**International Journal of Science and Research (IJSR)**
**ISSN (Online): 2319-7064**
**Impact Factor (2012): 3.358**

# A Secured Data Hiding Technique Using Video Sequences

**Y. Mahendhar[1], B. Satish Chandra[2]**

[1]Jyothishmathi Institute Of Technology and Science, Nustullapur, Karimnagar, India

**Abstract:** ***Secret communication using the Compressed Video file as cover medium and data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis, we target the motion vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The choice of candidate subset of these motion vectors are based on their associated macro block prediction error, which is different from the approaches based on the motion vector attributes such as the magnitude and phase angle, etc. A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bit stream is embedded in the least significant bit of both components of the candidate motion vectors. The method is implemented and tested for hiding data in natural sequences of multiple groups of pictures and the results are evaluated. The evaluation is based on two criteria: minimum distortion to the reconstructed video and minimum overhead on the compressed video size. Based on the aforementioned criteria, the proposed method is found to perform well and is compared to a motion vector attribute-based method from the literature***.

**Keywords:** Data hiding, motion vectors, Motion Picture Expert Group (MPEG), steganography.

## 1. Introduction

Information hiding has attracted lots of attention over recent years. It is the art and technique of concealing a message in a cover without leaving any remarkable trace on the cover signal [1]. There are three main compromising attributes for a data hiding system, known as capacity, imperceptibility, and robustness. The data hiding schemes are principally categorized into *steganography* and *watermarking*, according to the application based requirements. In the steganography systems, our goal is to provide more capacity, where a better robustness characteristic is of concern in watermarking. The capacity requirements are often satisfied with techniques in spatial domain, where transform domain techniques provide higher robustness against changes and attacks. Accordingly, majority of non-fragile watermarking algorithms use transform domain techniques because of their critical need for robustness, while spatial domain hiding methods are more attractive in steganography schemes due to the capacity concerns.

Data hiding [1] and watermarking in digital images and raw video have wide literature. This paper targets the internal dynamics of video compression, specifically the motion estimation stage. We have chosen this stage because its contents are processed internally during the video encoding/ decoding which makes it hard to be detected by image steganalysis methods and is lossless coded, thus it is not prone to quantization distortions. In the literature, most work applied on data hiding in motion vectors relies on changing the motion vectors based on their attributes such as their magnitude, phase angle, etc. In [2] and [3], the data bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs). A single bit is hidden in the least significant bit of the larger component of each CMV. In [4], the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region. Using the variable macro-block sizes of H.264, the authors in [5] used every 2 bits from the message bit stream to select one of the four sizes for the motion estimation process.

The authors in [6] and [7] embed the data in video using the phase angle between two consecutive CMV. These CMV are selected based on the magnitude of the motion vectors as in [2]. The message bit stream is encoded as phase angle difference in sectors between CMV. The block matching is constrained to search within the selected sector for a magnitude to be larger than the predefined threshold. The methods in [2]–[7] focused on finding a direct reversible way to identify the CMV at the decoder and thus relied on the attributes of the motion vectors. In this paper, we take a different approach directed towards achieving a minimum distortion to the prediction error and the data size overhead. This approach is based on the associated prediction error and we are faced by the difficulty of dealing with the nonlinear quantization process.

## 2. System Design Model

We overview lossy video compression to define our notation and evaluation metrics. At the encoder, the intrapredicted (I)-frame is encoded using regular image compression techniques similar to JPEG but with different quantization table and step; hence the decoder can reconstruct it independently. The I-frame is used as a reference frame for encoding a group of forward motion-compensated prediction (P)- or bi-directionally predicted (B)-frames. In the commonly used Motion Picture Expert Group (MPEG-2) standard [8], the video is ordered into groups of pictures (GOPs) whose frames can be encoded in the sequence: [I,B,B,P,B,B,P,B,B]. The message should survive the video lossy compression and can be identically extracted from . This robustness constrain should have low distortion effect on the reconstructed video as well as low effect on the data size (bit rate). Given that can be identically extracted, in this paper, we use two metrics to evaluate data-hiding algorithms in compressed video which are below.

**Algorithm:** We segment the wavelet representation of the image into 8×8 blocks and determine the capacity of each block, in terms of bit per pixel, using the BPCS. A random seed is used to determine the order of conveying blocks. For each block, the red, green, and blue channels are used for the message bit embedding. The pseudorandom generator is initialized using a session key, agreed between transmitter and receiver. The embedding rule is so simple: the pixel value is changed into the nearest integer with the last LSB bits equal to the input bits. For example, assume that capacity of the current block is found to be 3 bits. Then, the current pixel is equal to 17 or (00010001)b and the input bits are equal to (100)b. According to the rule described above, the value of pixel is changed into 20 or (00010100)b. In the same case, with the input equal to (110)b, the turned value of the pixel is 14 or (00001110)b. And, in the case of input equal to (101)b, there is no preference for choosing 13 or 21, as the output value.

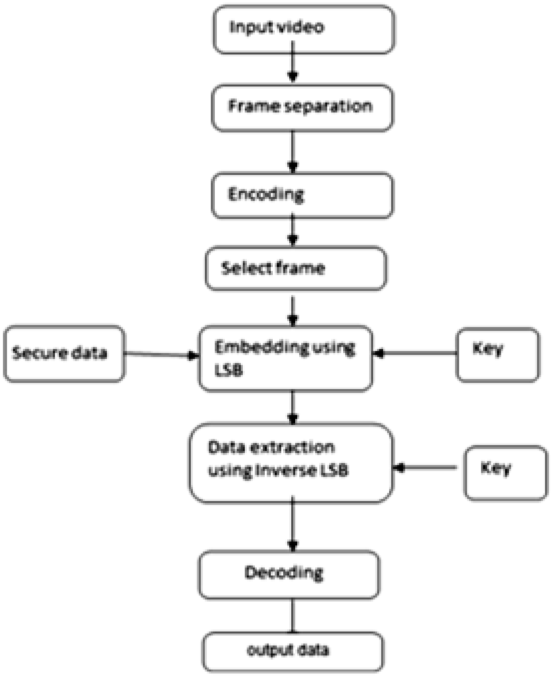


**Figure 1:** Proposed flow chart

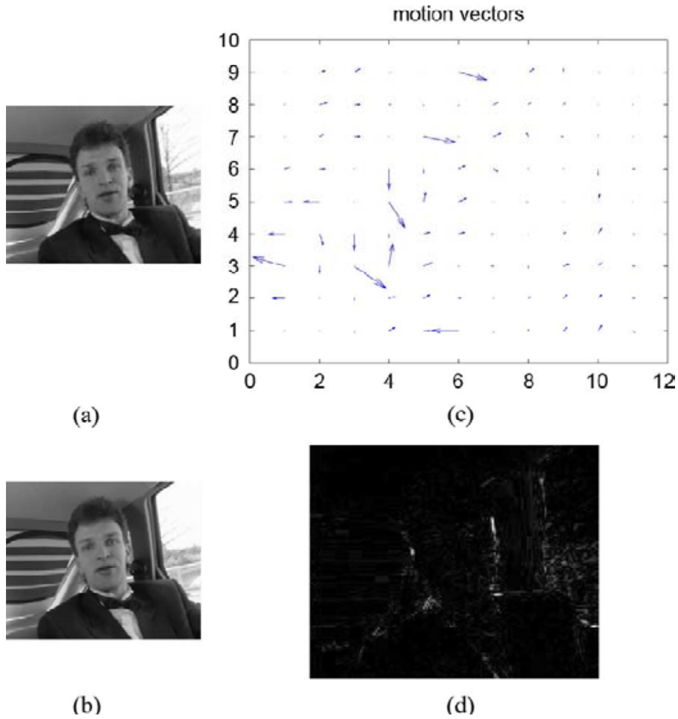


**Figure 2:** Sample from the Car-phone sequence. (a) Reference frame. (b) Predictive frame. (c) Motion vectors and (d) the associated prediction error frame.

**Embedding:** Compute the 2D wavelet transform of the image and segment it into 8×8 blocks. Use the secret key to determine the order of blocks selected for embedding. Find the maximum complexity of blocks of each channel and, hence, the appropriate complexity threshold for that channel. Determine the capacity of each block finding its first MSB plane possessing a complexity higher than the threshold. Embed the capacity of the block in its first pixel with $c=3$ and $m=capacity$. If the capacity is not equal to 1, embed the input bits of the block capacity in its remaining pixels. Otherwise, change the pixels such that to satisfy using the method. Generate the stego image by computing the inverse 2D wavelet transform.

**Extracting:** Compute the 2D wavelet transform of the image and segment it into 8×8 blocks. Use the secret key to determine the order of blocks selected for embedding. Extract the capacity of blocks using, with c equal to 3 from the first pixel of the block. Extract the message bits using, with $c$ equal to the capacity extracted in step3, if $c$ is not equal to one; otherwise, use for extraction.

We tested our algorithms on six standard test sequences: car-phone, foreman, coastguard, football, flower-garden, and mobile sequence which are all shown in Fig. 2. All the foreman, coastguard, flower-garden, and mobile sequence have a frame size of 352X288 which corresponds to 396 macro blocks per frame. The number of macro blocks per frame and the total number of frames for each sequence.

## 3. Simulation Results

We implemented the hiding and extraction Algorithm and integrated them to the MPEG-2 encoder and decoder operation. The parameters of our experiments, presented in this section, are: macro-block size , motion vector

ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

representation bits . We used both the fast three-steps and exhaustive search motion estimation algorithms with half pixel accuracy.


**Figure 3:** Input video for the system

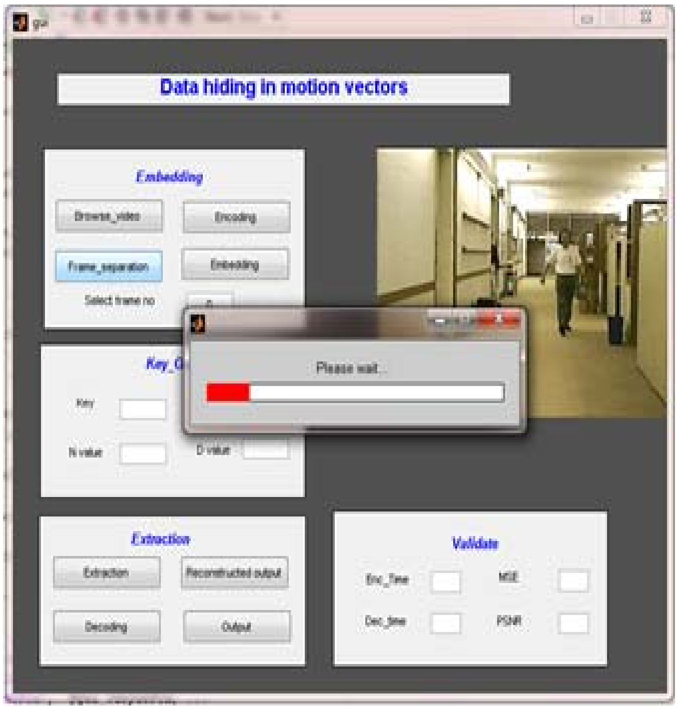


**Figure 4:** Frame separation from the video stream.

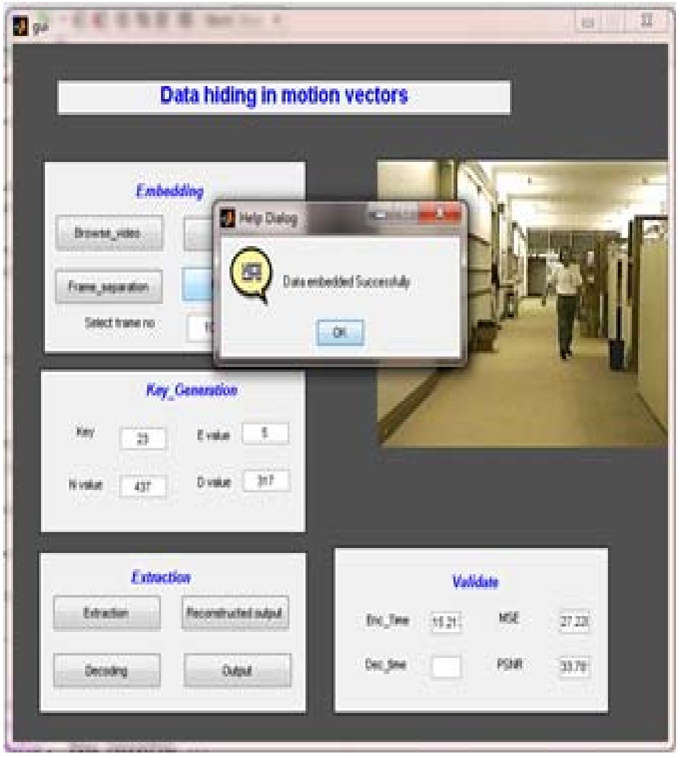


**Figure 5:** Data embedded in to the video stream with security sequence.

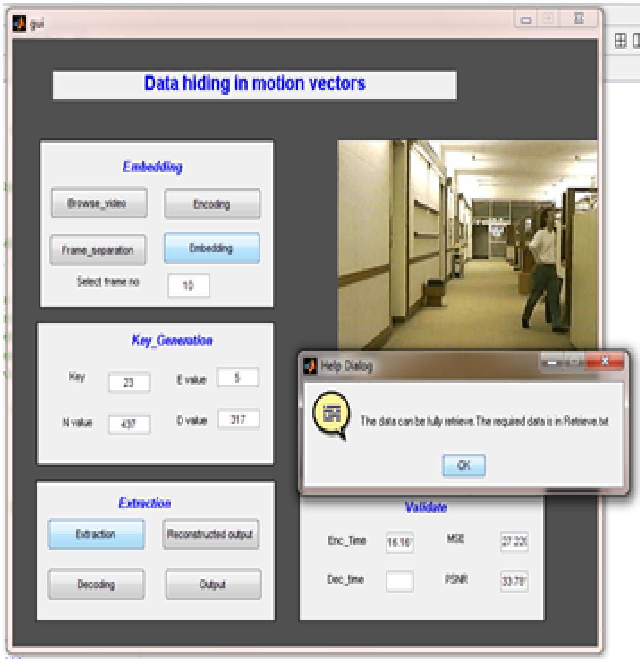


**Figure 6:** Final reconstructed video stream with hiding sequence.

## 4. Conclusion

We proposed a new data-hiding method in the motion vectors of MPEG-2 compressed video. Unlike most data-hiding methods in the motion vectors that rely their selection on attributes of the motion vectors, we chose a different approach that selects those motion vectors whose associated macroblocks prediction error is high (low PSNR) to be the candidates for hiding a bit in each of their horizontal and vertical components. The proposed method is found to have lower distortion to the quality of the video and lower data size increase. Future work will be directed towards increasing the size of the embedded payload while maintaining the robustness and low distortions.

## References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
[2] J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in Proc. XIV Symp. Computer Graphics and Image Processing, Oct. 2001, pp. 179–182.
[3] C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC'06), 2006, vol. II, pp. 803–806.
[4] P.Wang, Z. Zheng, and J. Ying, "A novel videowatermark technique in motion vectors," in Int. Conf. Audio, Language and Image Processing (ICALIP), Jul. 2008, pp. 1555–1559.
[5] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "Data hiding in H.264 encoded video sequences," in IEEE 9th Workshop on Multimedia Signal Processing (MMSP07), Oct. 2007, pp. 373–376.
[6] D.-Y. Fang and L.-W. Chang, "Data hiding for digital video with phase of motion vector," in Proc. Int. Symp. Circuits and Systems (ISCAS), 2006, pp. 1422–1425.
[7] X. He and Z. Luo, "A novel steganographic algorithm based on the motion vector phase," in Proc. Int. Conf. Comp. Sc. and Software Eng., 2008, pp. 822–825.
[8] Generic Coding of Moving Pictures and Associated Audio Information: Video, 2 Edition, SO/IEC13818-2, 2000.
[9] B. Chen and G. W. Wornell, "Quantization index modulation for digital watermarking and information embedding of multimedia," J. VLSI Signal Process., vol. 27, pp. 7–33, 2001.
[10] J. Choi, Y. Yoo, and J. Choi, "Adaptive shadow estimator for removing shadow of moving object," Comput. Vis. Image Understand., vol. 114, no. 9, pp. 1017–1029, 2010.

## Author Profile

**Y. Mahendhar** Pursuing M.Tech in Digital Systems And Computer Electronics Department of ECE in Jyothishmathi Institute of Technology & Science, Nustullapur, Karimnagar -District, A.P, India. B.Tech EEE from Vivekananda Institute of Technology and Science Bommakal, Karimnagar.

**B. Satish Chandra**, he received his B.Tech degree in Electronics & Communications Engineering from Nagarjuna University, Guntoor. He then received his M.Tech in Systems and Signal Processing from JNTU, Hyderabad. He started his career as an Assistant Professor in 1999 and currently he is working as an Associate Professor in Department of ECE at Jyothishmathi Institute of Technology and Science, Nustulapur, Karimnagar (A.P, India). B. Satish Chandra has guided several B.Tech Projects and M.Tech dissertations. He has published several research papers in National/International Journals/Conferences.