International Journal of Research in Engineering, Science and Management
Volume-1, Issue-11, November-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Robust and Secure Video Steganography Method in Curvelet Transform Based on Multiple Object Tracking and Error Correcting Code

S. Nandhini Devi[1], T. Saranya[2], P. Rekha[3], D. Rajinigirinath[4]
[1]*PG Student, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India.*
[2,3]*Assistant Professor, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India.*
[4]*Head of the Department, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India.*

***Abstract*: In recent times, video steganography has become a popular option for secure and secret data communication. The unperceivable, confidentiality, and robustness against attacks are three main requirements that any video steganography method should take into consideration. In this article, a robust and secure video steganographic method in curvelet tranform based on the Multiple Object Tracking (MOT) algorithm and Error Correcting Codes (ECC) is proposed. The secret message is preprocessed by applying both Hamming and BCH codes for encoding the secret data. First, motion-based MOT algorithm is implemented on source videos to distinguish the regions of interest in the moving objects. Then, the data hiding process is performed by concealing the secret message into the curve let transform. Experiment results demonstrate that the suggested algorithm not only improves the embedding capacity and unperceivable but also it enhances its security and robustness by encoding the secret message and withstanding against various attacks such as noise and interference.**

***Keywords*: Video steganography, multiple object tracking, Discrete Wavelet Transform, Error Correction Code, Discrete Curvelet Transform.**

1. Introduction

In the recent times, there are different ways evolved to transmit data using internet. The transmission of data is easy, quick and accurate, but main problem is that the hypnotic data has been hacked or stolen in different ways. Steganography is defined as the art of concealing secret information in specific carrier data, establishing covert communication channels between official parties a stego object (steganogram) should appear the same as an original data that has a slight change of the statistical features. The primary objective of the steganography is to eliminate any suspicion to the transmission of hidden messages and provide security and anonymity for legitimate parties. The simplest way to observe the steganogram's visual quality is to determine its accuracy, which is achieved through the Human Visual System (HVS). The HVS cannot identify slight distortions in the steganogram, thus avoiding suspiciousness. However, if the size of the hidden message in proportion with the size of the carrier object is large, then the steganogram's degradation will be visible to the human eye resulting in a failed steganographic method. Video Steganography is a technique used to hide multimedia files into a video file. Video steganography algorithms gain more attention to researchers due to size and memory requirements of video data, many of these stage to enhance the security and robustness of the steganographic method. This steganographic method has the capacity to withstand against both noises and signal processing operations.

Embedding efficiency, hiding capacity, and robustness are the three major requirements incorporated in any successful steganographic method. First, embedding efficiency can be determined by answering the following questions: 1) how secure is the steganographic method to obscure the hidden information inside the carrier object? 2) How accurate are the steganograms' qualities after the hiding procedure occurs? and 3) is the secret message undetectable from the steganogram? In other words, the steganography method is highly efficient if it includes encryption, imperceptibility, and undetectability characteristics. The high efficient algorithm conceals the covert information into the carrier data by utilizing some of the encoding and encryption techniques prior to embedding stage for improving the security of the underlying algorithm. Fig. 1 represents the general model of steganographic method.

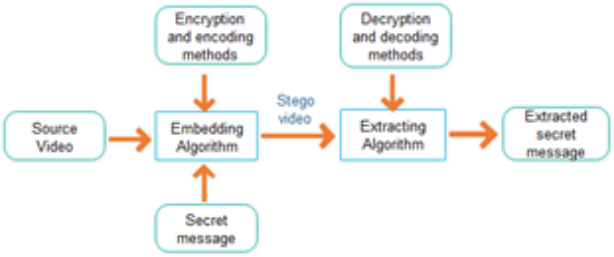

Fig. 1. General diagram of steganography method

The confidentiality is the second fundamental requirement which permits any steganography method to increase the size of hidden message taking into account the visual quality of the steganograms. The confidentiality is the quantity of the covert messages inserted inside the carrier object. In ordinary steganographic methods, both confidentiality and embedding efficiency are contradictory.Conversely, if the confidentiality is increased, then the quality of the steganograms will be diminished, decreasing the efficiency of underlying method. The embedding efficiency is affected by embedding capacity. To increase the confidentiality with the minimum alteration rate of the carrier object, many steganographic methods have been presented using different strategies. These methods utilize linear block codes and matrix encoding fundamentals which include BCH codes, Hamming codes, cyclic codes, Reed-Solomon codes, and Reed-Muller codes.

Robustness is the third requirement which measures the steganographic method's strength against attacks and signal processing operations. These operations contain geometrical transformation, compression, cropping, and filtering. A steganographic method is robust whenever the recipient obtains the secret message accurately, without bit errors. An efficient steganography method withstands against both adaptive noises and signal processing operations.

2. Literature survey

Ma et al [1] presented a video data concealing for H.264 coding without having an error accumulation in the intra video frames. In the intra frame coding, the current block detects its data from the encoded adjacent blocks, specifically from the boundary pixels of upper and left blocks. Thus, any embedding process that occurs in these blocks will propagate the distortion, negatively, to the current block. In addition, the distortion drift will be increased toward the lower right intra frame blocks. To prevent this distortion drift, authors have developed three conditions to determine the directions of intra frame prediction modes. To select 4x4 QDCT coefficients of the luminance component for data embedding, the three raised conditions must be satisfied together. However, this method has a low embedding capacity because only the luminance of the intra frame blocks that meet the three conditions are selected for hiding data.

Cheddad et al proposed a skin tone video steganography algorithm based on the YCbCr color space. YCbCr color space is a useful color transformation, which is used in many techniques such as compression and object detection methods. The correlation between three color channels (RGB) is removed, so that the intensity (Y) will be separated from colors chrominance blue and red (Cb and Cr). After the human skin regions are detected, the only Cr of these regions will be utilized for embedding the secret message [2]. Overall, the algorithm has a low embedding payload because it has embedded the secret message into the only Cr component of the skin region. Khupse et al. proposed an adaptive video steganography scheme using steganoflage. The steganography scheme has been used in region of interest video frames. Khupse et al. used human skin color as a cover data for embedding the secret message. The morphological dilation and filling operation methods have been used as a skin detector. After video frames have converted to YCbCr color space, the frame that has the minimum mean square error will be selected for data embedding process. Only the Cb component of this particular frame will be picked for embedding the secret message [3]. This scheme is very limited in capacity because only one frame is selected for the data embedding process. Zhang et al. proposed an efficient embedder using BCH codes for steganography. The embedder conceals the secret message into a block of cover data. The embedding process is completed by changing various coefficients in the input block in order to make the syndrome values null. The efficient embedder improves both storage capacity and computational time compared with other algorithms. According to the system complexity, Zhang's algorithm improves the system complexity from exponential to linear [4].

There is flexibility for both embedding efficiency and embedding payload in the previously mentioned algorithms. This flexibility can be used by our proposed algorithm to improve the algorithm's performance even further.

3. Proposed modelling

In the proposed system, we introduce a robust and secure video steganography method in curvelet transform based on MOT and ECC. The major stages of the proposed video steganography framework are illustrated in Fig. 2.The curvelet transform is a multiscale directional transform that allows an almost optimal nonadaptive sparse representation of objects with edges. A curvelet transform differs from other directional wavelet transforms in that the degree of localisation in orientation varies with scale. It actually overcomes the missing directional selectivity of wavelet transforms in images.

A Discrete Curvelet Transform (DCT) is a Fourier-related transform similar to the Discrete Fourier transform (DFT), but using only real numbers. The DCTs are generally related to Fourier series coefficients of a periodically and symmetrically extended sequence whereas DFTs are related to Fourier series coefficients of a periodically extended sequence. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), whereas in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

The proposed steganographic algorithm is structured into three stages:

1) Motion-based MOT stage

The process of establishing the moving objects in the video frames must be finalized when motion object regions are

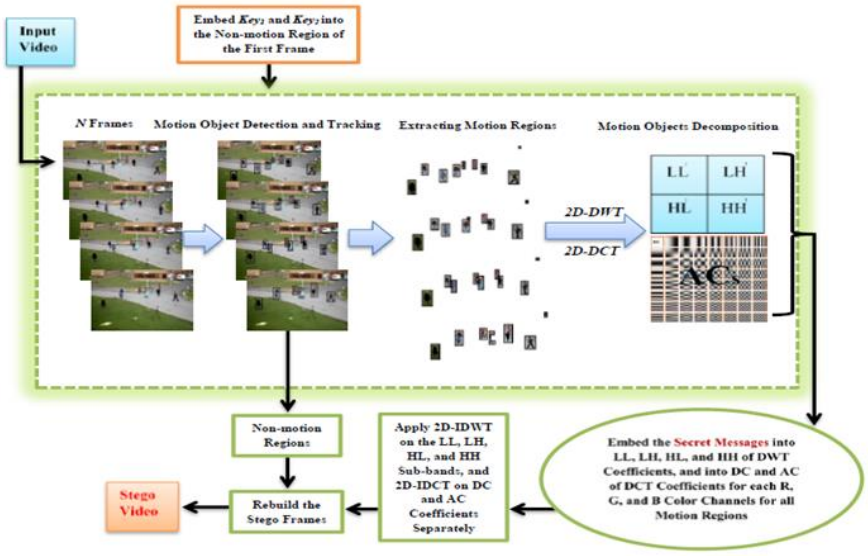

Fig. 2. The proposed video steganography framework

utilized as source data. This process is achieved by recognizing each moving object within an individual frame, and then associating these identifications throughout all of the video frames. The background subtraction method is applied to detect the moving objects based on the Gaussian mixture model. It also computes the variations between successive frames that generate the foreground mask. Then, the Kalman filter is selected to predict estimation trajectory of each moving region.

2) Data embedding stage

In entire video frames, the source data of our proposed method is the motion objects that are considered as regions of interest. By using the motion-based MOT algorithm, the process of detecting and tracking the motion regions over all video frames are achieved. The region of interest altered in each video frame is dependent on the number and the size of the moving objects. In every frame, 2D-DWT is implemented on RGB channels of each motion region resulting LL, LH, HL, and HH subbands.

In addition, 2D-DCT is also applied on the same motion regions generating DC and AC coefficients. Thereafter, the secret messages are concealed into LL, LH, HL, and HH of DWT coefficients, and into DC and AC of DCT coefficients of each motion object separately based on its foreground mask. Furthermore, both secret keys are transmitted to the receiver side by embedding them into the non-motion area of the first frame. Upon accomplishment, the stego video frames are rebuild in order to construct the stego video that can be transmitted through the unsecure medium to the receiver.

3) Data extraction stage

In order to recover hidden messages accurately, the embedded video is separated into a number of frames through the receiver side, and then two secret keys are obtained from the non-motion region of the first video frame. To predict trajectories of motion objects, the motion-based MOT algorithm is applied again by the receiver. Then, 2D-DWT and 2D-DCT are employed on the RGB channels of each motion object in order to create LL, LH, HL, and HH sub bands, and DC and AC coefficients, respectively. Next, the extracting process of the embedded data is achieved by obtaining the secret messages from LL, LH, HL, HH, DC, and AC coefficients of each motion region over all video frames based on the same foreground masks used in the embedding stage. The extracted secret message is decoded by Hamming and BCH and then decrypted to obtain the original message.

4. Results and discussion

Three S2L1 video sequences of different views (View1, View3, and View4) were used from the well-known PETS2009 dataset [13]. The implemented videos contain moving objects which are taken by different stationary cameras. Experimental results are obtained by using the R2013a version of the MATLAB software program. The videos contain a 768x576 pixel resolution at 30 frames per second, and a data rate of 12684 kbps. Each cover video sequence contains 795 frames. In all the video frames, the secret message appears as a large text file split in accordance with the size and number of the moving objects.

A. Visual Quality

The imperceptibility of our proposed scheme is measured by utilizing a PSNR measurement, which is a well-known metric and can be calculated as follows:

$$PSNR = 10 * Log_{10}\left(\frac{MAX_A{}^2}{MSE}\right) \quad (dB)$$

$$MSE = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}\sum_{k=1}^{c}[A(i,j,k) - B(i,j,k)]^2}{a \times b \times c}$$

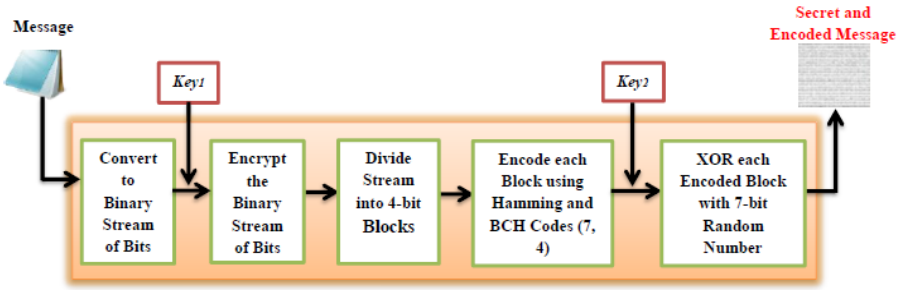

Fig. 3. Process of encrypting and encoding input messages

Where *A* and *B* indicate the original and embedded frames, respectively, *a* and *b* refer to video dimensions, and *c* refers to the RGB color components (k=1, 2, and 3). *MAXA* is the highest pixel value of the frame *A*.

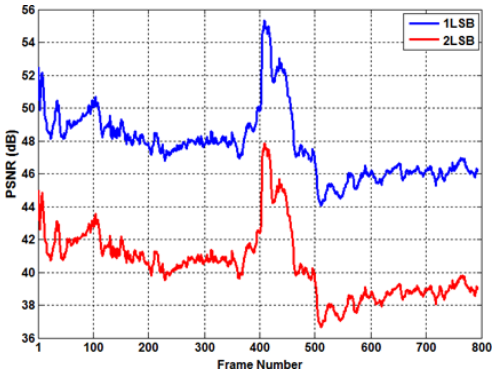

Fig. 4. The PSNR comparison of the View-1

The Fig. 4, shows the PSNR comparison of the first video (View1) when using 1 LSB and 2 LSBs of each motion object's RGB pixels. Here, the PSNR values equal 47.73 dB for 1 LSB and 40.45 dB for 2 LSBs.

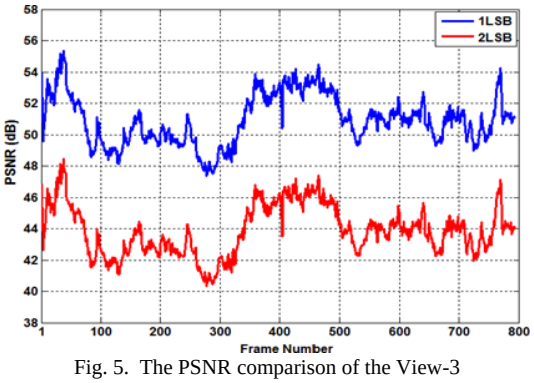

Fig. 5. The PSNR comparison of the View-3

The Fig. 5, illustrates the PSNR comparison of the View3 experiment when using 1 LSB and 2 LSBs of each motion pixel in the video frames. The PSNR values equal 50.93 and 43.88 dBs for 1 LSB and 2 LSBs, respectively.

The Fig. 6, shows the PSNR comparison of the View4 video when using 1 LSB and 2 LSBs of each motion object's RGB pixels. Here, the PSNR values equal 51.35 dB for 1 LSB and 44.16 dB for 2 LSBs.

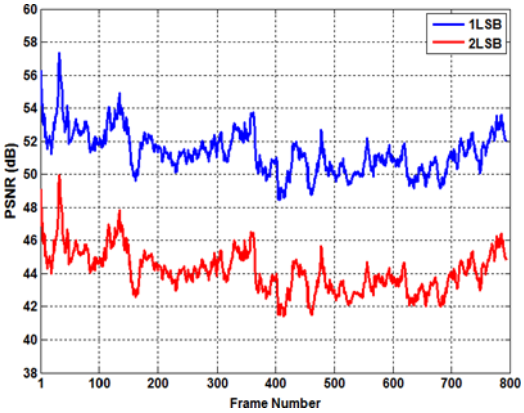

Fig. 6. The PSNR comparison of the View-4

The third View4 has better visual quality among other experiments because it has fewer regions of moving objects than others. This means that View4 video can embed less size of the secret data than the other two experiments. Overall, the stego videos' visual qualities are close to the original videos' visual qualities due to the high values of PNSRs for our proposed algorithm.

B. Embedding Capacity

Our proposed algorithm has a high embedding payload. Here, the average of obtained hiding ratios for three experiments is 3.37%. The size of the hidden secret message in each View1, View3, and View4 videos using 1 LSB is 31.38, 14.62, and 12.95 Megabits, respectively. Moreover, when using 2 LSBs, the amount of the secret message in each View1, View3, and View4 experiments will be 62.77, 29.25, and 25.92 Megabits, respectively. The hiding ratio (HR) is calculated as follows:

$$HR = \frac{Size\ of\ embedded\ message}{Video\ size} \times 100\%$$

The Fig. 7, 8, and 9 illustrate the data embedding payload of the proposed steganography algorithm for each View1, View3, and View4 experiments. These three figures have shown the comparison of the embedding capacity of each video when 1 LSB and 2 LSBs of the moving objects' pixels are utilized. The 2 LSBs were implemented in order to double the amount of the secret message in each experiment.

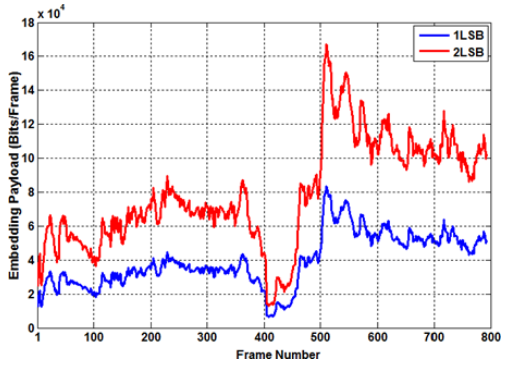

Fig. 7. The embedding payload comparison of the View-1

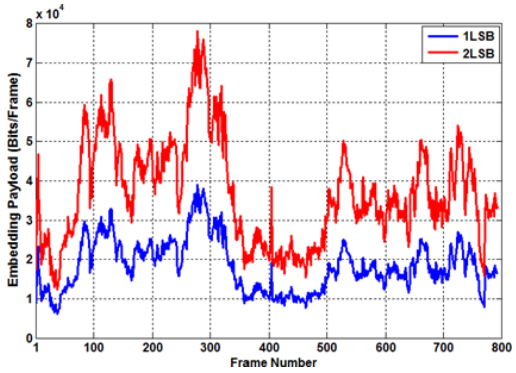

Fig. 8. The embedding payload comparison of the View-3

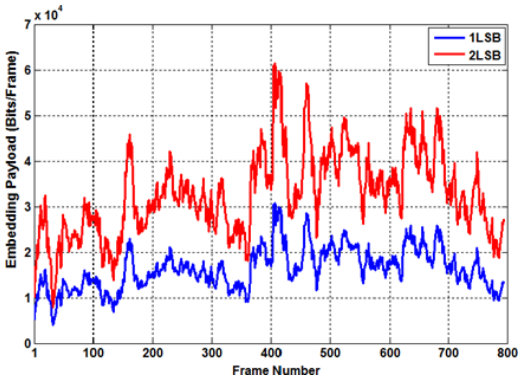

Fig. 9. The embedding payload comparison of the View-4

C. *Robustness*

Similarity (Sim) and Bit Error Rate (BER) metrics have been utilized [7]. The Sim ($0 \le Sim \le 1$) and BER can be calculated in the following equations:

$$Sim = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j)\times \hat{M}(i,j)]}{\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}M(i,j)^2}\times\sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}\hat{M}(i,j)^2}}$$

$$BER = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}[M(i,j)\oplus \hat{M}(i,j)]}{a\times b}\times 100\%$$

Where M and $\hat{M}$ are the original and obtained messages, respectively, and a x b is the size of the hidden messages. The algorithm used different attacks such as *Gaussian* noise, *Salt & pepper* noise, and *median filtering*. The highest robustness of our method can be achieved when the maximum *Sim* and minimum *BER* values are gained.

5. Conclusion

A robust and secure video steganography method in curvlet tranform domains based on MOT and ECC is proposed in this paper. The proposed algorithm is three-stage: 1) the motion-based MOT algorithm, 2) data embedding, and 3) data extraction. The proposed algorithm has utilized MOT and ECC as the preprocessing stages which in turn provides a better confidentiality to the secret message prior to embedding phase. Moreover, through experiments from different perspectives, the security and robustness of the method against various attacks have been confirmed. For future work, we would like to improve the embedding payload of the proposed algorithm with the respect of the video quality by using other techniques that operate in frequency domain. Also, we would like to conduct efficient linear block codes to enhance the security of the algorithm.

References

[1] X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift," IEEE Transactions on Circuits and Systems for Video Technology, vol. 20, pp. 1320-1330, 2010.

[2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," *Signal Processing*, vol. 89, pp. 2324-2332, 2009.

[3] S. Khupse and N. N. Patil, "An adaptive steganography technique for videos using Steganoflage," in Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, 2014, pp. 811-815.

[4] Z. Rongyue, V. Sachnev, M. B. Botnan, K. Hyoung Joong, and H. Jun, "An Efficient Embedder for BCH Coding for Steganography," Information Theory, IEEE Transactions on, vol. 58, pp. 7272-7279, 2012.

[5] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in *2015 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2015, pp. 1-7.

[6] S. Islam, M. R. Modi, and P. Gupta, "Edge-based image steganography," *EURASIP Journal on Information Security*, vol. 2014, pp. 1-14, 2014.

[7] K. Qazanfari and R. Safabakhsh, "A new steganography method which preserves histogram: Generalization of LSB++," *Information Sciences*, vol. 277, pp. 90-101, 2014.

[8] R. J. Mstafa and K. M. Elleithy, "Compressed and raw video steganography techniques: a comprehensive survey and analysis," *Multimedia Tools and Applications*, pp. 1-38, 2016.

[9] T. Yiqi and W. KokSheik, "An Overview of Information Hiding in H.264/AVC Compressed Video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, pp. 305-319, 2014.

[10] Y. Liu, Z. Li, X. Ma, and J. Liu, "A robust data hiding algorithm for H.264/AVC video streams," *Journal of Systems and Software*, vol. 86, pp. 2174-2183, 2013.

[11] M. A. Alavianmehr, M. Rezaei, M. S. Helfroush, and A. Tashk, "A lossless data hiding scheme on video raw data robust against H.264/AVC compression," in *2012 2nd International eConference on Computer and Knowledge Engineering (ICCKE)*, 2012, pp. 194-198.

[12] R. J. Mstafa and K. M. Elleithy, "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes," in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, 2015, pp. 335-340.

[13] Z. Rongyue, V. Sachnev, M. B. Botnan, K. Hyoung Joong, and H. Jun, "An Efficient Embedder for BCH Coding for Steganography," *Information Theory, IEEE Transactions on*, vol. 58, pp. 7272-7279, 2012.

[14] L. Tse-Hua and A. H. Tewfik, "A novel high-capacity data-embedding system," *Image Processing, IEEE Transactions on*, vol. 15, pp. 2431-2440, 2006
[15] J. Ferryman, in Pets 2009 dataset: Performance and evaluation of tracking and surveillance, 2009.
[16] S. Khupse and N. N. Patil, "An adaptive steganography technique for videos using Steganoflage," in *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*, 2014, pp. 811-815.
[17] A. Yilmaz, O. Javed, and M. Shah, "Object tracking: A survey," *Acm computing surveys (CSUR)*, vol. 38, p. 13, 2006.