International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

# A 3-Way Tensor Framework based Blind Steganalysis using Cyclic Ensemble Classifier

C. Arunvinodh
Research Scholar,
Computer Science and Engineering Dept.
JJT University, Rajasthan

Dr. S. Poonkuntran
Professor, Computer Science and Engineering Dept.
Vellamal College of Engineering and Technology,
Madurai, India

***Abstract*—This manuscript intends a Blind Steganalysis framework which can be applied irrespective of domain specific steganography algorithms. Extracting image features and classification are the significant process in Blind Steganalysis. The framework proposed uses a 3-way tensor model to extract the image features which is important for estimating the embedded change in stego image. Ensemble classification is depicted here uses forward and backward cyclic matricizing which improves the detection accuracy in most of the steganography algorithms. The experimental results evaluated on 3000 images which significantly reduce the false acceptance rate and false rejection rate. Our proposed framework produces an Average false acceptance rate of 1.99% and average false rejection rate of 0.78% based on the pay load when tested with spatial domain steganographic algorithms proposed in [12], [16], [29], [30] and transform domain steganography algorithms such as JPHS, JSTEG, MBS1, MMx, and nsF5.**

***Index Terms:- Spatial Domain, Transform Domain, Steganalysis, Tensor, Ensemble Classifier, Payloads***

## I. INTRODUCTION

Steganalysis is the art of determining concealed data in images. The Steganalysis techniques are classified into two categories. 1. Explicit Steganalysis 2. Blind Steganalysis. Explicit Steganalysis are intended for a targeted Steganographic technique [13], [5] where as in blind steganalysis technique focuses on the stego image irrespective of the steganographic algorithms. It has been acknowledged that most of the research findings paying attention on recognizing the embedded data instead of extracting the data [1],[2],[3],[5],[6].

Steganography can be done in two major domains. 1. Spatial domain. 2. Transform Domain. It has been recognized that design of steganalysis algorithm is focused mainly on Transform Domain [2], [4]. The algorithm which has been intended for Transform domain is moderately working for Spatial Domain [2], [3], [14]. Therefore the highlight of this manuscript is to develop a blind Steganalysis which does not bother about domain specific steganographic algorithms.

Tomas Pevny etal [4] focused their assumptions more on Transform domain. The investigation proposes to concentrate more on spatial domain steganography algorithm as well as JPEG Domain, it is difficult to predict how well the result will compare to Tomas Pevny results. Jan Kodovsky and Jessica Fridrich [1] assumed that both training and testing images were generated based on uniformly distributed payloads. This assumption leads to a development of a steganalysis algorithm which has to identify any distribution (uniform or non-uniform) of stego-payloads. The validation is done by the literature survey based on non-uniform distribution of stego-payloads as follows. T.Pevny etal.[15] highlighted about the challenge of steganalysis researchers for advanced content adaptive steganographic methods. Even though J.fridrich etal. [2] proposes a universal steganography detector which successfully attacked LSB matching revisited algorithm (LSBMR) proposed by LUO etal.[16]. Edge adaptive Image Steganography Based on LSB Matching Revisited (EALSBMR)[17] algorithm was not successfully attacked by [2] because of the adaptive methodology. Shunquan Tan etal. [18] proposes Targeted steganalysis of EALSBMR and it was successful only for the proposed steganography algorithm. There are many adaptive steganography algorithm [39],[40],[41],[42] where an embedding redundancy in LSB matching to select modification direction and takes the dependency of neighbouring pixels into consideration. Since the neighboring pixel dependency is considered the universal steganalysis may be a challenging part in my research [18],[36],[37],[38]. A combined spatial domain embedding and transform domain embedding makes difficulty in the attack [19].

Based on the above justification, this manuscript proposes a unique frame work based on 3 way tensor model which will accompany adaptive steganalysis as well as steganalysis of uniform payload distribution. Also the frame work satisfies the requirement of steganalysis in the spatial domain as well as the JPEG Domain

This paper is organized as follows. In section II, a Frame work has been proposed using 3-way tensor model and we discussed the details of SCI, Forward cycling and backward cycling of matrices and bit change rate estimation. The Results and Discussion claims the successful working of the framework by analyzing in various test bed created based on the steganography algorithms which is mentioned in the section III. Finally the conclusion is summarized in section V.

## II. FRAME WORK

In our system, the frame work proposed in figure 1 clearly shows the importance of tensor representation. The mathematical model of this frame work proposed is adopted from [20], [21] and [22] which give the foundation of tensor representation and manipulation

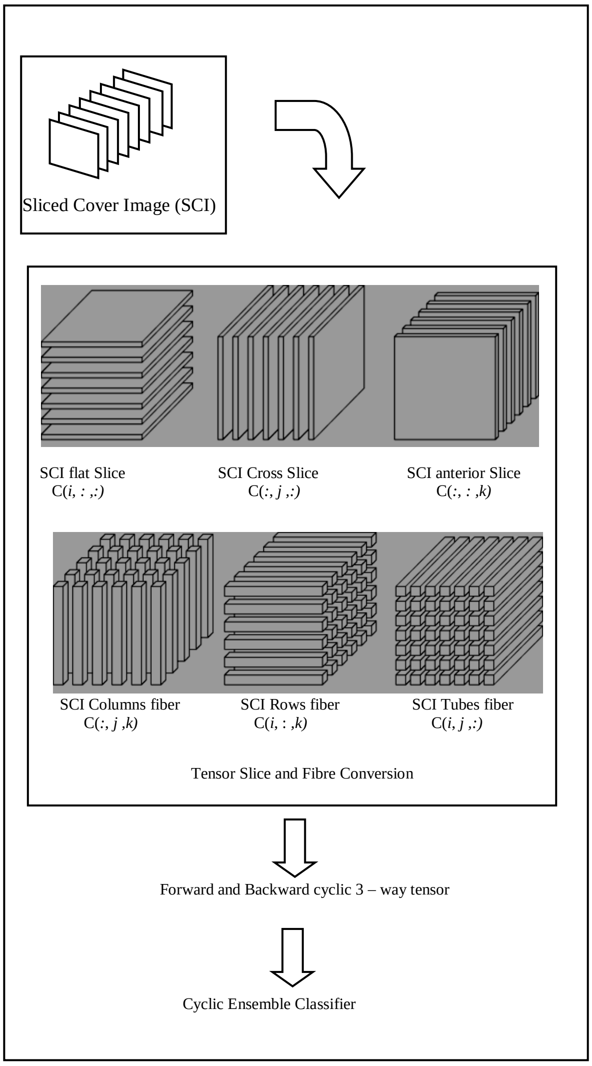



Figure 1: Proposed Frame work

### A. SCI Generation

The first step in SCI Generation based on [35] is to partition the image into N slices, where N is denoted as the number of bit slices. If the image is composed of N-l bit slices, ranging from slice 0 for least significant bit to slice N-l for the most significant bit. In terms of N bit slices, slice 0 contains all the lowest order bits in the bytes comprising the pixels in the image and slice N-1 contains all the high order bits. Therefore by separating the image into bit slices, we immediately have a method of identifying more important and less important information which is suitable for extracting the image features.

The image can be divided into bit slices by the following steps.

- Let I be an image where every pixel value is n-bit long
- Express every pixel in binary using n bits
- Form out of I n binary matrices

where the i-th matrix consists of the i-th bits of the pixels of I.

### B. Tensor Slice and Fibre Conversion

Let $C$ be a Bit Sliced Tensor of dimension

$$C_1 \times C_2 \times \cdots \times C_N. \quad (1)$$

The *order* of $C$ is $N$. The $n$th *dimension* (or *mode* or *way*) of $C$ is of size $C_n$. Let

$C(i,:,:)$ acquiesce the $i$th SCI flat slice,
$C(:,j,:)$ the $j$ th SCI Cross slice, and
$C(:,:,k)$ the $k$th SCI anterior slice
$C(:,j,k)$ yields a column fibers,
$C(i,:,k)$ yields a row fibers, and
$C(i,j,:)$ yields a so-called *tube* fibers

as shown in Figure 1.

Typically, a tensor is matricized such that all of the fibers associated with a particular *single* dimension are aligned as columns of the resulting matrix. In other words, we align the fibers of dimension $n$ of tensor $C$ to be the columns of the matrix. The resulting matrix is typically denoted by $\mathbf{C}_{(n)}$. The columns can be ordered in many ways. As discussed in [21], the ordering can be given as

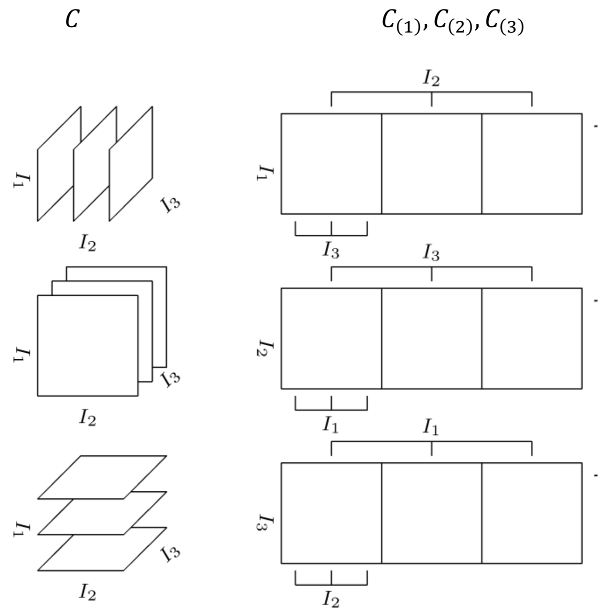



Figure 2: Backward cyclic matricizing a three-way tensor.

$$\{c_1, \ldots, c_L\} = \{n-1, n-2, \ldots, 1, N, N-1, \ldots, n+1\}, \quad (2)$$

and this ordering is named as *backward cyclic*. As per [23], the ordering is specified as follows

$$\{c_1, \ldots, c_L\} = \{n+1, n+2, \ldots, N, 1, 2, \ldots, n-1\}, \quad (3)$$

and this ordering is mentioned as *forward cyclic* or “fc” for short. This framework uses both backward and forward cyclic which is helpful for identifying the bit change rate.

Based on the matricizing process an Nth-order tensor is represented as follows

$$C \in \mathrm{R}^{I1\times I2\times\cdots\times IN} \quad (4)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

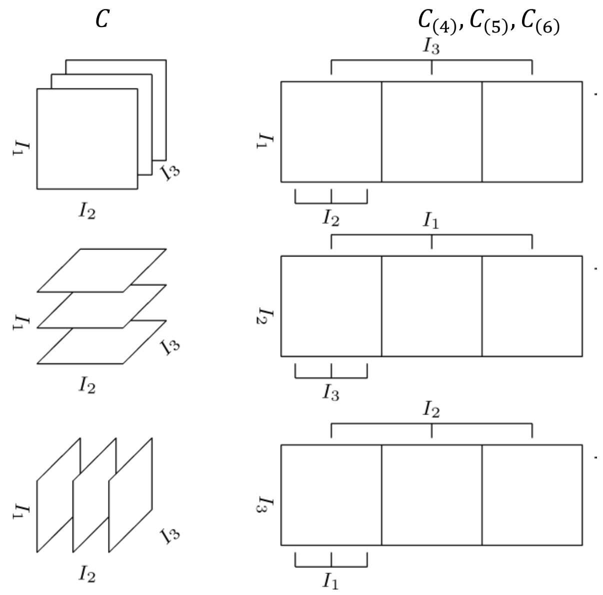



Figure 3. Forward cyclic matricizing a three-way tensor.

The matrix Unfolding is represented as follows.

$$C_{(n)} \in R^{I1In\times(In+1In+2\cdots INI1I2\cdots In-1)\times I2\times\cdots\times IN} \quad (5)$$

Which contains the element $a_{i1i2\cdots iN}$ at the position with row number $i_n$ and column number equal to

$$(i_{n+1} - 1)\ I_{n+2}\, I_{n+3} \ldots.\ I_N\, I_1\, I_2 \ldots..\ I_{n-1} + (i_{n+2} - 1)\ I_{n+3}\, I_{n+4} \ldots.\ I_N\, I_1\, I_2 \ \ldots\ldots.I_{n-1} + (i_N - 1)\ I_1\, I_2 \ldots.I_{n-1}(\, i_1 - 1)\ I_2\, I_3 \ldots\ I_{n-1} \quad (6)$$

## C. Ensemble Classifier

Forward cyclic and backward cyclic matricizing creates 6 matrices from 3-way tensor. Rate of intensity change in a particular region of an image always have slight variation. Therefore by analyzing the change in the bit rate, image features can be extracted. To estimate the embedding change rate we use a methodology called as hamming distance.

Let us take the same elements which are shown in the previous section. The element $a_{i1i2\cdots iN}$ at the position with row number $i_n$ and column number equal to

$$(i_{n+1} - 1)\ I_{n+2}\, I_{n+3} \ldots.\ I_N\, I_1\, I_2 \ldots..\ I_{n-1} + (i_{n+2} - 1)\ I_{n+3}\, I_{n+4} \ldots.\ I_N\, I_1\, I_2 \ \ldots\ldots.I_{n-1} + (i_N - 1)\ I_1\, I_2 \ldots.I_{n-1}(\, i_1 - 1)\ I_2\, I_3 \ldots\ I_{n-1} \quad (7)$$

which is XORed with row number $i_{n+1}$ and the corresponding column number is

$$(i_{n+2} - 1)\ I_{n+3}\, I_{n+4} \ldots.\ I_N\, I_2\, I_3 \ldots..\ I_{n-2} + (i_{n+3} - 1)\ I_{n+4}\, I_{n+5} \ldots.\ I_N\, I_2\, I_3 \ \ldots\ldots.I_{n-2} + (i_N - 1)\ I_2\, I_3 \ldots.I_{n-2}(\, i_2 - 1)\ I_2\, I_3 \ldots\ I_{n-1} \quad (8)$$

The number of change in bits can be estimated by counting the number of ones. This process can be repeated for all unfolded matrices.

The detector is designed with the help of an ensemble classifier method known as bagging which is proposed in [3],[43]. Our proposed framework uses bagging method to create classifiers based on forward and backward cyclic matricizing. To describe our cyclic ensemble classifier, we introduce the following modified notations.

The backward cyclic ensemble classifier is denoted as $B_m$ , where $m = 1 \ldots..M$. Then 3 fibers for backward cyclic ensemble classifier are denoted as $B_m^{C_1}, B_m^{C_2}, B_m^{C_3}$

The Forward cyclic ensemble classifier is denoted as $F_m$ , where $m = 1 \ldots..M$. Then 3 fibers for backward cyclic ensemble classifier are denoted as $F_m^{C_1}, F_m^{C_2}, F_m^{C_3}$.

The prediction of the complex classifier for Backward cyclic and Forward cyclic Ensemble Classifier can be represented as follows

$$B^{C_1}(d_i) = sign\left(\sum_{m=1}^{M} \alpha_m\, B_m^{C_1}(\,d_i)\right) \quad (9)$$

$$B^{C_2}(d_i) = sign\left(\sum_{m=1}^{M} \alpha_m\, B_m^{C_2}(\,d_i)\right) \quad (10)$$

$$B^{C_3}(d_i) = sign\left(\sum_{m=1}^{M} \alpha_m\, B_m^{C_3}(\,d_i)\right) \quad (11)$$

The prediction of the complex classifier for Forward cyclic and Forward cyclic Ensemble Classifier can be represented as follows

$$F^{C_1}(d_i) = sign\left(\sum_{m=1}^{M} \alpha_m\, F_m^{C_1}(\,d_i)\right) \quad (12)$$

$$F^{C_2}(d_i) = sign\left(\sum_{m=1}^{M} \alpha_m\, F_m^{C_2}(\,d_i)\right) \quad (13)$$

$$F^{C_3}(d_i) = sign\left(\sum_{m=1}^{M} \alpha_m\, F_m^{C_3}(\,d_i)\right) \quad (14)$$

*Algorithm 1 Backward Cyclic Ensemble Classifier*

1. *For $T_b$=1 to 3*
2. *Initialisation of the training set D*
3. *for m = 1, ..., M*
   a. *Creation of a new set $D_m$ of the same size D by random selection of training examples from the set D*
   b. *Learning of a particular classifier*

      $B_m$: $D_m^{C_{T_b}} \rightarrow R$

      *by a given machine learning algorithm based on the actual training set $D_m$.*
4. *Compound classifier B is formed as the aggregation of detailed classifiers $B_m$: m = 1, ...,M and an example $d_j$ is classified to the class $p_j$ in accordance with the number of votes obtained from particular classifiers $B_m$. and thus it is represented as*

$$B^{C_{T_b}}(d_i, p_j) = sign\left(\sum_{m=1}^{M} \alpha_m\, B^{C_{T_b}}(\,d_i, p_j)\right)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

*Algorithm 2 Forward Cyclic Ensemble Classifier*

1. *For $T_f$=1 to 3*
2. *Initialisation of the training set D*
3. *for m = 1, ..., M*
   a. *Creation of a new set $D_m$ of the same size D by random selection of training examples from the set D*
   b. *Learning of a particular classifier*

      $$B_m: D_m^{C_{T_f}} \rightarrow R$$

      *by a given machine learning algorithm based on the actual training set $D_m$.*
5. *Compound classifier F is formed based on the aggregation of detailed classifiers $F_m$: m = 1, ...,M and an example $d_j$ is classified to the class $p_j$ in accordance with the number of votes obtained from particular classifiers $F_m$. and thus it is represented as*

$$B^{C_{T_f}}(d_i, p_j) = sign\left(\sum_{m=1}^{M} \alpha_m\, B^{C_{T_f}}(d_i, p_j)\right)$$

## III. RESULTS AND DISCUSSIONS

Since we unfolded the matrix we organized our database as equally distributed training and testing set. Each training and testing set consist of $B^{C_1}(d_i)$, $B^{C_2}(d_i)$ , $B^{C_3}(d_i)$ , $F^{C_1}(d_i)$, $F^{C_2}(d_i)$ and $F^{C_3}(d_i)$. The framework proposed is effectively evaluated in 3000 images in the database provided by BOWS-2[34]. To construct the steganalyzer an approximation of an unknown function $\Phi: D\ x\ C \rightarrow \{true, false\}$ where D is the set of images of stego and cover image and $C = \{C_1, \dots\dots C_{|C|}$ is the set of predefined groups. The value of the function Φ for a pair $\langle d_i, c_j \rangle$ is true if the image $d_i$ belongs to group $C_j$. The function $\Phi: D\ x\ C \rightarrow \{true, false\}$ which approximates Φ is called a classifier.

For the entire algorithm the stego image bit change scatters a lot when it compared with the input image bit change. In this paper we use False Acceptance Rate (FAR) as the framework incorrectly detected as the stego image and False Rejection Rate (FRR) as the framework incorrectly rejected that the image is a cover image. Table I and II clearly shows that the average detection rate increases as the payload increases. The FAR and FRR increases only when the payload increases from 2.3 as shown in the figure 1 and 2. Almost for all unfolded matrix the average detection rate is 65% irrespective of the payload. The framework is applied to spatial domain steganography algorithms based on [12], [16], [29] and[30] which is shown in Table I. The FAR and FRR is very low at an average of 2.4% and 3.3%. The framework is applied to Transform Domain steganography algorithms based on JPHS [31], Jsteg [28], MBS1[27], MMx[32], nsF5 [33] which is shown in Table II. The FAR and FRR is very low at an average of 1.7% and 1.2%.

Table I: Detection Analysis of Spatial Domain Algorithms

| Algorithm | Average Detection Rate | Spatial Domain | |
|---|---|---|---|
| | | Average False Acceptance Rate | Average False Rejection Rate |
| [12] | 77.52% | 1.6% | 0.05% |
| [16] | 80.1% | 312% | 0.67% |
| [29] | 74.76% | 4.55% | 3.22% |
| [30] | 78.03% | 3.21% | 3.74% |

Table II: Detection Analysis of Transform Domain Algorithms

| Algorithm | Average Detection Rate | Spatial Domain | |
|---|---|---|---|
| | | Average False Acceptance Rate | Average False Rejection Rate |
| JP Hide&Seek (JPHS) [31] | 88.23% | 0.042% | 0 |
| Jsteg [28] | 94.51% | 0.86% | 0.033% |
| MBS1 [27] | 89.39% | 0.43% | 0.006% |
| MMx [32] | 86.12% | 1.08% | 0.56% |
| nsF5 [33] | 85.28% | 1.42% | 0.62% |

## IV. CONCLUSION

In this paper, a novel framework has been proposed based on 3 way tensor model. As a start of this invention, excellent results obtained for algorithms with an average detection rate of 65% irrespective of payloads. Based on the spatial domain an average detection rate achieved is 77.6% and for Transform domain we achieved is 88.71%. Also the framework was successful in both uniform and non uniform distribution of Stego-payloads. The disadvantage was the low average detection rate for [29] & [30] for spatial domain steganography algorithms and [27], [32] & [33] for transform domain steganography algorithms.

To increase the average detection rate and to decrease the Average false acceptance rate and average false rejection rate, the proposed framework can be applied to regions in an image.

## V. REFERENCES

[1] Jan Kodovský and Jessica Fridrich, "Quantitative Steganalysis Using Rich Models", Proc. SPIE 8665, Media Watermarking, Security, and Forensics, March 22, 2013.
[2] J. Fridrich and J. Kodovský. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3):868–882, June 2012.
[3] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media", IEEE Transactions on Information Forensics and Security , 7(2):432–444, April 2012
[4] T. Pevný, J. Fridrich, and A. Ker, "From blind to quantitative steganalysis," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 445–454, Apr. 2012.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 11, November-2016

Table I

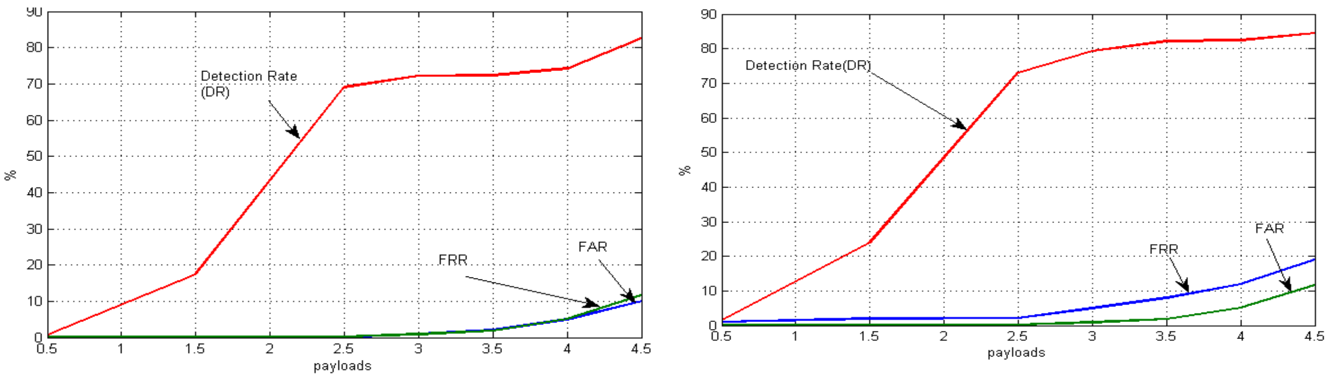
Training and testing details with payload increasing from 0.5 to 4.5 for $B^{C_1}(d_i)$, $B^{C_2}(d_i)$ and $B^{C_3}(d_i)$

| payloads | $B^{C_1}(d_i)$ | | | | $B^{C_2}(d_i)$ | | | | $B^{C_3}(d_i)$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | FAR % | FRR % | DA | DR % | FAR % | FRR % | DA | DR % | FAR % | FRR % | DA | DR % |
| 0.5 | 0.0 | 0.000034 | 1 | 0.8 | 1 | 0.00278 | 2 | 1.4 | 0 | 0.0033343 | 7 | 10.4 |
| 1.5 | 0.01 | 0.01461 | 4 | 17.5 | 2.01 | 0.01461 | 4 | 23.9 | 1.765 | 0.0151643 | 9 | 27.9 |
| 2.5 | 0.1 | 0.15275 | 16 | 69.1 | 2.1 | 0.15275 | 20 | 73 | 3 | 0.1533043 | 25 | 77 |
| 3 | 1.0 | 0.92694 | 16 | 72.2 | 5 | 0.92694 | 22 | 79.34 | 8 | 0.9274943 | 27 | 92.34 |
| 3.5 | 2.0 | 1.86436 | 16 | 72.4 | 8 | 1.86436 | 22 | 82.1 | 10 | 1.8649143 | 27 | 93.12 |
| 4 | 5.0 | 5.16743 | 19 | 74.3 | 12 | 5.16743 | 25 | 82.4 | 13 | 5.1679843 | 30 | 93.67 |
| 4.5 | 10.0 | 11.778 | 19 | 82.7 | 19 | 11.778 | 27 | 84.54 | 22 | 11.778554 | 32 | 94.55 |

Table II

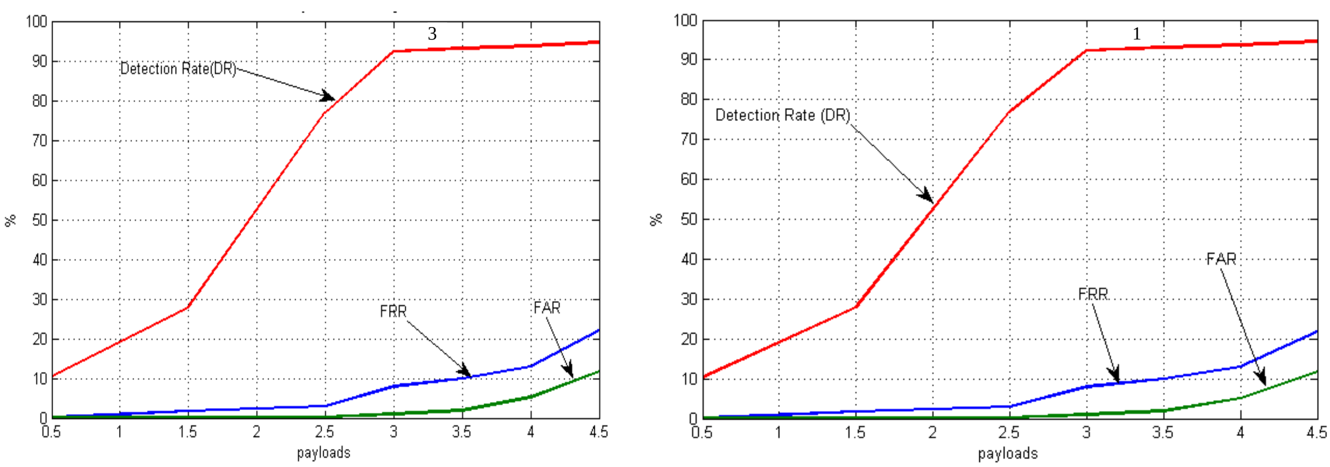
Training and testing details with payload increasing from 0.5 to 4.5 for $F^{C_1}(d_i)$, $F^{C_2}(d_i)$ and $F^{C_3}(d_i)$

| payloads | $F^{C_1}(d_i)$ | | | | $F^{C_2}(d_i)$ | | | | $F^{C_3}(d_i)$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | FAR % | FRR % | DA | DR % | FAR % | FRR % | DA | DR % | FAR % | FRR % | DA | DR % |
| 0.5 | 0 | 0.0033343 | 7 | 10.4 | 0 | 0 | 11 | 12.0789 | 1 | 0.00278 | 0 | 0.1544 |
| 1.5 | 1.765 | 0.0151643 | 9 | 27.9 | 1.3 | 0 | 14 | 39.543 | 2 | 0.01461 | 2 | 22.6544 |
| 2.5 | 3 | 0.1533043 | 25 | 77 | 2 | 1.3445 | 26 | 58.23 | 2 | 0.15275 | 18 | 71.7544 |
| 3 | 8 | 0.9274943 | 27 | 92.34 | 3.22 | 1.6768 | 29 | 85.66734 | 5 | 0.92694 | 20 | 78.0944 |
| 3.5 | 10 | 1.8649143 | 27 | 93.12 | 4 | 1.92354 | 31 | 94.4524 | 6 | 1.86436 | 20 | 80.8544 |
| 4 | 13 | 5.1679843 | 30 | 93.67 | 6.78 | 2.13 | 34 | 95.3489 | 8.3 | 5.16743 | 23 | 81.1544 |
| 4.5 | 22 | 11.778554 | 32 | 94.53 | 7.566 | 4 | 39 | 96.2289 | 11 | 11.778 | 25 | 83.2944 |

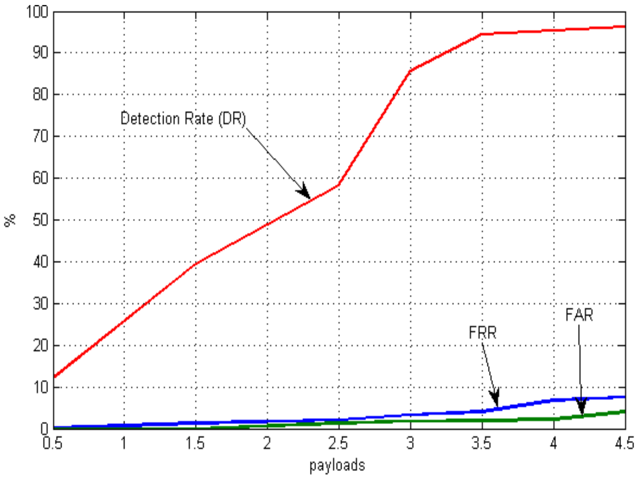



(a) (b)

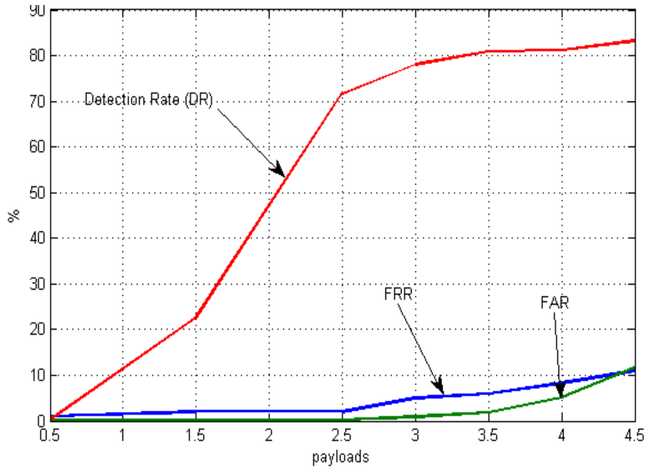
Figure 1: Detection rate on payloads for $(a)B^{C_1}(d_i)$, $(b)B^{C_2}(d_i)$




(a) (b)




(c)




(d)

Figure 2: Detection rate on payloads for $(a)B^{C_3}(d_i)$, $(b)F^{C_1}(d_i)$, $(c)F^{C_2}(d_i)$ and $(d)F^{C_3}(d_i)$


[5] Chunfang Yang, Fenlin Liu, Xiangyang Luo, and Ying ZengPixel, "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions On Information Forensics And Security, vol. 8, no. 1, January 2013

[6] Chunfang Yang, Fenlin Liu1, Xiangyang Luo1, Ying Zeng,"Fusion of Two Typical Quantitative Steganalysis Based on SVR", Journal Of Software, Vol. 8, No. 3, March 2013

[7] Tomas Pevny and Andrew D. Ker, "The Challenges of Rich Features in Universal Steganalysis", Proc. SPIE 8665, Media Watermarking, Security, and Forensics, 86650M, March 22, 2013.

[8] Ziwen Sun, Hui Li, "Quantitative Steganalysis Based on Wavelet Domain HMT and PLSR", 10th IEEE International Symposium on Distributed Computing and Applications to Business, Engineering and Science, 2011

[9] Gikhan Gul and Faith Kurugollu,"SVD-Based Universal Spatial Domain Image Steganalysis", IEEE Transactions on Information Forensics and Security,Vol.5,No.2,June 2010

[10] Changxin Liu, Chunjuan Oujang,"Image Steganalysis Based on Spatial Domain and DWT Domain Features", IEEE Second International Conference on Network Security, Wireless Communications and Trusted Computing, 2010.

[11] Souvik Bhattacharyya and Gautam Sanyal, "Steganalysis of LSB Image Steganography using Multiple Regression and Auto Regressive (AR) Model", Int. J. Comp.Tech. Appl., Vol 2 (4), 1069-1077

[12] Zhenhao Zhu, Tao Zhang, Baoji Wan, "A special detector for the edge adaptive image steganography based on LSB matching revisited", 2013 10th IEEE International Conference on Control and Automation (ICCA)

[13] Weiqi Luo, Yuangen Wang, Jiwu Huang, "Security analysis on spatial +_1Steganography for jpeg decompressed images", IEEE Signal Processing Letters, (Volume:18 ,Issue: 1)

[14] Tomas Pevny,Tomas Filler, Patrick Bas, "Using high-dimentional image models to perform undetectable steganography" , Lecture Notes in Computer Science Volume 6387,2010,pp 161-177

[15] Mielikainen, " LSB Matching revisited", Signal Processing Letters, IEEE (Volume:13 , Issue: 5), May 2006

[16] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions On Information Forensics And Security, vol. 5, no. 2, june 2010

[17] Shunquan Tan, "Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting", Signal Processing Letters, IEEE(Volume:19 ,Issue: 6), June 2012

[18] Chao Wang, Xiaolong Li, Bin Yang, Xiaoqing Lu, Chengcheng Liu, " Content- adaptive approach for reducing embedding impact insteganography", IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), 14-19 March 2010

[19] Yi-zhen Chen, Zhi Han, Shu-ping Li, Chun-hui Lu, Xiao-Hui Yao, "An Adaptive Steganography algorithm based on block sensitivity vectors using HVS features" 3rd International Congress on Image and Signal Processing (CISP) 16-18 Oct. 2010

[20] Brett w. Bader and Tamara g. Kolda, "MATLAB Tensor Classes for Fast Algorithm Prototyping" ACM Transactions on Mathematical Software, Volume 32 Issue 4, December 2006 Pages 635-653

[21] De Lathauwer, L., De Moor, B., and Vandewalle, J 2000a, "A multilinear singular value decomposition" SIAM J. Matrix Anal. Appl. 21, 4, 1253–1278, 2000.

[22] De Lathauwer, L., De Moor, B., and Vandewalle, J. 2000b, " On the best rank-1 and rank- (R1, R2, . . . , RN ) approximation of higher-order tensors". SIAM J. Matrix Anal. Appl. 21, 4, 1324–1342, 2000.

[23] Kiers, H. A. L, "Towards a standardized notation and terminology in multiway analysis" .J. Chemometrics 14, 105–122., 2000

[24] The MathWorks, Inc. 2004a. Documentation: MATLAB: Programming: Classes and objects *http://www.mathworks.com/access/helpdesk/help/techdoc/matlabprog/ch11 mat.html* .

[25] The MathWorks, Inc. 2004b. Documentation: MATLAB: Programming: Multidimensional arrays. *http://www.mathworks.com/access/helpdesk/help/techdoc/matlab prog/ch dat32.html#39663* .

[26] www.sandia.gov/~tgkolda/**Tensor**Toolbox/

[27] P. Sallee, "Model-based steganography," in Digital Watermarking, 2nd International Workshop, ser. Lecture Notes in Computer Science, T. Kalker, I. J. Cox, and Y. M. Ro, Eds., vol. 2939. Seoul, Korea: Springer-Verlag, New York, October 20–22, 2003, pp. 154–167.

[28] D. Upham, http://zooid.org/~paul/crypto/jsteg/.

[29] Guangjie Liu, Zhan Zhang and Yuewei Dai, "Improved LSB-matching Steganography for Preserving Second-order Statistics", Journal of Multimedia, vol. 5, no. 5, October 2010

[30] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," in Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, E. J. Delp and P. W. Wong, Eds., vol. 6072, San Jose, CA, January 16–19, 2006, pp. W1–W10.

[31] A. Latham, http://linux01.gwdg.de/~alatham/stego.html.

[32] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in Information Hiding, 8th International Workshop, ser. Lecture Notes in Computer Science, J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, Eds., vol. 4437. Alexandria, VA: Springer-Verlag, New York, July 10–12, 2006, pp. 314–327.

[33] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities," in Proceedings of the 9th ACM Multimedia & Security Workshop, J. Dittmann and J. Fridrich, Eds., Dallas, TX, September 20–21, 2007, pp. 3–14.

[34] http://bows2.ec-lille.fr/

[35] C.Arun Vinodh, Nisha P Nair, S.Poonkuntran, "A Lossless Compression Using BPS for Fingerprint Images", Proceedings of the IEEE Sponsored International Conference on Emerging Trends in

Computing ICETIC 2009, Virudhunagar, Tamilnadu, India, Page No. 147-150, 8-10 January 2009.
[36] Poonkuntran Shanmugam, Rajesh R.S, Eswaran Perumal, "A Reversible Watermarking with Low Warping: An Application to Digital Fundus Image", Proceedings of the International Conference on Computer and Communication Engineering, ICCCE 2008, Kuala Lumpur, Malaysia, Page No. 472-477, May 13-15,2008. (Indexed by IEEE Explore, IEEE Catalog Number: CFP0839D, ISBN: 978-1-4244-1692-9, Library of Congress: 2007936379).
[37] S.Poonkuntran, R.S. Rajesh, P.Eswaran, "A Robust Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding", Proceedings of the IEEE Sponsored International Conference on Emerging Trends in Computing ICETIC 2009, Virudhunagar, Tamilnadu, India, Page No. 433-436, 8-10 January 2009.
[38] S.Poonkuntran, R.S. Rajesh, P.Eswaran, "Reversible, Multilayered Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding", Proceedings of the IEEE International Advanced Computing Conference IACC 2009, Patiala, Punjab, Page No. 2583-2587, 6-7 March 2009. (ISBN: 978-981-08-2465-5).
[39] S.Poonkuntran, R.S. Rajesh, P.Eswaran, "Analysis of Difference Expanding Method for Medical Image Watermarking", Proceedings of 2009 International Symposium on Computing, Communication and Control, Singapore, Page No. 30-34, 9-11 October 2009. (ISBN: 978-9-8108-3815-7).
[40] S.Poonkuntran, R.S.Rajesh, P.Eswaran, "Imperceptible Watermarking Scheme for Fundus Images Using Intra-Plane Difference Expanding", International Journal on Computer and Electrical Engineering, Volume No. 1, Issue 4, Page No. 442-446, Oct 2009. (ISSN:1793-8198 for online 1793-8163 for Print).
[41] S.Poonkuntran, R.S.Rajesh, P.Eswaran, "Reversible, Imperceptible, Semi Fragile Watermarking Scheme for Digital Fundus Image Authentication", International Journal on Signal and Imaging System Engineering (IJSISE-Inderscience Publishers), Volume No.3, Page No. 116-125, 2010
[42] S.Poonkuntran, R.S.Rajesh, "Chaotic Model Based Semi Fragile Watermarking Using Integer Transforms for Digital Fundus Image Authentication" Springer International Journal on Multimedia Tools and Applications, Volume No.68, Issue No.1, Page No. 79-93, Jan 2014. ISSN 1380-7501, DOI 10.1007/s11042-012-1227-5, Springer Publications.
[43] Kristína Machová, František Barčák, Peter Bednár, "A Bagging Method using Decision Trees in the Role of Base Classifiers", Acta Polytechnica Hungarica, Vol. 3, No. 2, 2006

**C.Arunvinodh** received his B.E degree in Electrical and Electronics Engineering from Annamalai University, India in 2002 and the M.Tech. degree in Computer and Information Technology from Manonmaniam Sundaranar University, India in 2005. He is currently doing his Ph.D in JJT University, Rajasthan. He is having 9 years of experience in teaching. He has published papers in 1 international journal, 4 International conference and 2 National Conferences. His research interests include Information Security, Digital image processing and Biometrics.

**Dr. S. Poonkuntran** received B.E in Information Technology from Bharathidasan University, Tiruchirapalli, India in 2003, M.Tech in Computer and Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2005 and Ph.D in the department of computer science and engineering, Manonmaniam Sundaranar University, Tirunelveli, India in 2011. He is having 10 years of experience in teaching and research. He is a life time member of IACSIT, Singapore, CSI, India and ISTE, India. He has published papers in 4 national conference, 22 international conferences, 1 national journal and 10 international journals on image processing, information security and soft computing. Presently he is working on Computer Vision for under water autonomous vehicles and Information Security for Healthcare Information Systems. His areas of research interest include digital image processing, soft computing and energy aware computing in computer vision.