Motion-based Less Significant Frame for Improving LSB-based Video Steganography

Achmad Solichin
Informatics Department
Faculty of Information Technology, Budi Luhur University
Jakarta, Indonesia
achmad.solichin@budiluhur.ac.id

Painem
Information System Department
Faculty of Information Technology, Budi Luhur University
Jakarta, Indonesia
painem@budiluhur.ac.id

***Abstract*—Steganography is a technique to hide secret messages in certain media, such as images, audio, and video, so that are not visible to the human eye. In this study, we use the LSB (least significant bit) method to hide various documents into the video. The use of video as cover media has advantages, especially the amount of storage capacity and better security level. A video file consists of some frames or images. Commonly, other researchers are inserting a message in some frames starting from the first frame, or in a particular order. In this study, we proposed a method for selecting the location of the insertion of a message on some insignificant frames. We called it Less Significant Frame (LSF) method. Frame selection is based on the movement of each frame using optical flow features. Tests have been conducted to prove the quality of the stego-video using the fidelity aspect that was measured using PSNR value. The test results showed that in experiments with methods LSB and LSF, the quality of video that has been inserted proved to be better than the experiment without LSF. The average value of PSNR on trial with the LSB and LSF method amounted to 44.417638 dB, whereas in trials without LSF amounting to 39.513614 dB.**

Keywords— steganography, video, least significant bit, less significant frame, optical flow

I. INTRODUCTION

Steganography is a technique to hide messages that exploit flaws in the human sensory system [1], including human visual and auditory system. With the technique of steganography, secret messages can not be known presence by human sensory system easily. It also can face the processes of digital signal processing without damaging the quality of the data that have been inserted to some extent.

Today, the media type to hide the messages is very diverse, ranging from text, image, audio to video. Many researchers have proposed some methods to hide secret messages in the video. Steganographic methods can be grouped into two categories: spatial domain and frequency domain [2]. Steganography method in the spatial domain are popular, namely Least Significant Bit (LSB), Bit-Plane Complexity Segmentation (BPCS) [3], Pixel Value Differencing (PVD), Tri-Way Value Differencing (TPVD) and Edges based data embedding [4]. While examples of methods that included in the frequency domain are Discrete Cosine Transform (DCT), Fourier Transform (FT) and Discrete Wavelet Transform (DWT). Various methods of steganography well discussed by several researchers in [2], [4], [5].

The video is one of the media types that can be used to hide secret messages, with huge potential and is already widely used. Data that can be inserted or hidden in the video media has a far greater capacity than other media such as text, images and audio. Also, the video is available in a variety of formats so that it can be used for various purposes. The application of video steganography has many alternative methods. Almost all the steganographic methods that can be applied to the image can also be applied to video because the video is essentially a collection of some single image.

Currently, a variety of techniques and methods for hiding text or files data on video have been proposed by researchers. Sadek et al. categorize the various techniques of steganography in video media into six categories: substitution method, domain transformation, adaptive methods, methods based on format, real-time method and the method of generation cover [6]. Of the six categories, the substitution method is the method most popular and widely used. Some of the methods included in the substitution methods include Least Significant Bit (LSB), Bit-Plane Complexity Segmentation (BPCS) and Tri-way Pixel Value Differencing (TPVD).

Most of the substitution method proposed by the researchers is derived from the method LSB [6]. The LSB method inserts a message on the bits that are not significant or that do not significantly affect the image quality, especially visually. The advantages of this method are easy to implement and allow it to accommodate many secret messages.

One example application of the LSB method has been conducted by Singh and Agarwal to hide the digital image data in a video. The existence of the message is very difficult to be detected either by human eyesight as well as by specific program. Other studies combining LSB insertion method and encryption AES (Advanced Encryption Standard) to insert the digital image data in a video [8]. The encryption process is done after hiding a secret message in the video frame.

Some other researchers are also using the LSB method to insert data on the various video media. Yadav et al. implement XOR encryption and LSB method to insert data in a video frame with a specific pattern [9]. Paul et al. in [10] has proposed the implementation of LSB method to insert data in the form of a

.txt file. Data inserted in the video by observing changes in adjacent video frames. Meanwhile, Rachna Patel and Mukesh Patel had proposed the insertion of secret data on video with random position [11].

Frame selection of video as a location for insertion of data is one of the factors that affect the quality of the proposed methods. However, many methods have been proposed to apply the method LSB in each frame of a video sequence, such as in research [8], [10], [12]. Nowadays, only a few researchers are trying to make the selection frame insertion to improve the security of the data inserted. One of them uses the rules of Divide and Conquer algorithm to select the frame to be inserted [13]. Other researchers choose the frame randomly [11], [14].

TABLE I. RELATED PAPERS

Paper	Method	Data	Video Format	Hiding Location	PSNR (dB)
[7]	LSB	Text	Video	Each frame	-
[8]	LSB + EOF	Text	Video	Each frame	-
[9]	LSB + XOR	Video	Video AVI	Each Frame, pattern BGRRGBGR	35,45
[10]	LSB	Text	Video MPG, AVI, WMV	Each frame	141,41 s/d 155,29
[15]	LSB	Text	AVI	Particular frame	-
[16]	DCT, LSB	Image	Video AVI	Random frame	-
[17]	Motion Search Cost Minimized	Data	H.264 video	-	-
[11]	LSB	Video	Video	Random byte	-
[14]	RLSB	Text	Video	Random	-
[18]	LSB	Text	Video	RGB 2,3,3	95,5

In this study, we apply the LSB method to insert various media files documents on video. Also, the selection of the location to insert the data carried on the frame that was not significant (less significant frame) only. The frame selection is based on the value of optical flow that can characterize the movement on the video. Thus, the expected results of the quality of the video that has been inserted the data better than the previous method. Testing would be done using some video as media cover and also some types of documents that were inserted.

The purpose of this study was to produce a model that implements LSB and LSF methods to hide data in the video. We also develop a prototype to implement the proposed model. It prototype can enter the media-type container in the form of video AVI and the secret data type of Microsoft Word, Microsoft Excel, and Microsoft Powerpoint. The prototype can also calculate the value of PSNR that representing the quality of stego-video.

The contribution of this research is to produce a new method for selecting the right frame inserting a message in secret on a video. This study will introduce the concept of inserting a message on the insignificant frame which is determined by the movement of an object.

II. THE PROPOSED METHOD

A. Encoding and Decoding Model

The design model of steganography applications on video that implement the LSB and LSF (Less Significant Frame) method is constructed as Fig. 1

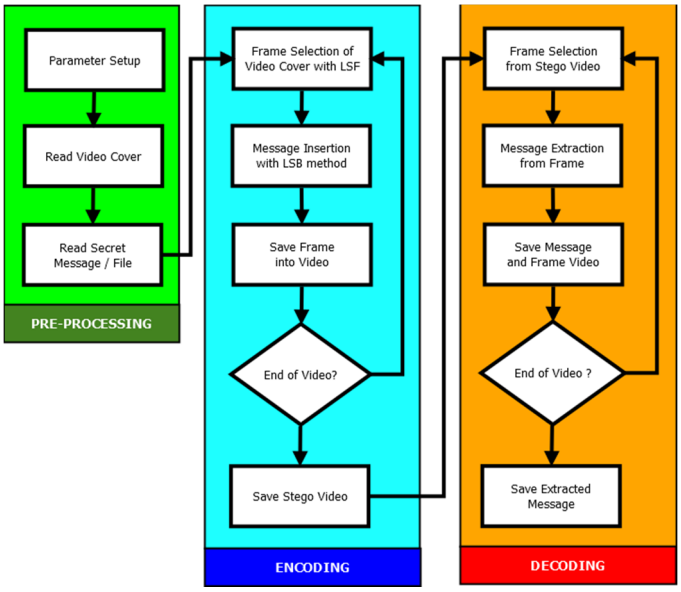

Fig. 1. Steganography Model.

The proposed model consists of three main processes: pre-processing, encoding and decoding. In the pre-processing stage, do the setting parameters such as the type of video cover, quality of output, the algorithms used and the selection of the frame to be inserted. Moreover, it also made the process of reading the video data and secret messages to be hidden. In the next stage, performed the process of reading the selected frame to be inserted a secret message, then combined or stored back into the video. The process will continue until all the secret messages have been inserted or video frame has ended. The video will be saved as a stego video.

Meanwhile, at the stage of decoding the secret message for each frame of video is extracted. The secret message will be extracted from the selected frame. Extracted messages will be reunited and saved into a file. Likewise, the cover video also saved.

B. Less Significant Frame (LSF)

In this study, we proposed Less Significant Frame (LSF) method to select the video frames to insert the message. The process of selecting a less significant frame is based on optical flow features representing the movement in the video. The value of optical flow indicates that there are some movements of the object in the video. Frames have a greater average value of optical flow will be selected as the location to hide the message because the movement in the video will obscure bits or pixels changes that occur as a result of the insertion process the message.

Optical flow is the movement pattern of objects, surfaces, and edges in a visual scene caused by the relative motion between an observer (an eye or a camera) and the object [19], [20]. The optical flow features describe the flow direction of the lighting of an object moving relative to a stationary observer or otherwise. Currently, optical flow is widely used in the field of robotics related to image processing, video, and navigation. Some of its applications are to movement detection, moving object segmentation and predictive direction of movement of the object.

The term optical flow first used in the field of human vision and introduced by psychologist James Jerome Gibson in the 1940s. However, in 1980-81, Horn and Schunck find a simple way to calculate the value of optical flow based on certain regularity [21]. Afterward, several optical flow calculation methods have been proposed by the experts, such as the Lucas-Kanade method [22], Camus [23], Nagel [24] and Simoncelli [25]. Some of it methods covered quite well by some researchers in [26]–[28].

$$r_{x,y} = \sqrt{{u_{x,y}}^2 + {v_{x,y}}^2} \quad (1)$$

$$\bar{r}_t = \frac{\sum_{x=1}^{w} \sum_{y=1}^{h} (r_{x,y})}{w.h} \quad (2)$$

$$\bar{r}_{tot} = \frac{\sum_{t=k}^{N} (\bar{r}_t)}{N} \quad (3)$$

In this research, we use Horn-Schunck method to obtain the optical flow value. The optical flow extraction performed on the whole frame of the video. For each pixel in the frame, the optical flow field is computed. The output value of the process is horizontal (u) and vertical (v) components in the complex form. Furthermore, based on the value of the vertical and horizontal components, the length of the vector (r) is computed for each point (x, y) using equation (1). The larger value of r means the larger movement of a point compared to the previous frame.

After having obtained the vector length for each point, then we calculated the average of the vector length for all the points in one frame ($\bar{r}_t$) using equation (2), whereis w is width of frame and h is height of frame. The entire value of r on each point are summed and divided by the number of pixels of the frame. Meanwhile, with the equation (3), the average of optical flow vector for N frames ($\bar{r}_{tot}$) is calculated. The value of N is the number of frames to be inserted with secret data. This amount is determined by the capacity needed to hide a secret file. A set of frames with the largest value of $\bar{r}_{tot}$ will be the location of a secret message insertion.

III. Results and Discussions

This section describes the experiments and results that performed in this study. The experiment is mainly aimed at the conclusion whether the proposed method has an influence on the quality of stego video.

A. Data Input

The experiments have been conducted using data input in any video cover and some files to be inserted into the video. The input data are obtained at random but represent a variety of file types. Video data that are used as a cover video in this study are presented in TABLE II. Meanwhile, the data of secret files have been presented in TABLE III. The experiment conducted by the two main scenarios: experiments with Less Significant Frame (LSF) method for selecting a frame, and experiment without LSF. The results of both scenarios will be compared to see the effect of the LSF method in the quality of stego video.

TABLE II. Video Cover

Num	File Name	Video Type	File Size	# of Frame
1	bunny.mp4	MP4	246 KB	69
2	video01.avi	AVI	6.350 KB	480
3	video02.avi	AVI	1.830 KB	120
4	video03.avi	AVI	8.850 KB	540

TABLE III. Secret File

Num	File Name	File Type	File Size
1	Bab-01-02-Presentasi.ppt	PPT	191 KB
2	Email Dosen FTI Genap 1112.xls	XLS	48 KB
3	Evaluasi Gasal 2015-2016.xlsx	XLSX	86 KB
4	Format-Makalah2011.doc	DOC	73 KB
5	Hasil Raker Kurikulum FTI.pptx	PPTX	2.490 KB
6	sherlock.txt	TXT	40 KB
7	TemplateKontrakKuliahFTI-Algo1.docx	DOCX	57 KB

B. Experiments with LSF

Experiments have been conducted by combining the video covers of TABLE II. with the message files of TABLE III. Thus performed as much as 28 times the experiment. In each experiment, the message file will be inserted into the video using the Least Significant Bit (LSB). At the first experiment phase, the process of selecting the frame to be inserted is determined at the N first frame of the video. N is the number of frames to be inserted, and it is determined by the size of the message file. Once the message was inserted into each frame, then calculate PSNR value to determine the quality of steganography results. The time required to perform the insertion (encoding) and the time required for the extraction (decoding) also noted.

The results of the experiments have been done on the prototype of steganography applications on video by the LSB method without using LSF (Less Significant Frame) indicates that the message insertion process fails three times or about 10%. The cause of the failure of the insertion process is the message file is too large to cover video capacity is insufficient. For example, the file "Hasil Raker Kurikulum FTI.pptx" required a

storage capacity of 496 frames, while the video "bunny.mp4" consists of 69 frames only.

Meanwhile, judging from the quality of steganography, the average PSNR value of the entire experiments is 39.513614 dB. It means the quality of the stego video is good. The highest average value of PSNR is 46.488725 dB, and the lowest average value of PSNR is 37.156272 PSNR dB. Fig. 2 presents a comparison chart of PSNR value for each experiment, both with and without LSF.

If seen from the time of insertion and extraction messages, in general, the insertion time for each frame includes fast. The average time of insertion for the entire experiments is 14.676 milliseconds and the average time of message extraction are 0.287 milliseconds.

C. Experiments with LSF

In the second scenario of the experiment, we performed by applying the LSF method for selecting insignificant frames. As already described in the previous section, the LSF method makes the selection frame based on the optical flow value of every frame. The frames that have a big value of optical flow indicates that there is a significant movement in the video. The frames are selected as the location of message insertion. When there is a significant movement in the video, by visual observation, the pixel value changes that occur will be more difficult to detect. Thus, the secret message will be well protected and secure.

The second experiment provides an average PSNR of 44.417638 dB. These results demonstrate the quality of the resulting steganography is GOOD. The lowest PSNR value is 39.875939 dB, and the highest value is 46.629572 dB. The graph in Fig. 2 shows the average PSNR for all experiments have been conducted.

Experiments also showed that the time of encoding and decoding messages fast enough. Overall, the average time the insertion of a message is approximately to 7.66 milliseconds for each frame, and the average time of message extraction is 0.366 milliseconds per frame. Figure 3 and Figure 4 presents the average chart time encoding and decoding processes of the whole experiment. In comparison, the average time required to perform the insertion longer than the time required in the extraction process messages. It happens because the message insertion process (encoding) there is a bit insertion operations on each pixel of the image (frame).

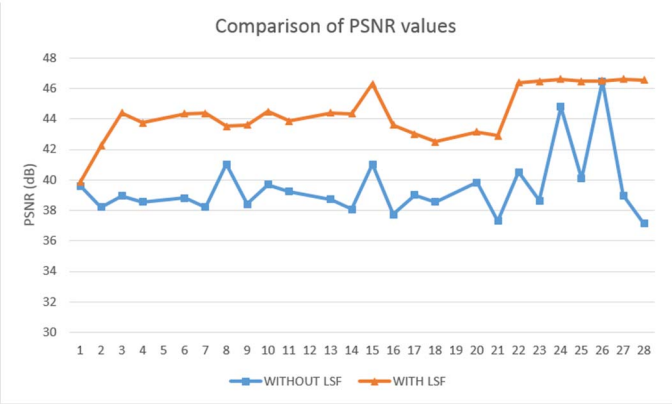

Fig. 2. Comparison of PSNR values.

D. Discussions

A series of experiments have shown differences in an image (frame) quality results between the LSB steganography method without and with LSF frame selection. Figure 2 displays the comparison of the average PSNR for the entire experiments. In comparison, the use of methods LSF (Less Significant Frame) produces better image quality than without using LSF. In experiments with LSF method has resulted in the PSNR average value of 44.417638 dB, whereas in testings without LSF method produces an average PSNR of 39.513614 dB. Although the difference in value amounted to only 4.904024 dB, it was enough to prove that the use of LSF method is better than no method of LSF.

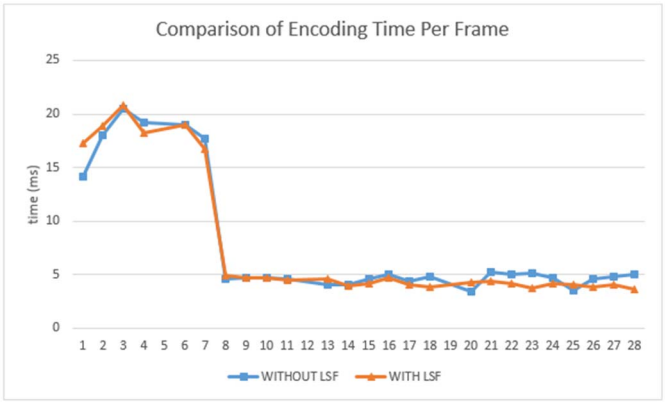

Fig. 3. Comparison of Encoding Time per Frame

Meanwhile, if viewed from the time the message insertion and extraction process the message, it was not a significant difference between the experiments with and without LSF. The time of the insertion process (encoding) with LSF method has an average time of 7.66 milliseconds per frame while on testing without LSF average time of 7.83 milliseconds per frame. The time difference between the two is not too significant, but experiment with methods LSF shows the average time better. Figure 3 shows a comparison of the encoding time for each frame of the experiments with and without LSF.

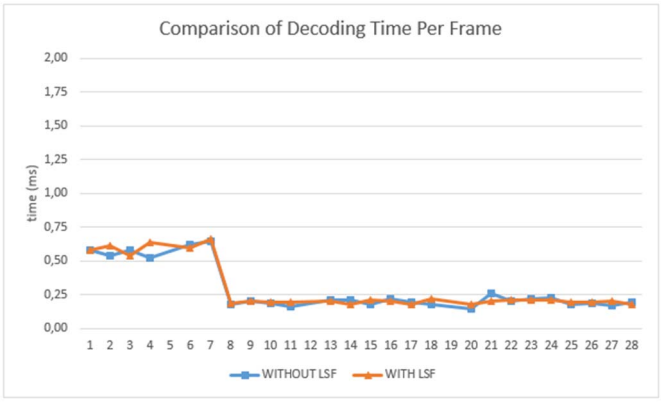

Fig. 4. Comparison of Decoding Time per Frame

Likewise, the ratio of the average time of message extraction (decoding). The average time of message extraction with LSF method are 0.287 milliseconds per frames and amounted to 0.294 milliseconds per frame for experiment without LSF. The time difference between the two is very small. The comparison between the decoding time of all experiments shown in Figure 4.

IV. Conclusion and Future Works

Based on the experiment results and discussions that have been performed, there are some conclusions. Secret messages insertion into the video using the LSB method can be done by first extracting the videos into single frames (images). Secret message can be inserted in the frames in sequence, or randomly chosen. In this study, we proposed a method of the inserting message by selecting a less significant frame as the insertion point.

The selection of a less significant frame is based on optical flow features that are representing the movement in the video. The greater value of optical flow indicates that there is a greater move. Frames with a large value of optical flow chosen as the location of the insertion, because visually a movement will blur the change bits or pixels that occur as a result of the insertion process.

The test results showed that in experiments with methods LSB and LSF, the quality of video that has been inserted proved to be better than the experiment without LSF. The average value of PSNR on trial with the LSB and LSF method amounted to 44.417638 dB, whereas in experiments without LSF amounting to 39.513614 dB. The experiment results also showed that regarding speed insertion process (encoding) and extraction (decoding) the message was not a significant difference between the use of methods LSF and not. Overall, we can conclude that the performance of the LSF method that we proposed in this research is good enough.

This research still needs to be continued in the future. The LSF (Less Significant Frame) method still need to be developed to produce a better quality of stego video. In this study, the selection of a less significant frame based on the movement using optical flow features. In a subsequent study, frame selection techniques can be tried a less significant by other methods, for example by color or contour features.

In addition to the improvement of the LSF method, in this study only tested the image quality of steganography. In further research can be tested from the another measurement such as visual perception (imperectibility) and resistance to external influences (robustness).

References

[1] R. Sigit, Step By Step Pengolahan Citra Digital. YOGYAKARTA: Andi Publisher, 2007.

[2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital Image Steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[3] E. Kawaguchi and R. O. Eason, “Principles and applications of BPCS steganography,” in Proceedings of SPIE, 1999, pp. 464–473.

[4] M. Hussain and M. Hussain, “A Survey of Image Steganography Techniques,” Int. J. Adv. Sci. Technol., vol. 54, pp. 113–124, 2013.

[5] X. Y. Luo, D. S. Wang, P. Wang, and F. L. Liu, “A review on blind detection for image steganography,” Signal Processing, vol. 88, no. 9, pp. 2138–2157, 2008.

[6] M. M. Sadek, A. S. Khalifa, and M. G. M. Mostafa, “Video steganography: a comprehensive review,” Multimed. Tools Appl., vol. 74, no. 17, pp. 7063–7094, 2015.

[7] S. Singh and G. Agarwal, “Hiding image to video : A new approach of LSB replacement,” Int. J. Eng. Sci. Technol., vol. 2, no. 12, pp. 6999–7003, 2010.

[8] H. Gupta and S. Chaturvedi, “Video Steganography through LSB Based Hybrid Approach,” Int. J. Eng. Res. Dev., vol. 6, no. 12, pp. 32–42, 2013.

[9] P. Yadav, N. Mishra, and S. Sharma, “A Secure Video Steganography with Encryption Based on LSB Technique,” in International Conference on Computational Intelligence and Computing Research, 2013, pp. 1–5.

[10] R. Paul, A. K. Acharya, V. K. Yadav, and S. Batham, “Hiding Large Amount of Data using a New Approach of Video Steganography,” in Long Island Systems, Application and Technology Conference, 2014, pp. 337–343.

[11] R. Patel and M. Patel, “Steganography over Video File by Hiding Video in another Video File, Random Byte Hiding and LSB Technique,” in International Conference on Computational Intelligence and Computing Research, 2014, pp. 5–10.

[12] K. S. Jenifer, G. Yogaraj, and K. Rajalakshmi, “LSB Approach for Video Steganography to Embed Images,” vol. 5, no. 1, pp. 319–322, 2014.

[13] P. Sangit and S. Shinde, “Steganography In Videos Using Unique Frame Selection Technique,” in 33th IRF Int Conference, 2015, pp. 1–4.

[14] A. Basu, G. Kumar, and S. Sarkar, “A Video Steganography Approach using Random Least Significant Bit Algorithm,” Int. J. Sci. Res., vol. 3, no. 6, pp. 1811–1816, 2014.

[15] K. U. Singh, “Video Steganography : Text Hiding In Video By LSB Substitution,” Int. J. Eng. Res. Appl., vol. 4, no. 5, pp. 105–108, 2014.

[16] M. S. Kumar and G. M. Latha, “DCT Based Secret Image Hiding In Video Sequence,” Int. J. Eng. Res. Appl., vol. 4, no. 8, pp. 5–9, 2014.

[17] M. Zhang and Y. Guo, “Video Steganography Algorithm with Motion Search Cost Minimized,” in 2014 IEEE 9th Conference on Industrial Electronics and Applications (ICIEA), 2014, pp. 940–943.

[18] M. Dixit, N. Bhide, S. Khankhoje, and R. Ukarande, “Video steganography,” in 2015 International Conference on Pervasive Computing (ICPC), 2015, pp. 1–4.

[19] A. Burton and J. Radford, Thinking in Perspective: Critical Essays in the Study of Thought Processes. Routledge, 1978.

[20] Wikipedia, “Optical Flow,” 2011. [Online]. Available: http://en.wikipedia.org/wiki/Optical_flow.

[21] B. K. P. P. Horn and B. G. Schunck, “Determining Optical Flow,” Elsevier Artif. Intell., vol. 17, no. 1–3, pp. 185–203, 1981.

[22] B. D. Lucas and T. Kanade, “An Iterative Image Registration Technique with an Application to Stereo Vision,” in Proc. 7th International Conference on Artificial Intelligence (IJCAI) 1981, 1981, pp. 121–130.

[23] T. Camus, “Real-Time Quantized Optical Flow,” Real-Time Imaging, vol. 3, no. 2, pp. 71–86, Apr. 1997.

[24] H.-H. Nagel, “On the estimation of optical flow: Relations between different approaches and some new results,” Artif. Intell., vol. 33, no. 3, pp. 299–324, Nov. 1987.

[25] E. P. Simoncelli, “Design of multi-dimensional derivative filters,” in Procs of 1st Int. Conf. on Image Processing, 1994, vol. 1, pp. 790–794.

[26] J. Barron, D. Fleet, and S. Beauchemin, “Performance of optical flow techniques,” Int. J. Comput. Vis., vol. 12, no. 1, pp. 43–77, 1994.

[27] R. Krishnamurthy, P. Moulin, and J. Woods, “Optical flow techniques applied to video coding,” in International Conference on Image Processing, 1995., 1995, pp. 570–573.

[28] E. Patel and D. Shukla, “Comparison of Optical Flow Algorithms for Speed Determination of Moving Objects,” Int. J. Comput. Appl., vol. 63, no. 5, 2013.