process involves the detection of the Steganographic software which is a critical component of active steganalysis. Tool detection process has been attempted with individual features screened by F-Score, composite / concatenated feature sets and then with specific feature sets. Steganographic Algorithm Detection was performed on the same challenging database over which Generic Steganalysis had been done ([8], [9], [10], and [11]). In an effort to identify the right approach which exactly characterizes the embedding process, various combinations of features have been used. Table 1 gives the feature sub-models that have been exploited from literature survey ([12]-[15]) along with its dimensionality.

Table 1. Feature sub-models employed

S.No	Feature Set	Dimensionality
1	Cm1Ch1SpSt[1-6]	6
2	Cm1Ch1SpCo[1-6]	6
3	Cm1Ch1SpRePeSt[1-6]	6
4	Cm1Ch1SpRePeCo[1-6]	6
5	Cm1Ch1Wav[1-3]St[1-6]	72
6	Cm1Ch1Wav[1-3]Co[1-6]	72
7	Cm1Ch1Bp1St[1-6]	6
8	Cm1Ch1Bp1Co[1-6]	6
9	Cm1Ch1SpRlH10St[1-3]	3
10	Cm1Ch1SpRlH11St[1-3]	3
11	Cm1Ch1SpRlH20St[1-3]	3
12	Cm1Ch1SpRlH21St[1-3]	3
13	Cm1Ch1SpRlV10St[1-3]	3
14	Cm1Ch1SpRlV11St[1-3]	3
15	Cm1Ch1SpRlV20St[1-3]	3
16	Cm1Ch1SpRlV21St[1-3]	3
17	Cm1Ch1WavCorr	204
18	Cm1Ch1WavFGP	16
19	Cm1Ch1WavFID	33
20	Cm1Ch1SpReNoise	12
21	Cm1Ch1SpMCF	3
22	Cm1Ch1SpRePeMCF	3
23	Cm1Ch1SpRePeNoise	27
24	Cm1Ch1WavMCF	36
25	Cm1Ch1WavRePeMCF	27
26	Cm1Ch1WavReLogPeMCF	27
27	Cm1Ch1SpMTM	81
28	Cm1Ch1SpNPCR	1
29	Cm1Ch1SpTWIN	1
30	Cm2Ch1WavBiorCWS	12
31	Cm2GBS	18
32	Cm1Ch1SpReSpm	686
33	Cm2Ch1SpReSpm	686
34	Cm2Ch2SpReSpm	686
35	Cm2Ch3SpReSpm	686
36	Cm3Ch1SpReSpm	686
37	Cm3Ch2SpReSpm	686
38	Cm3Ch3SpReSpm	686

A total of 38 sub-models have been used. Extracting feature sets 1 to 31 for each colour model and colour channel with exception of Gray Colour Model for feature models 30 and 31, a total of 246 sets of features have been considered for the experiments. All 246 features have been employed for the process of tool detection from which 10% of the individual feature sets have been selected after reordering the feature set by F-Score. Table 2 presents the confusion matrix for the scheme along with average detection accuracy for every bin. From the confusion matrix, it can be observed that IS tool is always identified by its signature. Except 1% bin, SE tool is also detected in all bins due to its accommodation of more payloads compared to other tools.

Table 2. Confusion matrix for tool detection with 10% of F-Scored individual feature sets

Payload bin	Tool	Classified as							
		IS	SE	TE	WB	2P	BS	BH	HS
1%	IS	96	0	1	3	0	0	0	0
	SE	0	45	14	8	10	9	14	0
	TE	0	25	25	7	14	14	15	0
	WB	0	20	21	11	18	15	15	0
	2P	0	24	20	13	14	12	17	0
	BS	0	18	25	12	12	17	16	0
	BH	0	20	20	6	20	10	24	0
	HS	0	0	0	0	0	0	0	4
Average Bin wise Tool Detection accuracy in %									29.5
2%	IS	100	0	0	0	0	0	0	0
	SE	0	77	6	6	2	1	2	6
	TE	0	12	22	19	4	17	12	14
	WB	0	10	24	24	3	20	13	6
	2P	0	11	22	17	7	16	17	10
	BS	0	12	22	16	4	27	13	6

	BH	0	11	21	15	5	16	23	9
	HS	0	33	25	13	3	12	5	9
Average Bin wise Tool Detection accuracy in %									36.125
3%	IS	100	0	0	0	0	0	0	0
	SE	0	78	4	7	4	5	0	2
	TE	0	5	20	16	11	27	8	13
	WB	0	8	16	21	11	21	10	13
	2P	0	5	13	13	30	14	12	13
	BS	0	6	20	16	12	20	9	17
	BH	0	7	14	10	18	21	14	16
	HS	0	4	20	16	17	19	11	13
Average Bin wise Tool Detection accuracy in %									37
4%	IS	96	2	1	0	0	0	1	0
	SE	1	75	6	6	4	2	3	3
	TE	0	4	18	22	18	14	17	7
	WB	0	5	20	28	14	9	17	7
	2P	0	5	13	20	26	15	16	5
	BS	0	6	19	21	16	18	13	7
	BH	0	5	16	21	18	12	21	7
	HS	0	4	19	18	24	11	12	12
Average Bin wise Tool Detection accuracy in %									36.75
5%	IS	95	2	0	0	2	0	1	0
	SE	1	89	1	0	1	0	4	4
	TE	0	2	23	18	9	11	21	16
	WB	0	1	14	15	21	9	21	16
	2P	0	2	11	20	26	6	23	12
	BS	0	2	17	23	10	13	16	19
	BH	0	2	12	11	20	4	38	13
	HS	0	2	20	14	14	12	19	19
Average Bin wise Tool Detection accuracy in %									39.75
10%	IS	94	2	1	2	0	1	0	0
	SE	2	96	0	1	0	0	0	1
	TE	0	0	29	16	17	18	4	16
	WB	1	1	18	32	16	15	7	10
	2P	0	0	18	18	33	10	15	6
	BS	0	1	25	17	14	24	8	11
	BH	1	1	12	18	23	6	34	5
	HS	0	0	26	16	10	16	7	25
Average Bin wise Tool Detection accuracy in %									45.875

Tool detection process is not able to differentiate clearly among the other tools. The maximum tool detection accuracy achieved with individual feature sets is 45.875%. Throughout results presented here, monotonicity i.e., improvement in detection accuracy with payloads cannot be observed due to the facts that mostly all the tools embed using LSB and the payload bins are too close to each other. A 5-fold cross-validation helped to reduce these fluctuations as can be observed from Table 3. The maximum detection accuracy obtained for the 10% bin improved to 47.7% after cross-validation.

Table 3. Improvement in monotonicity after cross-validation

Payload bin (%)	Tool Detection Accuracy in %	
	Without cross validation	With cross validation
1	29.5	30.18
2	36.125	37.35
3	37	39.72
4	36.75	39.12
5	39.75	42.42
10	45.875	47.7

Payload bin (%)	Tool Detection Accuracy in %	
	Without cross validation	With cross validation
1	29.5	30.18
2	36.125	37.35
3	37	39.72
4	36.75	39.12
5	39.75	42.42
10	45.875	47.7

In an effort to lift up tool detection accuracy, the concatenated / composite feature sets designed for Generic Steganalysis have been extended for steganographic tool detection. The composite feature set gathered colour model wise and domain wise improves tool detection accuracy in all the bins except the 1% bin as shown in Table 4. The classifier employed is a SMO multi class classifier employed in one against one fashion. Results presented in Table 4 indicate the enormity associated with tool detection that too when stego images hide low volume payloads and it can be also observed that composite feature sets perform better than individual feature sets as in the case of Generic Steganalysis.

Table 4. Tool detection accuracy with 5% F-Scored composite feature sets

Payload bin (%)	Average Detection Accuracy in %		
	Feature Wise (687)	Colour Model Wise (726)	Domain Wise (700)
1	29.125	28	28.25
2	36.75	38.5	39
3	36.375	41	39
4	38.25	40.25	41.125
5	41.875	43.5	44.625
10	46.875	49	48.25

The most discriminative 5% features of the composite feature set selected by F-Score applied for tool detection is able to push the detection accuracy to 49%. Doubling the significant fraction, the tool detection accuracy marginally improved as can be observed from Table 5. Yet another composite feature, referred to as specific composite feature set has been framed as described in the proposed approach section. To fix the optimum size of the feature set, experimentation has been done with various fractions of the composite feature set. Significant fractions of the entire feature set have been considered for experimentation and higher significant fractions namely 20% & 30% are not found to improve tool detection accuracy as can be observed from Table 6. Hence the optimum significant fraction has been fixed as 10%. It

can be also observed from Table 6 that this specific composite feature set is able to achieve only 52.5% for the even fully stuffed 100% payload bin.

Table 5. Tool detection accuracy with 10% F-Scored composite feature sets

Payload bin (%)	Average Detection Accuracy in %		
	Feature Wise (1336)	Colour Model Wise (1455)	Domain Wise (1403)
1	29.25	28.375	27.375
2	37.5	40.5	38
3	37.25	44.25	41.875
4	37.25	41.25	41.375
5	42.125	45.375	44.5
10	48	49.5	48.5

Table 6. Tool detection accuracy for different fractions of F-Scored specific composite feature set

Payload bin (%)	Average Detection Accuracy in %			
	5% (133)	10% (266)	20% (532)	30% (798)
1	27.875	28.375	24.625	23.5
2	36	40.5	34.75	29
3	39.5	37.75	34.5	25
4	39	41.875	36.75	29.625
5	41.5	41.375	34.875	33.75
10	41.125	37	40.375	40.375
100	50.125	52.5	49.625	46.5

With the experience gathered from Generic Steganalysis, two specific feature sets have been gathered to be employed for tool detection. Specific Feature set I is gathered from the feature sets which performed well in identification of tools only in the 10% bin so that dimensionality of the feature set can be confined and are shown in Table 7. Bitplane co-occurrences have been used to represent IS tool since they characterize the signature of IS by statistical means. Also features extracted from spatial domain identify BS tool than any other individual feature, this concatenated feature set has been used to represent BS. Similarly the concatenated feature set from transform domain has been used to represent HS along with MTM feature.

Table 7. Details of specific feature set – I

Steganographic Tool	Feature Set(s)
IS	Bit plane Co-occurrence
SE	Correlation
TE	Correlation + Wavelet
WB	Runlength + Co-occurrence
2P	Statistical + Runlength
BS	Spatial
BH	Co-occurrence + Statistical + MCF
HS	MTM + Wavelet

Specific Feature set II as shown in Table 8 has been accumulated from feature sets which have identified individual tools in all the bins. The results of the experimentation are given in Tables 9 and 10.

Table 8. Details of specific feature set – II

Steganographic Tool	Feature Set(s)
IS	Co-occurrence + MTM + FID
SE	Co-occurrence + Correlation
TE	Co-occurrence + Statistical + MCF + Correlation + Runlength
WB	MCF + FID + Correlation + MTM + Statistical + Runlength
2P	MCF + Correlation + Co-occurrence + FID + Runlength
BS	Runlength + Statistical + MCF + Co-occurrence + FID + MTM
BH	Runlength + Statistical + Correlation + MTM
HS	Co-occurrence + Statistical + MCF + Correlation + Runlength

The feature sets framed have been employed for tool detection along with an ensemble classifier. Specific Feature sets I and II have been coined from the results obtained for Generic Steganalysis. The ensemble classifier has been crafted from individual classifiers which make use of a specific feature set to identify a particular tool. Hence weights have been assigned for decision of an individual classifier in favour of a particular steganographic tool. The effect of the weighted decision function can be inferred from Tables 9 and 10. This specific feature set has been made use of with an ensemble classifier summarizing individual results with a weighted decision function. As this feature set needs to be trained with 26 instances which comprise the classifier and also taking into account, the dimensionality of this specific feature set, the 'Multi Classifier' is employed for this approach. The one against all approach used by this classifier reduces the instances to a mere 8 where every instance either decides in favour of a particular steganographic tool or not. As the classifiers are driven by specific feature sets, the decision of the classifier when it votes for a specific tool, it is given more weight than the other classifiers. i.e.) when a classifier making use of a specific feature set votes for a specific tool, a weight of 0.79 is assigned to that decision and all the remaining classifiers are given a weight of 0.03, a value obtained after dividing the balance weight with the number of classifiers. The process is pictorially illustrated in Fig 2 where 8 specific feature sets along with 8 classifiers will have decisions weighted and then combined by majority voting

Fig 2. Schematic of the multiclass ensemble classifier

Table 9. Tool detection accuracy with 10% F-Scored specific feature sets

Payload bin (%)	Detection Accuracy in %	
	Specific Feature Set I	Specific Feature Set II
1	30.875	33.625
2	46	39
3	46	38.75
4	47	41.125
5	45.25	45.875
10	54.125	46.625

As can be observed from Table 9, Specific Feature Set I performs better than the higher dimensional Specific Feature Set II. Specific Feature Set I provided the best steganographic tool detection accuracy of 54.125% for the 10% payload bin. Specific Feature Set I excels Specific Feature Set II in terms of both detection accuracy and dimensionality providing the required trade-off. Specific feature Set II outperformed Specific feature Set I in the 1% payload bin with a tool detection accuracy of 33.625%, the highest ever achieved for 1% bin.

As monotonicity cannot be observed with payload bins, tool detection accuracy is not monotonic with dimensionality too and this fact can be observed from Table 10. Hence all the individual feature sets have been concatenated together to form one giant set referred to as Feature set III. When a significant fraction of 5% is extracted from all 246 features after they are ordered with F-Score, 85.25% detection accuracy is achieved but decreased to 73.375% if the significant fraction is made as 10%.

Table 10. Tool detection accuracy with different fractions of F-Scored all feature sets

Payload bin (%)	Average Detection Accuracy in %	
	5%	10%
100	85.25	73.375

A. Comparison with SPAM

As shown in Table 11, the proposed tool detection process surpassed SPAM features in all the bins but with optimum dimensionality, the reason being SPAM features are second order Markov features with a threshold [-3 3] used as such.

Table 11. Comparison of tool detection accuracies with SPAM feature set

Approach	Detection Accuracy for various Payload bins in %					
	1%	2%	3%	4%	5%	10%
SPAM (Pevny *et al.*)	29.875	32.25	36.375	35.125	36.25	42.625
Proposed Method	30.875	46	46	47	45.25	54.125

The proposed approach frames feature sets from features derived from co-occurrences and correlations and hence dimensionality reduces significantly whereas SPAM features are co-occurrences, the elements of the co-occurrence matrices themselves. The improvement in detection accuracy is also due to the fact that the derived features are of higher order compared to SPAM features. An important attribute is that SPAM features are spatial features while in the proposed approach, features are extracted from both spatial and transform domain making it hybrid in a sense. Another notable aspect is that in the proposed feature set, the individual components can be extracted in parallel and then concatenated but SPAM features can be extracted only in a sequential fashion. Thus computational complexity and time complexity issues have been addressed for the Steganalyzer.

V. CONCLUSION

Experimentation has been done with hybrid feature sets collected individually from colour planes and domains and also used in concatenated, composite as well as specific mode to perform steganographic tool detection. The problem has been dealt with two perspectives as important for any pattern recognition problem; effective feature extraction with the features derived from mutually exclusive sets of the feature space still specific in characterizing a steganographic tool and classifier design housing a weighted decision function. As the experimentation involved very minimal payloads, even Generic Steganalysis will be tough. The hybrid composite feature set along with the ensemble classifier managed to achieve 85.25% accuracy in detecting the Steganographic tool employed. This can be a vital clue to the Steganalyst in extracting the embedded secret. Future works in this direction are towards building a hybrid ensemble classifier i.e., different types of classifiers to work along with different specific feature sets aiming to boost the detection accuracy.

REFERENCES

1. Xiaodan Hou, Tao Zhang, 'Universal Blind Steganalysis via Reference Points-Based Local Outlier Factor', 9th IEEE International Conference on Communication Software and Networks, pp. 1287 – 1291, 2017.
2. Roman A. Solodukha and Igor V. Atlasov, 'Modification of RS-steganalysis to Attacks Based on Known Stego-program', Second Russia and Pacific Conference on Computer Technology and Applications, pp. 176-179, Sept. 2017.
3. Fridrich J, Goljan M, Hogea D and Soukal D, 'Quantitative steganalysis of digitalimages: estimating the secret message length', ACM Multimedia Systems Journal, Special issue on Multimedia Security, vol. 9, no. 3, pp. 288-302, 2003.
4. Lu J, Liu F and Luo X, 'Selection of image features for steganalysis based on the fisher criterion', Digital Investigation, vol. 11, no. 1, pp. 57-66, 2014.
5. Hou X, Zhang T, Xiong G, Lu Z and Xie K, 'A novel steganalysis framework of heterogeneous images based on

GMM clustering', Signal Processing: Image Communication, vol. 29, no. 3, pp. 385-399.
6. Wenhao Chen, Li Lin, Min Wuy, and Jennifer Newman, 'Tackling Android Stego Apps in the Wild', Proceedings, APSIPA Annual Summit and Conference, pp. 1564 – 1573, 2018.
7. Bin Li, Zhongpeng Li, Shijun Zhou, Shunquan Tan, and Xiaoling Zhang, 'New Steganalytic Features for Spatial Image Steganography Based on Derivative Filters and Threshold LBP Operator', IEEE Transactions on Information Forensics and Security, Vol. 13, No. 5, May 2018.
8. Sylvia Lilly Jebarani. W, Some Studies on the Usage of Multi – Resolution Transforms for Image Steganography and Steganalysis, Thesis, May 2016.
9. S.Arivazhagan, W.Sylvia Lilly Jebarani, and S. T. Veena, 'Steganographic Tool Detection using Concatenated Moments of Characteristic Functions derived from Colour Models', International Conference on Frontiers of Computational Intelligence, Mar-2016.
10. S.Arivazhagan, W.Sylvia Lilly Jebarani, and S. T. Veena, 'Enormity of Low Volume Blind Steganalysis in Clean uncompressed Image Formats', IEEE International Conference on Circuit, Power &Computing Technologies, Mar-2016.
11. S.Arivazhagan, W.Sylvia Lilly Jebarani, and S. T. Veena, 'Low Volume Generic Steganalysis with improved Generalization', IEEE International Conference on Circuit, Power &Computing Technologies (ICCPCT '16), Mar-2016.
12. Chunfang Yang, Yi Zhang, Ping Wang, Xiangyang Luo, Fenlin Liu and Jicang Lu, 'Steganalysis Feature Subspace Selection Based on Fisher Criterion', International Conference on Data Science and Advanced Analytics, pp. 514-521, 2017.
13. Veenu Bhasin and Punam Bedi, 'Steganalysis of Colored JPEG Images using Ensemble of Extreme Learning Machines', Int. Journal on Recent Trends in Engineering and Technology, Vol. 11, No. 1, July 2014.
14. Mehdi Zohourian, Morteza Heidari, Shahrokh Ghaemmaghami, and Iman Gholampour, 'Towards Higher Detection Accuracy in Blind Steganalysis of JPEG Images', 24th Iranian Conference on Electrical Engineering, pp. 1860-1864, 2016.
15. Weixuan Tang, Haodong Li, Weiqi Luo, and Jiwu Huang, 'Adaptive Steganalysis Based on Embedding Probabilities of Pixels', IEEE Transactions on Information Forensics and Security, Vol. 11, No. 4, pp. 734-745, April 2016.
16. L.Mary Gladence,Karthi,M.,Ravi, T "A novel technique for Multi-class ordinal regression-APDC" IndianJournal of Science and Technology Vol.9/ No.10/March 2016/1-5
17. Saravanan, M.,Jyothi, V.L.," Implementation of getting similarity images using the concept of IWSL "Indian Journal of Science and Technology,Vol 9(22),2016.
18. Vadavalli, A.K., Subhashini, R, ECDH-ECC: A combination of Elliptic Curve Cryptography and Diffie Hellman based cryptography technique for big data security, Journal of Engineering and Applied Sciences, 2018.