A hybrid KNN & ANN based approach for video steganalysis

Gargi Kalia
M.Tech CSE
USET, RBU
Mohali, India
Surbhi Gupta
Associate Professor, Deptt. of CSE,
USET, RBU
Mohali, India

Abstract*—Steganalysis is an art of detecting secret message under a cover image. Several researchers have proposed several techniques to hide the data efficiently. However, there is a room for a novel approach which can hide the data with high accuracy, correction and reduce error rate. Considering this fact, this paper proposed a new approach which is based on Artificial neural network. Initially, three steps are followed such as data hiding, Feature extraction and classification. Proposed approach utilizes several feature extraction approach to extract the features from video frames. In order to conclude the performance of proposed technique, comparison has made with the traditional technique. The simulation analysis confirmed that proposed technique outperforms the traditional technique in view of different performance parameters. The probability of correction and detection has increased with decrease in probability of error rate.

***Keywords*— Steganalysis, Artificial Neural Network, Discrete Wavelet Transform, classification**

I. INTRODUCTION

Steganalysis is a process that detects the hidden information from the carrier signals without affecting the originality of the carrier signal whether it is image, video or audio [1]. The objective of steganalysis is to gather the enough evidence regarding information that is present in carrier signals. Steganalysis should not be confused with reversible data hiding process [2]. Reversible Data Hiding (RDH) is a process to restore the carrier signal fully after extracting the hidden message from it whereas steganalysis aims to extract the hidden message from the carrier signal without distorting the carrier signals [3]. In steganalysis the emphasis is laid on hidden message whereas in reversible data hiding the emphasis is on carrier signals[4]. The necessity of steganalysis is increasing day by day with the advancement in the technologies. Steganalysis has various applications for different purpose from which the security concern is the major one [5]. The domains such as computer forensics, tracking illegal activities, Cyber Warfare etc. utilize the steganalysis [6]. From the beginning of data hiding behind various carrier signals, the researchers start focused on the concept of steganalysis. Much advancement has been made in steganography but much is yet to be achieved for steganalysis. Following are some techniques that can be used for steganalysis [7].

II. RELATED WORK

In 2000, Fridrich et al. in [10] proposed a method which was used to detect LSB embedding in 24 bit color images. This method exploited the fact of decreasing the number of colored pairs after the process of embedding. As the proposed method was based on the number of unique colored pairs, so there were several constraints that restricted the success of the method. Several authors focused on the infeasibility of embedding messages in digital joint photographic expert group (JPEG) format. This work was proved to be advantageous to detect the pseudorandom binary message that was randomly distributed in the color images. In 2001 and 2002 [8, 9] image quality metrics as well as multivariate regression analysis were used by different authors. Basically, these methods provided detection of presence of converted data in an image. The experimental analysis was performed and distance was evaluated between watermarked and filtered version. From the proposed technique, it was concluded that distance between watermarked image and filtered image was greater than in comparison with the non-watermarked image and filtered image. The metrics related to image quality were sensitive to different embedding schemes which were chosen to measure the change happen in distance. The weighted sum of the distance was measured using the mentioned metrics that was calculated and then comparison was done with a threshold in order to identify the hidden messages. It accurately recognized the images that were marked by various watermarked techniques.

Similar implementation had been done in 2001, [8] by Aycibas et al. by using binary similarity analysis to evaluate the correlation interference among 7th and 8th bit plane that occurred because of Least Significant Bit (LSB) embedding. The temporal filters were utilized so that the used watermark corresponding to each and every frame could be detected in a best way. The advantage was that it was proved to be effective technique for classifying the stego and cover image. In 2005, [14] Trivedi et al. Proposed locating the secret key in images in which the data is embedded by using the sequential embedding process [14]. The major focus was to analyze the performance of the spread spectrum technique in order to prove that it has some statistical properties which were an aid for active steganalysis.

In contrast to this study, Fridrich et al.[11] recommended a different proposal for measuring the length of the message in images by using various steganography algorithms. It was evaluated that the proposed technique was able to calculate the message length effectively in JPEG format using F5. The major contribution was that it used the sequential embedding system since key management in this mechanism was quite easy and simple.

Su et al. in 2005 [12] proposed a mathematical formulation based model for linear collusion in frames extracted from videos along with the statistical measurements [15]. It was proved that if the watermark embedding was done individually with little correlation in the host sequence then the removal of the watermark became efficient. The corresponding solution also worked even if the collision model fails to detect the watermark. The major advantage of this work is the initiative taken to represent the linear collusion model for recognizing the watermark in a video sequence.

III. LIMITATION OF EXISTING SUPPORT VECTOR MACHINE (SVM) BASED STEGANALYSIS

Steganalysis is usually accomplished using the classifiers.. Classifier makes the classification by analyzing the video frame that it has hidden message or not. In existing work of steganalysis, the author implements the Support Vector Machine based models for the purpose of classification, but there are some limitations.

1. SVMs do not perform well on highly skewed/imbalanced data sets. These are training data sets in which the number of samples that fall in one of the classes far outnumbers those that are a member of the other class.
2. SVMs are also not a good option especially if we have multiple classes. Ultimately in this case, we get back to a binary classifier and then use some kind of a voting mechanism to classify a sample to one of the classes.
3. If the data sets are such that they arrive in batches and every time we want to increment our learning model, then SVMs are not a good option for incremental learning.

Due to these limitations the SVM is not effective approach for the video steganalysis as number of variation are there So, the need is to provide a system with effective classification process.

IV. PROPOSED WORK

From the literature, it is observed that the Support Vector Machine (SVM) is used as an alternative to the classifiers in order to detect the frame with message in existing technique. Similarly, a new approach has been proposed by hybridizing the K-Nearest Neighbor (KNN) and Artificial Neural Network (ANN). The KNN classifier works on the basis of the clustering . Then the clustered data will be given to the ANN for the classification which will improve the classification process with much effectiveness and the high accuracy rate as KNN has no limitation of the classes as it was in the SVM.

Along with this as a data hiding approach the enhanced spread spectrum approach will be applied so data can be encoded in the video frame in a better manner and the advanced system will provide better results with respect to traditional approaches.

V. METHODOLOGY

The proposed method is divided into three different blocks such as Data hiding, Feature extraction and Classification. Each block performs some steps which have been shown below:

A. *Data Hiding*

1. Initially, the process starts by selecting a video whose frames needs to be extracted.
2. From the selected video, frames are extracted in which watermark is to be hidden.
3. Correspondingly, a watermark is generated and collaborated with the extracted frame and thus data hiding process is accomplished.
4. Lastly, encrypted video is acquired. As shown in figure 1.

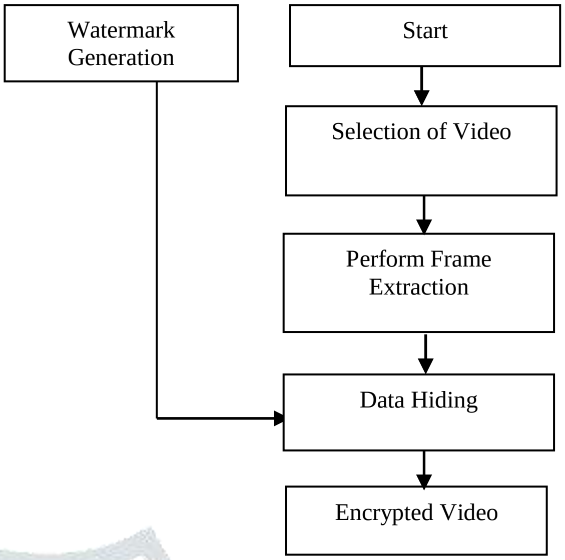

Figure 1 Block Diagram of Data Hiding

B. *Feature Extraction*

1. In the process of feature extraction, encrypted video is treated as input headed for processing.
2. Required features are extracted from the encrypted video using different feature extraction approaches.
3. The Local Binary Pattern (LBP) feature extraction approach, Edge detection, Kurtosis and Variance is applied on the video. The Discrete Wavelet Transformation (DWT) approach is also applied to the video for feature extraction whose further features as H (Horizontal), V (Vertical) and D (Diagonal) are also extracted. Further Singular Value Decomposition (SVD) features are extracted from H, V and D and then K1, K2 and K3 features are acquired.
4. Extracted features through different extraction techniques are headed to the ANN model for training purpose.

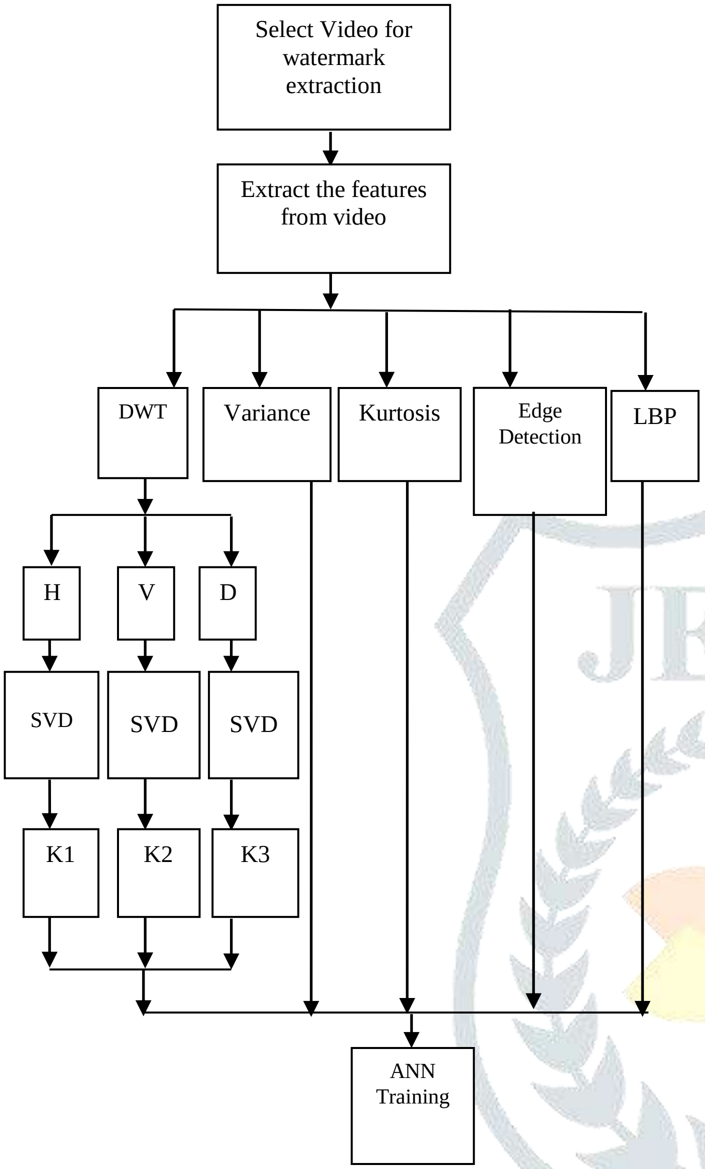
Select Video for watermark extraction
Extract the features from video
DWT
Variance
Kurtosis
Edge Detection
LBP
H
V
D
SVD
SVD
SVD
K1
K2
K3
ANN Training

Figure 2 Block Diagram of Features Extraction and ANN training

C. *Classification*

After extracting the features from the encrypted video, classification is performed. The steps followed in classification are as follows (Fig 3:

1. The video's frame is forwarded to the ANN for classification.
2. ANN checks whether a hidden message contained in the frame or not. If yes, then hidden message, gain factor and original frame estimation is performed and if no, then remain the frame is kept as it is.

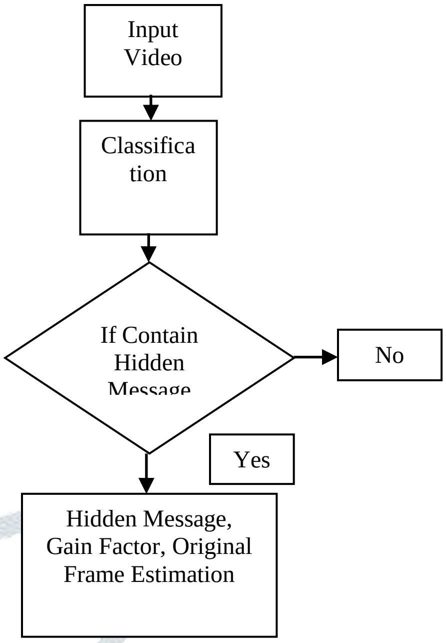
Input Video
Classification
If Contain Hidden Message
No
Yes
Hidden Message, Gain Factor, Original Frame Estimation

Figure 3 Block Diagram of Classification

VI. ALGORITHM OF PROPOSED TECHNIQUE

The algorithm used for steganalysis is shown as:

Step 1: Read the video from the directory and extract the frames from the selected video.

Step 2: Generate watermark i.e. random matrix of values which will be used to hide under a cover image.

Step 3: Initiate multiplicative and additive Data hiding process. Equations (1,2,3) are used for the evaluation of both rules as:

$$y_i = x_i + \alpha . w_i \ldots\ldots\ldots\ldots\ldots (1)$$

$$y_i = x_i(1 + \alpha . w_i) \ldots\ldots\ldots\ldots\ldots\ldots . (2)$$

$$y_i = x_i . e^{\alpha . w_i} \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

In the above equation, alpha is the gain factor and x_i, w_i and y_i are considered as the ith samples of cover signal, watermark data and watermarked signal correspondingly. Additive rule is defined in the equation 1 and equation 2 and 3 shows multiplicative rules.

Step 4: Calculate LBP and edge features of cover as well as stego images. Canny edge detector has used to calculate the edges of the images. The equation (4) used for the evaluation is:

$$G = \sqrt{G_x^2 + G_y^2} \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

In the equation 4, G_x is the horizontal direction and G_y is the vertical direction values for first derivative.

Step 5: Apply DWT transformation on the selected frames. This technique acquires four different features such as Approximation, Horizontal, Vertical and Diagonal as A, H, V and D features respectively. Further applied SVD feature extraction technique over H, V and D features and evaluate F factor as per equation (5).

$$K_K = \frac{\sigma_{max}(A_k)}{\sigma_{min}(A_k)}, K = 2,3,4\ldots.. (5)$$

σ_{max} and σ_{min} are considered as the maximum and minimum singular values of A_k respectively.

Step 6: Evaluate variance estimator of the sample set by using equation (6):

$$s^2 = \frac{1}{N-1}\sum_{i=1}^{N}(z_i - \bar{z})^2, \text{ where} \bar{z} = \frac{1}{N}\sum_{i=1}^{N} Z_i \ldots\ldots\ldots.(6)$$

Step 7: Calculate Kurtosis value of the sample set as given in equation (7):

$$b_2 = \frac{\left(\frac{1}{N}\right)\sum_{i=1}^{N}(Z_{i}-\bar{Z})^4}{(\left(\frac{1}{N}\right)\sum_{i=1}^{N}(Z_{i}-\bar{Z})^2)^2}\ldots\ldots\ldots\ldots\ldots(7)$$

Step 8: Compute Peak Distribution Function and its maximum peak value as per equation (8):

Peak = max $f_R\ (r)$………….(8)

Step 9: Perform classification using ANN classifier where training has taken place. For the proposed work, Cascade forward back propagation network is implemented.

Step 10: now check the occurrence of hidden data under a cover image. Considering this fact, extract the frames from the selected video.

Step 11: Perform ANN training to evaluate whether the data has been hidden under the cover image or not.

Step 12: Estimate different parameters such as Alpha, Watermarked image and Original frame in case of hidden data.

VII. RESULTS AND DISCUSSION

The graph in figure 4 represents the comparison of proposed and existing method with respect to obtained probability error. The x axis in graph shows the values of $\alpha_A$which ranges from 1 to 5. The y axis depicts the values of probability of error (in % age) from 0 to 0.8.

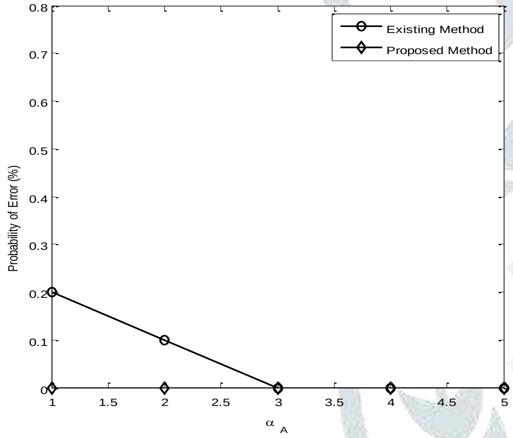

Figure 4 Comparison of probability of error in proposed and existing work

As per the observations of the graph (Fig 4) it can be said that the Probability Error (PE) of proposed work is low and constant in comparison to the existing method whereas in existing method the curve of probability of error varies from 0 to 0.2. Therefore, the proposed work is better than the existing work with lower value of probability of error.

The figure 5 shows the comparison of probability of correction in proposed and existing work. the x axis calibrates the data in α_A which starts from 1 and ends at 5.the y axis depicts the values of probability of correction from 0 to 100 percent. The graph represents that the probability of correction of proposed work is 90 and for existing work it is 85. Thus it is certain that the proposed work is better than the traditional work.

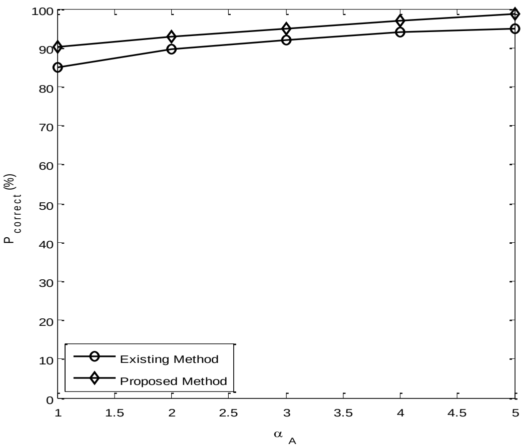

Figure 5 Comparison of probability of correction in proposed and existing
Work

The figure 6 shows the comparison of proposed and traditional work. The comparison is drawn on the basis of the probability of detection. The highest the probability of detection, the most reliable the system is. The evaluated probability of detection in case of proposed work is higher in comparison to the proposed work. in case of proposed it is evaluated to be 99.9% whereas in case of traditional work it lies at 93% initially and then suddenly raised to 98% when the value of α_A reached to the 2.

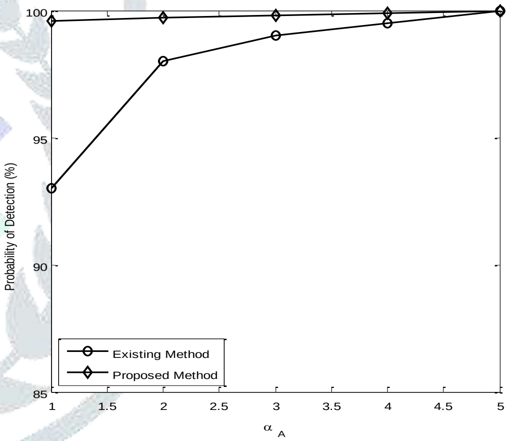

Figure 6 Comparison of probability of detection in proposed and existing work

The probability of error is a performance parameter that is used for measuring the chances of the occurrence of the error in the obtained results. The graph in figure 7 depicts the comparison of proposed and existing work in which the x axis represents the value of α_M from 0.01 to 0.08. The graphs portrays that the probability of error in case of traditional work is higher in comparison to the proposed work. In proposed work this values lies at 1% and also remains stable with the increment in the value of α_M. But for traditional work the probability of error is obtained to be 25% initially and a fall can be seen in the probability of error with the enhancement in the value of α_M.

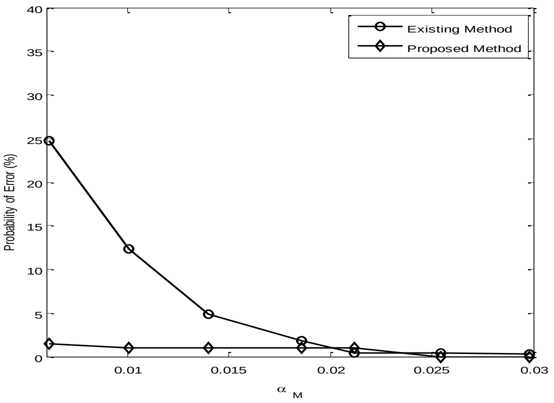

Figure 7 Comparison of probability of Error in proposed and existing work

The fig 8 and 9 represents the comparison of proposed work on the basis of probability y of correction and probability of detection for α_M.The value of α_M Varies from 0.01 to 0.08. The graph in figure 5.5 depicts that the probability of correction in proposed work is higher in comparison to the traditional work. The probability of proposed work is measured to be 91% initially whereas for traditional work it is evaluated to be 69% at the same value of α_M. The probability of detection in proposed work with respect to α_M is analyzed to be 100% and for proposed work it is 95% and then rose to 99% when the value of α_M is 0.010 and then with the value of α_M=0.015 it reached to the 100%. The results prove that the proposed work is better than the traditional work.

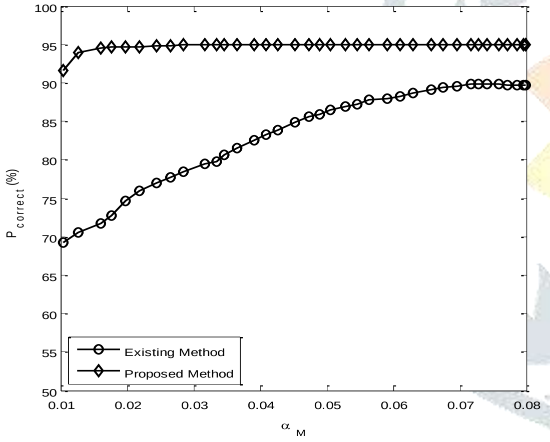

Figure 8 Comparison of probability of correction in proposed and existing work

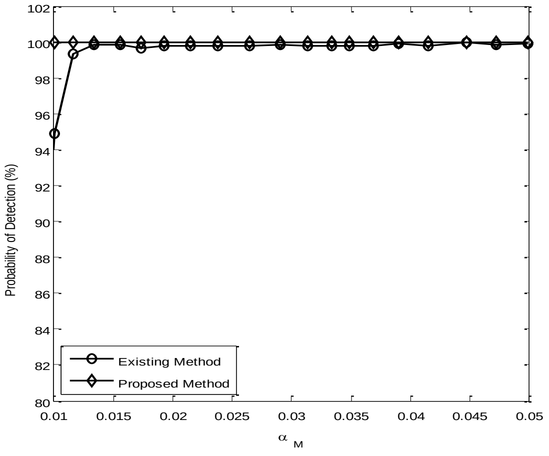

Figure 9 Comparison of probability of detection in proposed and existing work

VIII. CONCLUSION AND FUTURE SCOPE

A novel approach for steganalysis method has proposed in this work where data hiding feature extraction and classification steps are taken place. Initially data is hided in the frames of video whose features are extracted using different feature extraction approaches and finally the classification is performed. The main idea behind proposed technique is to extract the secret message hidden in frames effectively and accurately. The experimental analysis is performed using MATLAB software tool. The results are acquired in terms of probability of detection, correction and error. From the results, it can be concluded that proposed technique outperforms the traditional method as former reduces the error rate, increases the detection and correction probability.

The proposed technique is an effective and efficient approach that can be further improved in terms of data hiding and classification. Artificial neural network technique can be further optimized using swarm intelligence optimization technique to further increase the correction and detection rate.

REFERENCES

[1] A Nissara and A.H. Mir, "Classification of steganalysis techniques: A study", ELSEVIER, Vol. 231, Pp 123-134, 2013

[2] C F Christie and D Lo, "A Combination of Active and Passive Video Steganalysis to Fight Sensitive Data Exfiltration through Online Video", IEEE, Vol. 2, Pp. 371-376, 2016

[3] D C Lou, C L Chou, H Y Wei and H F Huang, "Active steganalysis for histogram-shifting based reversible data hiding", ELSEVIER, Vol. 285, No. 10, Pp. 2510-2518, 2012

[4] F. G Mohammadi and, M. S Abadeh, "Image steganalysis using a bee colony based feature selection algorithm", ELSEVIER, Vol. 31, Pp 35-43, 2014

[5] G. Doerr and J.L. Dugelay, "New intra-video collusion attack using mosaicing," in ¨ IEEE International Conference on Multimedia and Expo, Baltimore, Maryland, July 2003

[6] H Sajedi, "Steganalysis based on steganography pattern discovery", ELESEVIER, Vol. 30, Pp 3-14, 2016

[7] H. Zhao, M. Wu, J. Wang, and K.J.R. Liu, "Nonlinear collusion attacks on independent multimedia fingerprints," in IEEE International Conference on Multimedia and ExpoSignal Processing, Baltimore, Maryland, July 2003.

[8] I. Avcibas, B. Sankur, and N.D. Memon, "Steganalysis based on image quality metrics - differentiating between techniques," in Proc. IEEE Workshop on Multimedia, Cannes, France, October 2001

[9] I. Avcibas, B. Sankur, and K. Sayood, "Image steganalysis with binary similarity measures," in IEEE International Conference on Image Processing, Rochester, New York, Vol. 3, Pp. 645–648, June 2002

[10] J. Fridrich and L. Meng, "Steganalysis of LSB encoding in color images," in Proc. IEEE Conference on Multimedia and Expo, New York, July-August 2000.

[11] J F Miroslav and G D Hogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm", Springer, Pp 310-323, 2002

[12] K. Su, D. Kundur, and D. Hatzinakos, "Statistical invisibility for collusion-resistant digital video watermarking," IEEE Transactions on Multimedia, Vol. 7, No. 1, Pp. 43–51, February 2005.

[13] K Tasdemir, F Kurugollu and S Sezer, “A steganalysis system utilizing temporal pixel correlation of HEVC video”, IEEE, Pp 2446-2449, 2015

[14] S. Trivedi and R. Chandramouli, “Secret key estimation in sequential steganography,” IEEE Transactions on Acoustics, Speech and Signal Processing, Vol. 53, No. 2, Pp. 746–757, February 2005.

[15] Y Deng, Y Wu, H Duan and L Zhou, “Digital Video Steganalysis based on vector statistical characteristics”, ELSEVIER, Vol. 124, Pp. 1705-1710, 2013