Journal of Theoretical and Applied Information Technology
15th November 2020. Vol.98. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A PROPOSED TECHNIQUE FOR DETECTING VIDEO STEGANOGRAPHY

CHO DO XUAN[1,2], TISENKO VICTOR NIKOLAEVICH[3], LAI VAN DUONG[2], NGUYEN TUNG LAM[2]

[1] Faculty of Information Technology, Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

[2]Information Assurance dept. FPT University, Hanoi, Vietnam

[3] Department Quality Systems, Peter the Great St. Petersburg Polytechnic University, Russia, St.Petersburg

Corresponding Author E-mail: [1]chodxptit.edu.vn, [2]chodx@fe.edu.vn

ABSTRACT

In this paper, we propose the method of detecting video steganography based on the blind spot. Accordingly, our method will use the calibration method to pre-process image frames and the SVM supervised learning algorithm to classify images containing information. The difference between our research and the traditional methods are in two factors: i) for the calibration method, we use the correlation technique between space and time factors to calibrate in order to seek the frames that are most similar to the original ones; ii) For the feature extraction method, we use DCT and Markov techniques to extract the features of the frames that are calibrated and the original frames. The experimental results of the method (in section 4) demonstrate that our proposed technique is more effective than traditional approaches.

Keywords: *Steganography, Video Steganography Technique, Video Steganography Detection, Feature Selection*, *SVM.*

1. INTRODUCTION

1.1. Introduction to Video Steganography Technique

Video steganography techniques are being researched and developed increasingly. This can be explained by the diversity of the video that other media don't have. Changes in the video are difficult to detect with the naked eye because frames are displayed on the screen in a very short amount of time. Moreover, video files have a larger capacity than audio or video, so the use of video steganography solves the data capacity problem. Video has many formats, encoders, and decoders, so the applicability of video in steganography is huge. According to statistics from the documents [1], [2], there are many different steganography methods such as Steganography in coefficients domain, Steganography in bit plane, Steganography into context change, Steganography on energy difference coefficients, Steganography in standard H.264, H.265 video. Video steganography techniques can also be classified based on whether this technique applies in the compressed video or the raw video (uncompressed video), or based on steganography domain as space domain or frequency domain. Because video is a file that includes images and audios, the steganography techniques in images and audio can be applied to video.

1.2. The Problem of Detecting Video Steganography

As mentioned above, video steganography techniques are essentially applying and optimizing image steganography techniques for video. Therefore, to detect video steganography, all methods detect steganography in on some or entire

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

frames of video in order to make a final conclusion about whether the video is stego (means that the video contains hidden or secret information) or not. However, directly applying image steganography detection techniques for video encounters two main problems: i) The algorithms or methods of image steganography detection are not really optimal when deployed directly on video; ii) Deciding whether the video is stego or not is based on the decision about steganography in each frame of video. Recent studies indicate that classifying video into stego or normal depends on the design of each steganography method [3]. Method [4] applies a "majority rule" approach to make decisions. Specifically, if more than half of the video's frame is classified as stego, the entire video may be classified as containing secret information. This method requires decoding the entire video and classifying the majority of image frames in the video so the complexity of the method is quite high. A more optimal solution is applied in [5] by checking in turn. In this solution, after checking a frame, making a decision whether the video is stego or not, or needs to be checked for the next frame. Specifically, if the number of frames classified as stego is more than the number of frames calculated from the False Positive Rate, the video will be classified as stego. On the contrary, if the number of frames that are classified as non-stego is more than the number of frames calculated from the False Negative Rate, the video will be classified as non-stego.

1.3. Contribution of Paper

The scientific and practical significance in our paper includes:

- Proposing video steganography detection model based on analysis technique that combine space and time factors. Accordingly, in order to seek the frames that are most similar to the original ones, we propose a calibration method combining both space and time factors. This is a novel approach. Details about this approach are presented in section 3 of the paper.
- Proposing to use machine learning method to detect videos hidden information. Accordingly, in the paper, we propose a new method for selecting and extracting the features of the original frames and calibration frames in the video based on 2 transforming techniques: DCT and Markov. Finally, based on the extracted features, we use Support Vector Machine (SVM) algorithm to classify frames into hidden information or not. Details of the feature extraction process are presented in section 3.2 of the paper. In section 4, we present the experimental results of video steganography classification according to our proposed method.

2. RELATED WORK

There are two main approaches to detect video steganography [3]:

- Target-oriented detection technique: These techniques only work on a specific system or steganography technique and are sometimes limited by the format of images and videos. These techniques are based on the research on a specific steganography algorithm in order to find the statistically significant changes of the containing object after embedding secret information. The detection result for these techniques is usually very accurate. However, these techniques don't have the flexibility and high applicability because it is difficult to expand their operation for other steganography techniques. Accordingly, Budhia [6] proposed the first targeted video steganography detection method. The method focuses on detecting hidden messages inserted in frames of the original video by exploiting redundant information between frames on the time domain. These hidden messages are inserted into the original video based on the Gaussian spread-spectrum steganography algorithm [7], [8]. In this method, the original video or cover video is denoted by $U_k(m,n)$ where $1 \le k \le N$ is the number of frames and m,n is row and column index of pixels. The hidden message is expressed as a binary, after being transformed into a signal, it is embedded in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the original video and denoted by $W_k(m,n)$.

The video signal that is embedded secret message is represented by the following equation:

$$X_k(m,n) = U_k(m,n) + \alpha_k(m,n).W_k(m,n) \text{ with } k = 1,2,3,...N \quad (1)$$

Where $\alpha_k(m,n)$ is a ratio coefficient that is used to control the magnitude of the hidden message in order to balance the sustainability and the invisibility of the steganography algorithm.

- Blind detection technique: The technique is designed to detect in every steganography technique and format of the containing objects. The blind detection technique 'learns' the differences in the statistical features of stego and non-stego images to classify these two image layers. The 'learning' process is performed by applying machine learning and deep learning algorithms on an existing data set. Blind steganography detection techniques are often less accurate than target-oriented detection techniques, but they are more scalable and higher applicability. Pankajaksan and Ho [9] proposed applying the blind detection technique for static image steganography proposed by Xuan [10]. In order to works optimally for video, the image steganography detection method was modified and exploited the time correlation between the frames in the video. Accordingly, in the method of detecting image steganography, Xuan proposed to use the statistical moments of the characteristic wave function (CF) as the feature vector. The image is first separated using a three-level discrete wavelet transform (DWT) and the features are extracted from the image channels created after the transformation. The characteristic function of a random variable is actually a Fourier transform (with the sign of the exponential function reversed) of the probability density function (PDF). In the study [11], Shi and et al showed that noise caused by the content of the original image in the feature vector for classification can be excluded based on spatial prediction techniques. Accordingly, the adjacent frames in the video often have a high degree of correlation between space-time. This correlation was applied to optimize the image steganography detection method that is presented in section 1 for detecting video steganography. Jainsky [12] proposed a blind video steganography detection method using time correlation between frames to improve detection capability. This method uses the interpolation technique in video processing to create new frames in order to increase the ability to detect video steganography. The special in this method is the use of signal processing technology and detection theory to detect steganography instead of using machine learning or deep learning.

In this paper, we propose a method to detect video steganography based on the blind spot. Besides, based on the existing studies and proposals, we propose a new feature extraction method to improve the effectiveness of the steganography detection method.

3. PROPOSE THE MODEL OF DETECTING VIDEO STEGANOGRAPHY

3.1. Model of Detecting Video Steganography Using Machine Learning

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

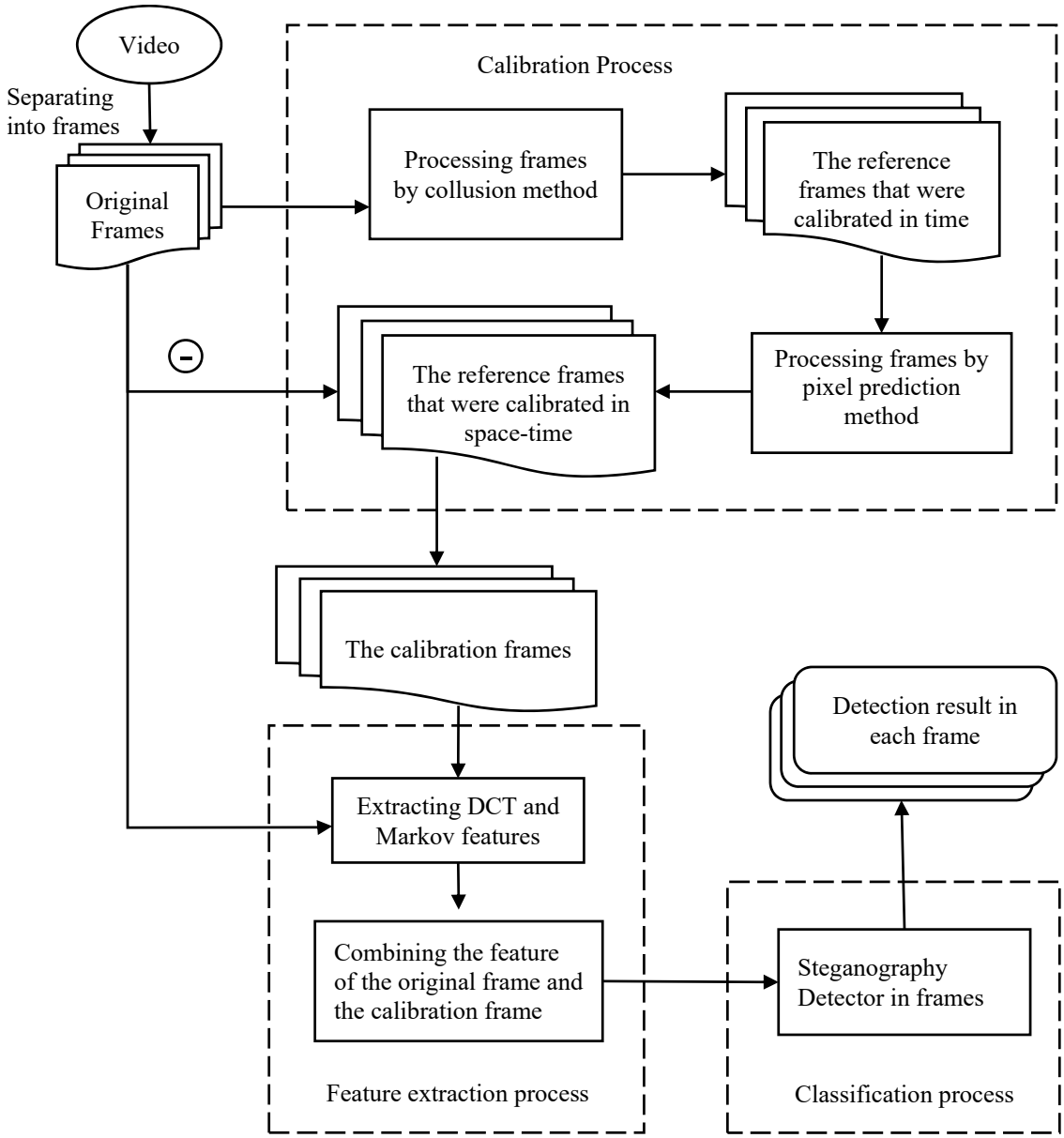

Figure 1: Proposed Model for Detecting Video Steganography Using Machine Learning

From Figure 1, our method for detecting video steganography is described as follows: The video is first separated into frames. These frames are then put into the calibration process. At the calibration step, we will try to recreate the original frame (or frame that has approximately value with the original frame of the video) to calculate the feature vector. In this study, we propose to combine the two calibration methods used in the two studies [9], [13] including collusion and pixel prediction. The collusion method exploits time correlation and the pixel prediction method exploits the space correlation of frames in order to obtain the most optimal reference frame that closes to the original frame value of the video before being embedded. The frames will be processed by the collusion method.

Specifically, the estimated value of the k-th frame is calculated by the collusion method as follows:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$U_k^{'} = \Pi_L(Y_k) = \begin{cases} \frac{1}{2L+1}\sum_{i=1}^{2L+1} Y_i & 1 \le k \le L \\ \frac{1}{2L+1}\sum_{i=k-L}^{k+L} Y_i & L < k \le N-L \\ \frac{1}{2L+1}\sum_{i=N-2L}^{N} Y_i & N-L < k \le N \end{cases} \quad (2)$$

Where $U_k^{'}$ is the k-th estimated frame of the video, Y_i is the frame of the video that needs to be checked in position i, L and N are respectively the number of frames to estimate and the total number of frames of the video.

The estimated frame $U_k^{'}$ is then predicted pixel to obtain the final reference frame according to the following formula:

$$\hat{x} = \begin{cases} \max(a,b) & c \le \min(a,b) \\ \min(a,b) & c \ge \max(a,b) \\ a+b-c & otherwise \end{cases} \quad (3)$$

With $\hat{x}$ is the predicted value of the pixel x and a, b, c are the neighboring pixels.

- The feature extraction process: The feature vector set that is selected to test consists of 274 features proposed by Fridrich [14], [15], [16], [17]. This feature set is used in the blind image steganalysis system and is applied and tested in a number of other studies on video steganography detection [5], [18] and had good results. The feature set is divided into two groups: the DCT feature group and the Markov feature group.
- Classification process: The block of detecting steganography in frames of video is built based on the machine learning method. It means that a data set consisting stego and non-stego frames will be prepared in advance. The frames are embedded secret information by many different steganography methods in order to increase the detection ability of the system for many steganography algorithms and methods. This data set is the input data of the machine learning algorithm to build a steganography detection model. The system is divided into two main stages: the training phase and the testing phase. In the training phase, the first is building a dataset consisting of the stego frames that are embedded secret information by different algorithms and the normal frames that do not contain hidden information. Then extracting features from the frames and using them directly as inputs to machine learning algorithms. These features were selected to provide the most accurate predictive model. In the testing phase, the model that is obtained after the training phase will be used to detect frames containing hidden information. The testing phase is essentially the implementation phase of a steganography detection system in reality, verifying whether a new video contains frames containing hidden information or not. The test results on each frame will be the input of the decision block to make the final classification result of the whole video.

3.2. The Feature Selection and Extraction

Fridrich [19] proposed a feature set to classify and the concept of calibration in the blind image steganalysis method applied to JPEG images. In the paper, the concept of calibration is described as some information of the stego image object that can be restored almost fully based on the information of the stego image object. The calibration process helps increase the influence or sensitivity of features in embedding processes. Calibration is also applied in Markov's feature set described in [17]. Combining calibration with feature dimension reduction in this feature set, Penvny has created a unified feature set including 274 dimensions. This feature set has the ability to classify multiple classes that hidden secret information with six different common steganography algorithms [16]. Besides, Lyu and Farid [20] use the assumption that the probability density function (PDF) of coefficients on wave channels can be changed after the embedding process. In [21], a three-level wave transformation was applied to separate image, then the first four moments of the PDF consisting of the mean, standard deviation, skewness and kurtosis of coefficients in channels in three directions (vertical, horizontal and diagonal lines) of each level are used as a feature set. Sullian [22] modeled the dependency

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

between pixels in a Markov series and described it by the gray-level co-occurrence matrix (GLCM) in reality. The idea of this method is that embedding data can disturb local correlations in the image. The correlation mentioned here mainly refers to the dependence between pixels of the image in space, and the dependence between intra-block and inter-block DCT coefficients in JPEG images. In this paper, we will use two main methods to extract features: DCT and Markov.

3.2.1. DCT feature extraction

The frame is converted to the block DCT coefficients in the same way as the processing in the JPEG image standard. These coefficients are denoted $d_{i,j}(k)$ with $i, j = 1...8$, $k = 1...n_b$, with $d_{i,j}(k)$ is the (i, j)-th quantized DCT coefficients of k-th block (with the total block is n_b). Feature extraction functions are described below:

1) The first function is the histogram H of $64 \times n_b$ DCT coefficients:

$$H = (H_L, ..., H_R) \quad (4)$$

Where $L = \min_{i,j,k} d_{i,j}(k)$, $R = \max_{i,j,k} d_{i,j}(k)$. Only 11 histogram features H_l with $l \in \{-5,...,5\}$ are used.

2. The next five functions are histograms of the coefficients of 5 distinct DCT samples $(i, j) \in \{(1,2),(2,1),(3,1),(2,2),(1,3)\}$ and only the histogram value in the range $\{-5,...,5\}$ is used

$$h^{ij} = (h_L^{ij}, ..., h_R^{ij}) \quad (5)$$

3. The next 11 function is dual histograms that are performances by the matrix 8x8 $g_{i,j}^d$, with $i, j = 1,...,8$, $d = -5,...,5$.

$$g_{i,j}^d = \sum_{k=1}^{n_b} \delta(d, d_{ij}(k)) \quad (6)$$

Where $\delta(x, y) = 1$ if $x=y$ and equal to 0 otherwise. To minimize the number of feature, only $(i, j) \in \{(2,1),(3,1),(4,1),(1,2),(2,2),(3,2),(1,3),(2,3),(1,4)\}$ are selected. The next six functions record the inter-block dependence between the DCT coefficients.

4. The first function is the deviation V

$$V = \frac{\sum_{i,j=1}^{8} \sum_{k=1}^{|I_r|-1} \left| d_{ij}(I_r(k)) - d_{ij}(I_r(k+1)) \right| + \sum_{i,j=1}^{8} \sum_{k=1}^{|I_c|-1} \left| d_{ij}(I_c(k)) - d_{ij}(I_c(k+1)) \right|}{|I_r| + |I_c|} \quad (7)$$

With I_r and I_c symbols for block index vectors $1,..., n_b$ when scanning images in rows and columns.

5. The next two functions record the closure of the image

$$B_\alpha = \frac{\sum_{i=1}^{\lfloor (M-1)/8 \rfloor} \sum_{j=1}^{N} \left| c_{8i,j} - c_{8i+1,j} \right|^\alpha + \sum_{j=1}^{\lfloor (N-1)/8 \rfloor} \sum_{i=1}^{M} \left| c_{i,8j} - c_{i,8j+1} \right|^\alpha}{N \lfloor (M-1)/8 \rfloor + M \lfloor (N-1)/8 \rfloor} \quad (8)$$

Where M, N is the length and width of the image, $c_{i,j}$ is the pixel value in the grayscale of the image, $\alpha = 1, 2$

6. The remaining functions are calculated from the co-appearing matrices of the surrounding DCT coefficients.

$$C_{st} = \frac{\sum_{i,j=1}^{8} \sum_{k=1}^{|I_r|-1} \delta(s, d_{ij}(I_r(k))) \delta(t, d_{ij}(I_r(k+1))) + \sum_{i,j=1}^{8} \sum_{k=1}^{|I_c|-1} \delta(s, d_{ij}(I_c(k))) \delta(t, d_{ij}(I_c(k+1)))}{|I_r| + |I_c|} \quad (9)$$

Where $(s,t) \in [-2,+2] \times [-2,+2]$

3.2.2. Markov feature group

Firstly, the matrix $F(u,v)$ of the image is built from the block DCT coefficients of the image. From this matrix, we obtain other matrices in the horizontal, vertical, main diagonal, and sub diagonal directions as follows:

$$F_h(u,v) = F(u,v) - F(u+1,v) \quad (10)$$

$$F_v(u,v) = F(u,v) - F(u,v+1) \quad (11)$$

$$F_d(u,v) = F(u,v) - F(u+1,v+1) \quad (12)$$

$$F_m(u,v) = F(u+1,v) - F(u,v+1) \quad (13)$$

To reduce the number of feature dimensions, only the values $[-4,+4]$ in the matrix are used. From here, we calculate the conversion matrix as follows:

$$M_h(i,j) = \frac{\sum_{u=1}^{S_u-2} \sum_{v=1}^{S_v} \delta(F_h(u,v) = i, F_h(u+1,v) = j)}{\sum_{u=1}^{S_u-1} \sum_{v=1}^{S_v} \delta(F_h(u,v) = i)} \quad (14)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$M_v(i,j)=\frac{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-2}\delta(F_v(u,v)=i,F_v(u,v+1)=j)}{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-1}\delta(F_v(u,v)=i)} \quad (15)$$

$$M_d(i,j)=\frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v-2}\delta(F_d(u,v)=i,F_d(u+1,v+1)=j)}{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v-1}\delta(F_d(u,v)=i)} \quad (16)$$

$$M_m(i,j)=\frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v-2}\delta(F_m(u+1,v)=i,F_h(u,v+1)=j)}{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v-1}\delta(F_m(u,v)=i)} \quad (17)$$

Where: S_u and S_v are dimensions of image, δ =1 if and only if input condition is satisfied. The final feature is the average of the four conversion matrices.

3.3. Classification Method

To evaluate the effectiveness of the video detection process, in this paper, we will use the SVM algorithm. SVM is a supervised machine learning method, introduced by Vapnik (1995) [23]. For simplicity, consider the binary classification first, then extend to multi-class classification problem. The basic idea of SVM is to construct a border which separate the data samples into two parts, corresponding to two classes, so that the distance from the training samples to the border are farthest possible [24, 25].

A linear function which discriminates two classes will be in following form:

$$y(x) = w^T\Phi(x) + b \quad (1)$$

In which:

- $w \in R^m$ is a weight vector or standard vector of hyperplane.
- $b \in R$ is deviation.
- $\phi(x) \in R^m$ is the feature vector, ϕ is the mapping function from input space to feature space.

Let's say the input data set includes N samples $\{x_1, x_2,...,x_N\}$, with the labels vector is $\{t_1,\ldots,t_N\}$, in which $t_n \in \{-1,1\}$.

SVM approach to solves this problem is based on a margin concept. Margin is the minimum distance from the hyperplane to every data point or the distance from the hyperplane to the nearest point, and the best hyperplane is the one that has max margin.

The formula for distance from data point to the hyperplane is as the follow:

$$\frac{|y(x)|}{\|w\|}$$

Suppose the hyperplane divides the training data set into two separate classes, then $t_n y(x_n) > 0$. Therefore, the distance from xn to the hyperplane can be rewritten as the follow:

$$\frac{t_n y(x_n)}{\|w\|} = \frac{t_n(w^T\phi(x_n)+b)}{\|w\|} \quad (18)$$

Margin is the distance to the nearest point xn in the data set, and we want to find the optimal values of w and b by maximizing this distance. This problem can be rewritten as the below formula:

$$\arg\max_{w,b}\left\{\frac{1}{\|w\|}\min_n[t_n(w^T\phi(x_n)+b)]\right\} \quad (19)$$

The problem of maximum optimization $\|w\|^{-1}$ can be converted to the problem of minimum optimization of $\|w\|^2$ and with adding the Largange factors, the above formula becomes:

$$\min_{w,b}\max_a\{\frac{1}{2}\|w\|^2 - \sum_{n=1}^N a_n\{t_n(w^T\phi(x_n)+b) - 1\}\} \quad (20)$$

In which $a = (a_1,\ldots,a_N)^T$ are Lagrange factors.

After a number of transformations, such as calculate the derivatives by w and b, then calculate w and b and do the substitution, will lead to the following optimization problem:

$$\sum_{n=1}^N a_n - \frac{1}{2}\sum_{n=1}^N\sum_{m=1}^N a_n a_m t_n t_m k(x_n,x_m) \quad (21)$$

In above formula, the kernel function is defined by $k(x_n,x_m) = \phi(x_n)^T\phi(x_m)$. Note that all the points which are not on the margin will not affect to the value of objective function, because we can choose an = 0. The remain data points ($a_n \neq 0$), called the support vectors, are interested in the process of SVM training. The classification of a new data point only depends on the support vectors.

We can determine the parameter b based on the support vectors. Although by using only one vector xn we can find out the value of b, but to ensure

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the stability, b will be calculated by average values based on all the support vectors.

$$b = \frac{1}{N_S}\sum_{n\in S}(t_n - \sum_{m\in S} a_m t_m k(x_n, x_m)) \quad (6)$$

In which, N_S is the total number of support vectors.

In the case of multi-class classification, we can build the classification process based on a number of binary-class classifications or build k linear functions $y_k(x)$ similar to the above function.

SVM has a main advantage that it can process a huge number of features but no need to reduce them to avoid the over-fitting problem. This characteristic is very useful when solving the problems which have big number of dimensions.

4. EXPERIMENTS AND EVALUATIONS

The sample data set is made from 10 AVI videos that have different resolutions and lengths. The 10 selected videos include videos with slow-moving objects (such as slow-motion videos), videos with fast-moving objects (such as sports videos), and videos with fixed frames from the dashcam. To embed secret information in videos, the study used 4 image steganography tools: Openstego, Stegano, Cloackedpixel, and LSBSteg. The frames of video are embedded in turn with a secret message as a 1024-bit hash code of a random string. The data set collected after the steganography process includes 20 videos consisting of 10 stego videos and 10 normal videos with a total number of nearly 30,000 frames. Training in the classification model uses the SVM classifier with testing different parameter values [25]. The result that has the most optimal value achieved when the kernel parameter is linear and C is in the range [10, 100].

Table 1: Training Results for Detection Model with SVM Algorithm

No.	Kernel	C	Gamma	Data set	Accuracy
1	Linear	1	None	274 [17]	68%
2	Linear	10	None	274 [17]	70%
3	Linear	100	None	274 [17]	69%
4	Rbf	10	0.001	274 [17]	40%
5	Rbf	10	0.0001	274 [17]	44%
6	Rbf	10	0.00001	274 [17]	46%
7	Linear	1	None	548 [17]	80%
8	**Linear**	**10**	**None**	548 [our]	**84%**
9	Linear	100	None	548 [our]	83%
10	Rbf	10	0.001	548 [our]	46%
11	Rbf	10	0.0001	548 [our]	48%
12	Rbf	10	0.00001	548 [our]	51%

The initial experiment was run with a video data set that is created with a set of 274 features of the calibration image frame. In the second experiment, a feature set consisting of 548 features was run to demonstrate the proposed hypothesis with the improved calibration technique. The results proved the hypothesis. In the first experiment, the accuracy is only 70%. However, in the second experiment, the accuracy is approximately 84%. This is a significant improvement. From the experiment results, we can see that the feature set 274 works effectively in the blind steganography detection system with a relatively high accuracy rate. Besides, the space-time correlation between frames can be used to increase the accuracy of the steganography detection system. Finally, we see that the hypothesis proposed by [12] about improving calibration techniques is correct.

5. CONCLUSIONS

Detecting video steganography has been and will be a difficult task for steganography detection systems. In this paper, we solved 2 main tasks. For the video steganography detection model based on the analysis technique that combine both space and time factors, we succeeded in calculating

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the correlation between these factors to be able to extract the frames most similar to the original frame. This problem is very important and necessary in order to improve the efficiency on time and accuracy of the process of seeking and extracting original frames based on the transformed frames. In addition, for the feature selection and extraction, we successfully extracted the basic characteristics of the frame based on DCT and Markov methods. The experimental results in Table 1 have shown that our proposed method is more effective than other studies. This result proves that the features we selected and proposed are effective in classifying videos into stego or not. Thus can see that the research results in our paper have opened up a novel approach to detect video steganography where original frames are recreated not only based on time but also based on space, as well as features of the frame are fully built and extracted. In the next studies, in order to improve the effectiveness of video steganography detection, we will optimize 2 main problems: For the stego frame detection algorithm, we will research and build deep learning models for classifying stego frames based on feature sets presented in the paper; For the video steganography conclusion method, we will use several statistical algorithms and Fuzzy to identify and conclude about hidden video based on each frame.

REFRENCES:

[1] Konakhovich Georgiy Filimonovich; Puzyrenko Alexander Yurievich. Computer Steganography. Theory and practice. "MK-Press", 2006; 288p

[2] Gerrit Cornelis LANGELAAR (2000). Real-time Watermarking Techniques for Compressed Video Data. Veenendaal ISBN 90-9013190-6

[3] B. Li, J. He, J. Huang, and Y.Q. Shi. "A survey on image steganography and steganalysis." *Journal of Information Hiding and Multimedia Signal Processing*. Vol 2, 2011, pp. 142-172.

[4] C. Xu and X. Ping, "A Steganographic Algorithm in Uncompressed Video Sequence Based on Difference between Adjacent Frames. *Proceedings of Fourth International Conference on Image and Graphics* (ICIG 2007) , Sichuan, 2007, pp. 297-302,

[5] Kevin Bryan, "Video Steganalysis for Digital Forensics Investigation". Dissertations. Paper 48. 2013. https://doi.org/10.23860/diss-bryan-kevin-2013

[6] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compability," *Proceedings of SPIE - The International Society for Optical Engineering*. November 2001, https://doi.org/10.1117/12.448213

[7] A. Westfeld and A. Phitzmann, "Attacks on steganographic systems," *Proceedings of* 3rd Information Hiding Workshop, Dresden, Germany, September-October 1999. pp 61-76.

[8] N. Provos, "Defending against statistical steganalysis," *Proceedings of the 10th USENIX Security Symposium*. Dresden, Germany, August 2001. pp. 474-481

[9] Vinod Pankajakshan and A. T. S. Ho, "Improving Video Steganalysis Using Temporal Correlation". *Proceedings of Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007). 26-28 Nov. 2007, Kaohsiung, Taiwan, pp. 287-290.*

[10] P. Sallee, "Model-based methods for steganography and steganalysis," *International Journal of Image and Graphics*, vol. 5, no. 1, pp. 167–189, 2005.

[11] Y. Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, and C. Chen. " Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network". *Proceedings of the IEEE International Conference on Multimedia and Expo*, July 2005, Amsterdam, Netherlands, pp. 16- 21.

[12] Jan Kodovský, "Calibration Revisited". *Proceedings of the 11th ACM workshop on Multimedia and security, September 2009*. pp. 63–74. https://doi.org/10.1145/1597817.1597830

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] Udit budhia, "Steganalysis of video sequences using collusion sensitivity". Texas A & M University, 2006.

[14] M. Goljan, J. Fridrich, and R. Du, "Distortion-Free Data Embedding for Images," 4th International Workshop, Pittsburgh, PA, USA, April 25–27, 2001, pp. 27–41.

[15] E.L. Lehmann and J.P. Romano, "Testing Statistical Hypotheses", 3rd. Edition, Springer Texts in Statistics, 2005.

[16] J. Fridrich. "Feature-based steganalysis for jpeg images and its implications for future design of steganography schemes". LNCS, Vol 3200. pp. 67- 81. 2004.

[17] Tom Pevnya, Jessica Fridrich, "Merging Markov and DCT Features for Multi-Class JPEG Steganalysis". *Proceedings of SPIE - The International Society for Optical Engineering*. 2007, pp.6505- 6511. https://doi.org/10.1117/12.696774

[18] K.Kancherla, "Video Steganalynis Using Spatial and Temporal Redundancies". *Proceedings of International conference on high performance computing & simulation*. 21-24 June 2009, Leipzig, Germany, pp. 200 - 207.

[19] Y. Q. Shi, C. Chen, and W. Chen." A Markov process based approach to effective attacking jpeg steganography. *LNCS*, Vol 4437, 2006, pp. 249- 264.

[20] Lyu Siwei and H. Farid. Detecting hidden message using higher-order statistics and support vector machines. *LNCS*, Vol 2578, 2002. pp. 131-142.

[21] J. Harmsen and W. Pearlman. "Steganalysis of additive noise modelable information hiding". *SPIE*, Vol 5020, 2003, pp. 131- 142.

[22] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath. "Steganalysis for markov cover data with applications to images". *IEEE Transactions on Information Forensics and Security*, Vol 1, No 2, 2006, pp.275- 287.

[23] JohnShawe-Taylor, ShiliangSun. Kernel "Methods and Support Vector Machines". *Academic Press Library in Signal Processing* Vol 1, 2014, pp. 857-881.

[24] C. Corinna, V. Vladimir. "Support-vector networks". *Machine Learning*. Vol 20, 1995, pp. 273-297.

[25] S.S. Shai, B.D. Shai. Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press 2014.