# Frames Selection Based On Modified Entropy And Object Motion In Video Steganography

**Muhammad Fuad, FerdaErnawan**

**Abstract:** Steganography schemes have been widely implemented in multimedia communication. Multimedia data, such as videos are often compressed to reduce the storage in the limited bandwidth. However, most video steganography schemes are not resistant to compression. The video provides additional hidden space in the image frame sequences. This research proposes a frame selection technique based on object motion and modified entropy in video steganography. The object motions in the video frame are determined by horizontal and vertical of motion vectors. The video frames that have object motion are computed by using modified entropy. The lowest modified entropy frames are selected for concealing a secret message. The proposed frame selections able to produce minimum distortion of stego-video compare to non-frame selection. The experimental results show that our scheme achieves good robustness of message recovery in terms of Bit Error Rate (BER) and Normalized Cross-Correlation (NC). The recovered messages of the proposed steganography scheme can survive under video compression.

**Index Terms:** Video Steganography, Edge Entropy, Object Motion, Frame Selection, Entropy.

## 1. INTRODUCTION

THeprivate and secure communication becomes important due to the rapid growth of digital communications. Data transmission in open network is not secure and it can be tempered by unauthorized user [1].Hence, to solve that problem, data hiding is developed to protect the data by hiding them in cover media. Steganography is a technique for concealing the message in digital communications [2][3][4][5].Video provides a large hidden capacity and it also provides a large redundancy along with the sequence image frames [6]. Therefore, video steganography becomes a potential medium for concealing a message in digital communication.Video data is usually compressed in digital communication. Most of video steganography schemes are not resistant against compression method. The hidden message will be destroyed under the quantization process in video compression [7]. This issue becomes considerable critical attention because most of the applications have been integrated with digital compression. Hence, developing video steganography technique that can maintain video quality close to the original video and the hidden data become resistant to compression are quite challenging. It motivates us to develop frame selection scheme in video steganography that can maintain the stego-video quality. The challenges in video steganography are to protect hidden data from compression and secure the concealing message from stego-analysis [8][9]. This paper proposes a frame selection scheme based on object motion and modified entropy in video steganography. The movement of the object is used to determine the hiding frame in the steganography. The selected frames that have object motions are computed by using modified entropy. The hiding data will be performed in the selected frames, which have the lowest entropy. The selected frame potentially to hide the message and it becomes less sensitive to the human visual characteristics. The proposed video steganography scheme hides the message into the selected frequency coefficients using the proposed hiding algorithm. The proposed selected frame can maintain the minimum distortion in the quality of stego-video.

## 2 RELATED WORK

The video steganography technique transfers the hidden data to the right receiver and avoids any unwanted third-party.The hidden data into the cover video should not be seen by the human visual system.Ramalingam M [10] presented a video steganography scheme that provides a robust and secure hiding message.Ramalingam presented video steganography scheme using modified Least Significant Bit (LSB) for cover video. LSB method is widely applied in steganography technique. LSB becomes effective for hidden data due to fast concealing and it can maintain the quality of stego-video.While, their scheme does not consider the location and frame selection for concealing the secret message.Jaya et al [11] presented enhanced LSB technique by using human detection method as stego key that describe the location of the hidden message. Their scheme able to maintain the appearance of the cover video and it can secure the hiding message. Their scheme achieved the average of PSNR value about 48 dB for all sample videos. LSB techniques in video steganography are not able to withstand against MPEG compression.Hashemzadeh [12] presented hiding information using features points' technique. The feature point is used to determine the suitable region for hiding the information. This scheme used LSB map to conceal the message along the region of interest (ROI). The results reported that it achieved high perceptual invisibility of the hidden data. Video steganography using LSB preserves high video quality, while it generally can be removed by compression attacks. The hiding technique that can resist under compression become a challenge in video steganography.Ramalingam and Isa [13] presented video steganography based on scene change technique for hiding the message. In this technique, their scheme used Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) to hide the secret message. Transform domain technique are generally robust than spatial domain. The hidden message at the scene change of video can make it difficult to be detected by attackers.The normalized DWT improve the quality of stego-video, however DWT request a large computation time and complexity.Jangid and Sharma [14] presented video steganography using Multi Level Clustering (MLC) algorithm. Their scheme used LSB substitution for hiding data. The proposed MLC used K-mean clustering to cluster the video frames. The results reported thattheir scheme produced a high PSNR value of stego-video. The clustering video frames based on K-means algorithm can produce different results for the same input video.

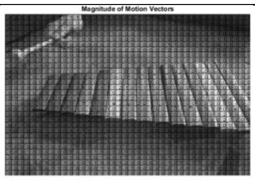

***Fig. 2**. Illustration of the magnitude of motion vectors*

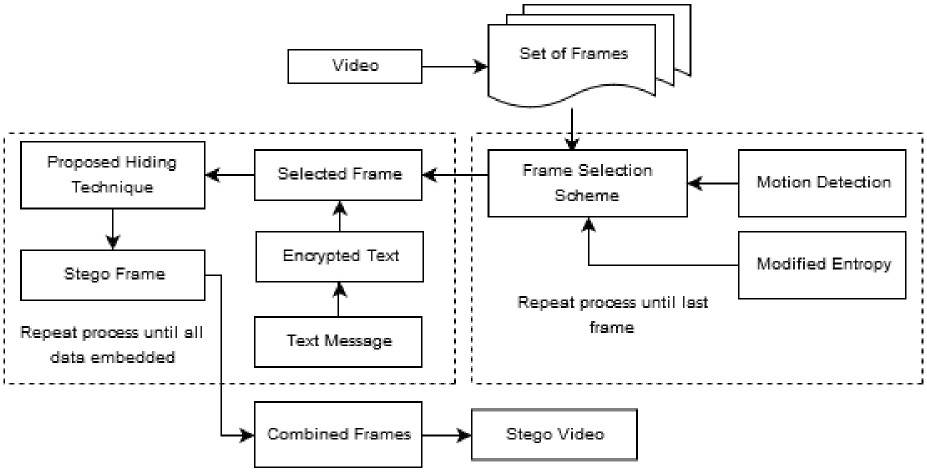

***Fig. 1.** Proposed Hiding Scheme*

## 3 PROPOSED SCHEME

### 3.1 Hiding Technique

The proposed video steganography scheme is shown in Fig. 1. The first step, a video was split into frame-by-frame. Each frame was computed by the motion detection method to find the motion vector. Motion detection was performed with non-overlapping blocks of 8x8 pixels from left to right and top to bottom. Motion vector can be calculated by Cumulative Absolute Difference (CAD) between current and previous frames. The blocks that have motion vector can be utilized to conceal the message. The magnitude of motion vector can be defined by:

$$m = \sqrt{x^2(i) + y^2(i)} \qquad (1)$$

Where m denotes the magnitude value, x[i] represents the horizontal motion vector and y[i] is denotes vertical motion vector in the i-thmacro-block. The visual illustration of the magnitude of motion vector is shown in Fig. 2.

Referring to Fig. 2, the macro-block with the significant magnitude values are selected for hiding location. This paper proposes frame selection scheme based on motion detection and modified entropy as shown in Fig. 3. After we obtained all motion vectors, each frame is computed by using modified entropy. The modified entropy is defined by:

$$E = -\sum_{i=1}^{n} p_i \log 2(p_i) + p_i \exp 1 - p_i \qquad (2)$$

$p_i$indicates the probability of i, $0 \le p_i \le 1$ . The entropy of image frames is sorted by ascending order. The frame with the lowest modified value are selected for first hiding message. The hiding location is determined by the significant magnitude of motion vectors. Before the message is being inserted, the message is encrypted by using Advanced Encryption Standard (AES) 128 bits. The scrambled message bits by AES provide additional security in the video steganography from attackers [15].

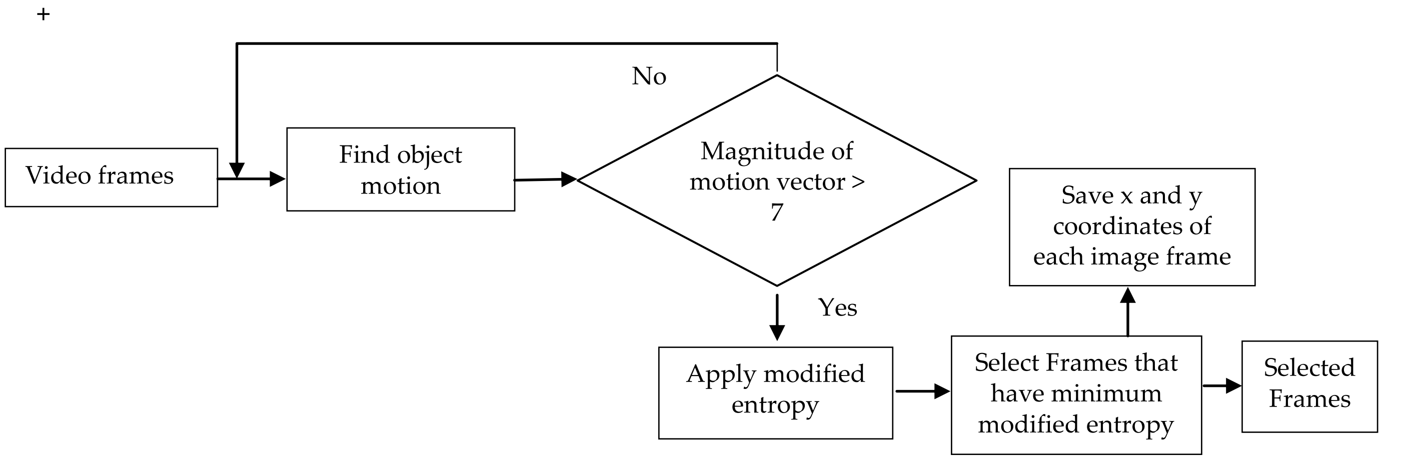
+
Video frames
Find object motion
Magnitude of motion vector > 7
No
Yes
Save x and y coordinates of each image frame
Apply modified entropy
Select Frames that have minimum modified entropy
Selected Frames

***Fig. 3**. Frame Selection Scheme*

Each selected frame is transformed by DCT. The message is hidden by examining the selected DCT coefficients of ((3,2) (2,3)), ((1,3) (0,4)) and ((1,4) (2,3)) coordinates. The selected coefficients are grouped into three pairs. If the hiding message equal to 1, the first coefficient is less than the second coefficient, the value will swap and add the threshold value of the first coefficient. Else, the value of the first coefficient will be replaced with the second coefficient and add to the threshold value. The hiding technique for message bit equal to 1 is given as follows:

```
        if(|SC(2x)|<|SC (2x+1)|)then
             C= SC (2x);
             SC (2x)= SC (2x+1)+ s;                    (3)
             SC (2x+1)=C;
        else
             SC (2x)= SC (2x)+ f;
             SC (2x+1)=A(2x+1);
```

The hidden message will consider the length of message bits. If the hidden message equal to 0, then the first coefficients is less than the second coefficients, the value of the second coefficient is added with a threshold coefficient. Else, the value of the first coefficient will be swapped with the second coefficient and the second coefficient will be addedbya threshold. The hiding technique for message bit equal to 0 is given as follows:

```
         if(|SC (2x)|<| SC (2x+1)|)then
             SC (2x)= SC (2x)+ s;
             SC (2x+1)= SC (2x+1);                     (4)
         else
                C= SC (2x);
                SC (2x)= SC (2x+1);
                SC (2x+1)=C+ f;
         end (if)
```

where for x = 0,1 and 2. SC (2x) represents SC(0), SC(2) and SC(4) and SC(2x+1) denotes SC(1) and SC(3). f and s are the proposed scaling factor for hiding data. Then merge all frames into a video data.

### 3.2 Extracting Technique

A stego-video is divided into the image frames. Referring to the motion analysis from the database, x and y block coordinates of the hidden message are identified for each selected frame. Each selected block is transformed by 8x8 DCT. The message can be extracted with certain rules. If the first coefficient pair is less than the second coefficient, the message bit equal to 1. If the first coefficient pair is greater than second coefficients, then the message bit equal to 0. The extracted message is decrypted by AES 128 bits. Next, the message bits are rearranged to reconstruct the message.

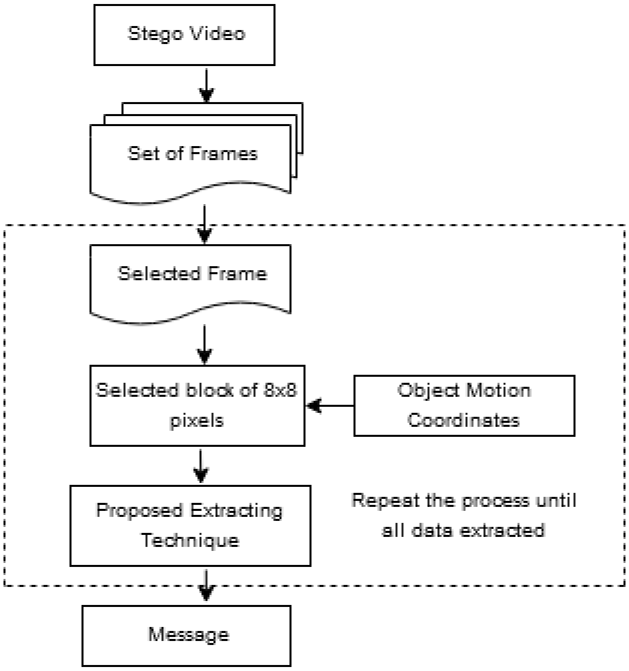
Stego Video
Set of Frames
Selected Frame
Selected block of 8x8 pixels
Object Motion Coordinates
Proposed Extracting Technique
Repeat the process until all data extracted
Message

***Fig. 4**. Proposed extracting messages*

### 3.3 Evaluation

The invisibility of the stego-video is evaluated by mean absolute reconstruction error (MARE).It measures the difference quality between the original video and stego-video. The lowest MARE represents highest invisibility of stego-video. The MARE is defined by:

$$ARE = \frac{1}{MNR}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\sum_{k=0}^{2}\left(f\left(i,j,k\right)-g\left(i,j,k\right)\right) \quad (5)$$

$$MARE\left(x,y\right)=\frac{1}{S}\sum_{j=1}^{S} ARE\left(x_j,y_j\right) \quad (6)$$

The extracting message fromstego-video under MPEG compression is evaluated by Bit Error Rate (BER) and

Normalized-Cross Correlation (NC). If the BER value is small, message recovery is closer to the original message. The higher NC value indicates that the extracting message resistance against attacks. The BER and NC are defined by:

$$NC = \frac{\sum_{i=1}^{D} H(i).H^{*}(i)}{\sqrt{\sum_{i=1}^{D} H(i)^{2} \sum_{i=1}^{D} H^{*}(i)^{2}}} , \quad MNC = \frac{1}{S}\sum_{j=1}^{S} NC(j) \tag{7}$$

$$BER = \frac{\sum_{i=1}^{D} H(i) \oplus H^{*}(i)}{D} , \quad MBER = \frac{1}{S}\sum_{j=1}^{S} BER(j) \tag{8}$$

where H denotes the original message, H* represents the recover messages, D is the length of message bits and S denotes the number of selected video frames.

## 4 EXPERIMENTAL RESULTS

These experiments used ten videosto test the proposed steganography scheme. The sample videos [16]are shown in Fig. 5. The general video information is listed in Table 1. The experiments were performed in Matlab running on a CPU @ 2.3GHz processor under windows operating.

**Table 1**
General Information Videos

| Video | Resolution | Bit rate | Duration | File Size |
|---|---|---|---|---|
| Akiyo | 352x264 | 30 | 10s,120ms | 710kb |
| Foreman | 352x288 | 30 | 10s,43ms | 2.22mb |
| Xylophone | 320x240 | 30 | 4s,700ms | 464kb |
| Soccer | 352x288 | 60 | 9s,823ms | 2.09mb |
| Football | 352x240 | 30 | 11s,566ms | 1.79mb |
| Coastguard | 352x288 | 30 | 10s | 87.1mb |
| Mobile | 352x288 | 30 | 10s | 87.1mb |
| Waterfall | 352x288 | 30 | 8s,667ms | 73.1mb |
| Flower | 352x288 | 30 | 8s,333ms | 73.1mb |
| Bus | 352x288 | 30 | 5s | 43.6mb |

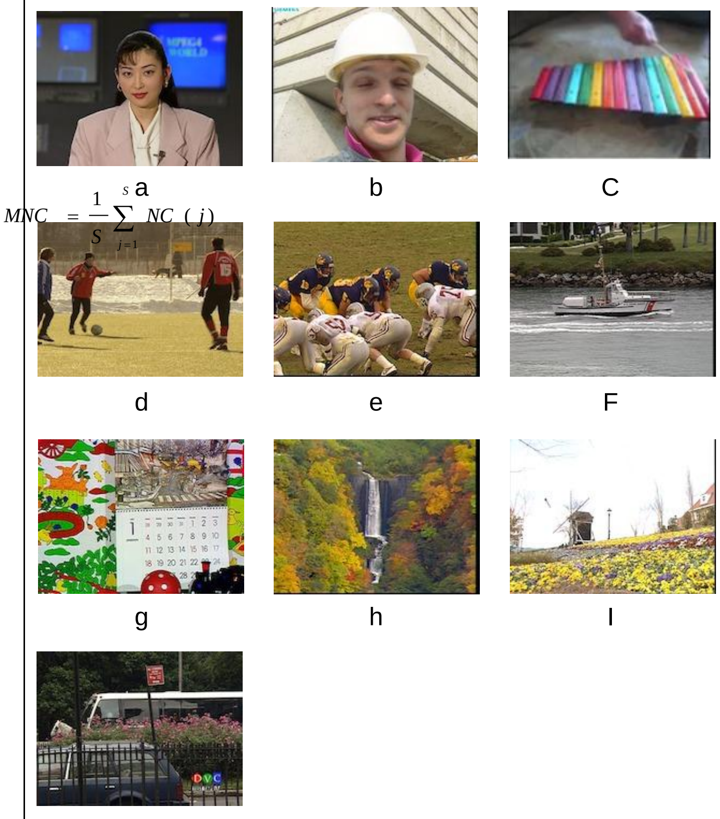

Fig 5. Sample videos:a. Akiyo, b. Foreman, c. Xylophone, d. Soccer, e. Football, f. Coastguard, g. Mobile, h. Waterfall, i. flower, j. Bus

The invisibility of the proposed video steganography is listed in Table 2. The lowest absolute error reconstruction indicates the highest imperceptibility. The experimental results show that the embedding based on LSB produces lower error reconstruction than the proposed scheme under different amounts of hidden data. Meanwhile, our scheme produces relatively small distortion of stego video. The experiments have been tested by MPEG compression as shown in Tables 3 and 4. The proposed scheme outperforms LSB technique in terms of BER and NC values for recovering a message under MPEG compression. Our scheme hides a message into the selected frame based on modified entropy frames. It can avoid message removal when the stego-video was cropped at the first frame. The frame selection also able to improve the security from unauthorized user. Our technique demonstrates potentially resistant of the hidden data against MPEG compression 3.The proposed scheme has limitations such as the hidden data's capacity depends on the number of detected motion in the video data. This scheme only suitable for video data that have object movement. The proposed scheme is not suitable for video content without object movement.

**Table 2**

Absolute Reconstruction Error of The Stego-Video

| Video | 1600 bit | | | 5600 bit | | |
|---|---|---|---|---|---|---|
| | LSB | Without Frame Selection | Proposed scheme | LSB | Without Frame Selection | Proposed scheme |
| Akiyo | 0.0000146 | 0.0118 | 0.0088 | 0.0000498 | 0.0339 | 0.0745 |
| Foreman | 0.0000134 | 0.0109 | 0.0122 | 0.0000468 | 0.0403 | 0.0422 |
| Xylophone | 0.0000355 | 0.0159 | 0.0163 | 0.0001206 | 0.0559 | 0.1827 |
| Soccer | 0.0000068 | 0.0139 | 0.5536 | 0.0000221 | 0.1560 | 0.5860 |
| Football | 0.0000145 | 0.0402 | 0.0632 | 0.0000460 | 0.0839 | 0.1065 |
| Coastguard | 0.0000133 | 0.0085 | 0.0085 | 0.0000433 | 0.0300 | 0.0300 |
| Mobile | 0.0000068 | 0.0160 | 0.0161 | 0.0000221 | 0.0547 | 0.0540 |
| Waterfall | 0.0000153 | 0.0091 | 0.0094 | 0.0000500 | 0.0321 | 0.0333 |
| Flower | 0.0000160 | 0.0040 | 0.0039 | 0.0000640 | 0.0125 | 0.0125 |
| Bus | 0.0000267 | 0.0106 | 0.0107 | 0.0000867 | 0.0389 | 0.0406 |

**Table 3**

Bit Error Rate of The Recovered Message Under Mpeg4 Compression

| Video | 1600 bit | | | 5600 bit | | |
|---|---|---|---|---|---|---|
| | LSB | Without Frame Selection | Proposed scheme | LSB | Without Frame Selection | Proposed scheme |
| Akiyo | 0.4906 | 0.1099 | 0.0672 | 0.4816 | 0.0333 | 0.0499 |
| Foreman | 0.5220 | 0.1778 | 0.3329 | 0.5039 | 0.0621 | 0.3317 |
| Xylophone | 0.4611 | 0.0741 | 0.0025 | 0.4934 | 0.0220 | 0.0122 |
| Soccer | 0.4466 | 0.0691 | 0.4001 | 0.4705 | 0.0300 | 0.4049 |
| Football | 0.4805 | 0.0264 | 0.0302 | 0.5018 | 0.0377 | 0.0315 |
| Coastguard | 0.4749 | 0.0923 | 0.1394 | 0.4971 | 0.1261 | 0.1295 |
| Mobile | 0.4692 | 0.0584 | 0.0754 | 0.4882 | 0.1094 | 0.1218 |
| Waterfall | 0.4899 | 0.0955 | 0.000628 | 0.4830 | 0.0290 | 0.000715 |
| Flower | 0.5151 | 0.3700 | 0.3474 | 0.4823 | 0.4174 | 0.4034 |
| Bus | 0.4981 | 0.0942 | 0.1024 | 0.4941 | 0.1264 | 0.0959 |

**Table 4**

Normalized Cross-Correlation The Recovered Message Under Mpeg4 Compression

| Video | 1600 bit | | | 5600 bit | | |
|---|---|---|---|---|---|---|
| | LSB | Without Frame Selection | Proposed scheme | LSB | Without Frame Selection | Proposed scheme |
| Akiyo | 0.8434 | 0.9301 | 0.9624 | 0.8134 | 0.9738 | 0.9690 |
| Foreman | 0.8309 | 0.9292 | 0.9643 | 0.8311 | 0.9673 | 0.9712 |
| Xylophone | 0.8405 | 0.9559 | 0.9932 | 0.8337 | 0.9857 | 0.9941 |
| Soccer | 0.8435 | 0.9527 | 0.9951 | 0.8251 | 0.9796 | 0.9830 |
| Football | 0.8258 | 0.9828 | 0.9821 | 0.8332 | 0.9673 | 0.9813 |
| Coastguard | 0.8204 | 0.9587 | 0.9276 | 0.8287 | 0.9354 | 0.9305 |
| Mobile | 0.8204 | 0.9568 | 0.9458 | 0.8188 | 0.9363 | 0.9328 |
| Waterfall | 0.8254 | 0.9312 | 0.9966 | 0.8219 | 0.9757 | 0.9980 |
| Flower | 0.8146 | 0.8976 | 0.9047 | 0.8085 | 0.8953 | 0.8971 |
| Bus | 0.8146 | 0.9389 | 0.9359 | 0.8075 | 0.9321 | 0.9429 |

## 5 CONCLUSION

This paper presented frame selection invideo steganography using modified entropy and object motion. The message is hidden along with the object motion. The hidden message is not sequentially concealed into the video frames. The frames of video that havelowest modified entropy are first hiddenthe message bits. The proposed hidden message examines the DCT coefficients with the certain rules. The proposed scheme has some limitation such as it can't be used for videos without object motion in the video frames. The video that has high-object motion is most suitable for the proposed scheme. The proposed scheme requires high computational time for identifying object motion and entropy value for each frame. However, the proposed hiding scheme able to withstand against compression attack. Our scheme also produces high invisibility of the stego-video.The results show that the proposed scheme achieves high robustness, the extracting message along object movement survives under MPEG4 compression

## ACKNOWLEDGMENT

This research was endorsed by the Postgraduate Research Grant Scheme PGRS190390, University Malaysia Pahang.

## REFERENCES

[1] T. Idbeaa, S. A. Samad, H. Husain, " A Secure and Robust Compressed Domain Video Steganography for Intra and Inter Frames Using Embedding Based Byte Differencing (EBBD) Scheme," Plos One vol. 11, pp. 1-22, 2016.

[2] N. Kar, K. Mandal, B. Bhattacharya, "Improved chaos-based video steganography using DNA alphabets," ICT Express vol. 4, pp. 6-13, 2018.

[3] M.M. Sadek, A.S. Khalifa, M.G.M. Mostafa, "Robust video steganography algorithm using adaptive skin-tone detection," Multimedia Tools and Applications vol. 76,pp. 3065-3085, 2017.

[4] M. Dalal, and M. Juneja, "Video Steganography Techniques in Spatial Domain—A Survey," Proceedings of the International Conference on Computing and Communication Systems, pp. 705-711, 2018.

[5] K. Rajalakshmi, K. Mahesh, "Robust Secure Video Steganography Using Reversible Patch-wise Code Based Embedding," Multimedia Tools and applications vol. 77, pp. 27427-27445, 2018.

[6] M.E. Eltahir, L.M. Kiah, B.B. Zaidan, A.A. Zaidan, "High rate video streaming steganography," International Conference on Information Management and Engineering," ICIME'09, IEEE, 2009, pp. 550–553.

[7] D. Sarmah, A. J. Kulkarni,"JPEG based steganography methods using cohort intelligence with cognitive computing and modified multi random start local search optimization algorithms,"Information Science, vol. 430, pp. 378-396, 2018.

[8] L. Xin, Q. Zheng, D. Liping,"Data embedding in digital images using critical functions,"Signal Process: Image Communication, vol. 58, pp. 146-156, 2017.

[9] D. Sarmah, A. J. Kulkarni,"Image steganography capacity improvement using cohort intelligence and modified multi random start local search methods," Arabian Journal for Science and Engineering vol. 43, no. 8, pp. 3927-3950, 2018.

[10] M. Ramalingam, "Stego Machine Video Steganogprahy using Modified LSB algorithm,"International Journal of Information and Communication Engineering,vol. 50, no. 2, pp. 497-500, 2011.

[11] P. G. P. Jaya. B. Hidayat, I. F. Y. Suratman, "Enhanced LSB Steganography with People Detection as Stego Key /generator," International Conference on Sognal and Systems (ICSigSys), pp. 99- 104, 2017.

[12] M. Hashemzadeh, "Hiding Information in videos Using Motion Clues of Feature Points," Computers and Electrical Engineering, pp. 14-25, 2018.

[13] M. Ramalingam, N. A. M. Isa, "A data-hiding technique using scene change detection for video steganography," Computers and Electrical Engineering, pp. 423-434, 2016.

[14] S. Jangid, S. Sharma, "High PSNR based Video Steganography by MLC Algorithm," International Conference on Intelligent Computing and Control System, pp. 589-594, 2017.

[15] R. Padate, A. Patel, "Encryption and Decryption of Text using AES Algorithm," International Journal of Emerging Technology and Advance Engineering, pp. 883-886, 2014.

[16] Video test media (derf's collection) 2018. Available: https://media.xiph.org/video/derf