RESEARCH ARTICLE OPEN ACCESS

A Novel Algorithmic Approach for Information Hiding In a Video with Low Video Distortion

Praveen Kumar Reddy. M, D. Adithya Chandra Varma, Prof. Varunkumar.M
School of Computing Science Engineering, VIT University, Vellore - 632014, Tamil Nadu, India.
School of Information Technology & Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

Abstract
Data hiding in compressed video is the recent way of providing security. The main objective of data hiding in video is to transmit the message with security (by encryption) in streaming video. This paper presents a technique to hide secret data in the motion vectors of a compressed video which is not vulnerable to Stag analysis and also to maintain the quality and size of the reconstructed video. In this technique the secret message bit stream is embedded in the least significant bit of both components of the candidate motion vector. Also this paper uses a standard encryption mechanism (AES) in order to improve more security for the message. The proposed technique is found to have lower distortion to the quality of the video. “

Keywords: Data hiding, Motion vectors, steganography.

I. Introduction

“Data hiding and watermarking in digital images and raw video have wide scope in security related issues. The related work presents that 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 [1]. In the data bits method the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs) [2]. A single bit is hidden in the least significant bit of the larger component of each CMV. The limitation of this approach is, the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region. This paper is formatted as follows. In section 2, the related work of the paper is discussed. In section 3, the architecture of the proposed approach is discussed. Finally in section 4 conclusions of the proposed technique and future work are discussed.

II. Literature Survey

D.-Y. Fang *et al.* [3] and X. He *et al.* [4] proposed a technique to embed the data in video by 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 streams are 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. J. Zhang *et al.* [2] and X. He *et al.* [4] proposed a technique that mainly focused on finding a direct reversible way to identify the CMV at the decoder and thus relied on the attributes of the motion vectors. The problems associated with this data hiding approach are increase in data size and drop in reconstruction quality.

In this paper, we take a different approach directed towards achieving a minimum distortion to the quality and the data size overhead. This approach is based on the quantization algorithm for providing security by encryption and decryption.”

III. Proposed Approach Architecture

Thus we are proposing Advanced Encryption Standard (AES) encryption and decryption for security. AES is a specification for the encryption of electronic data. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level.

Our data-hiding algorithm is applied at the encoder side, uses the regular pair produced, tampers to become, and thus replaces them by the pair for each P and B-frame in the GOP as in Algorithm 1. The secret message is organized as a bit stream: message length. A subset of is selected to be the CMV. The selection of (line 6 of Algorithm 1) is performed if their associated macro block prediction error measured in PSNR is below an initial threshold value. The least significant bit (LSB) of both components, are replaced by bits of the message after data embedding.

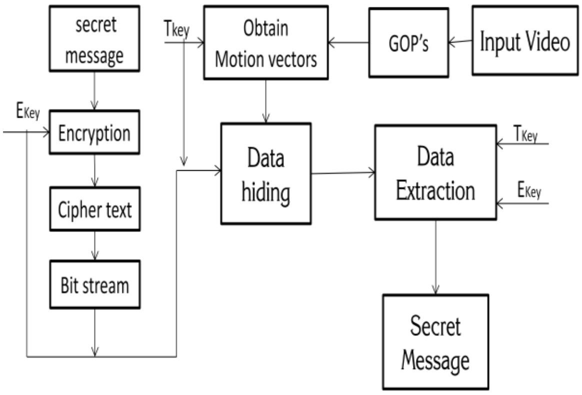

Fig 3.1 Data Hiding and Data Extraction in Compressed video using Quantization Algorithm

In this approach, the motion vectors are used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The proposed approach is divided into 3 phases.

3.1 Phase 1- Conversion of video into frames

In phase-1 the video input is given to the system initially for data hiding and then the input video is converted into the frames. In this phase the frames are only converted and it doesn't any features of the video.

Input video
System
GOP, Candidate motion vectors.

Fig 3.2 Input and output of phase 1

3.2 phase 2- Data Hiding in Group of Pictures

Data hiding in motion vectors at the encoder replaces the regular pair, due to tampering the motion vectors, where the superscript denotes hiding. We define data hiding in motion vectors of compressed video in the context of super-channel; the secret message is hidden in the host video signal to produce the composite signal. The composite signal is subject to video lossy compression to become. The message should survive the video lossy compression and can be identically extracted. This robustness constraint should have low distortion effect on the reconstructed video as well as low effect on the data size (bit rate). Here we use two metrics to evaluate data-hiding algorithms in compressed video which are:

1) Increase in data size
2) Drop in the reconstruction quality

The proposed data-hiding algorithm is applied at the encoder side, uses the regular pair produced, tampers to become, and thus replaces them by the pair for each P and B-frame in the GOP as in Algorithm 1.

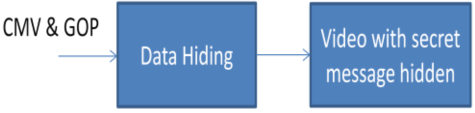

Fig 3.3 Input and Output of Phase 2

3.3 Phase 3- Data Extraction

The data extractor operates to extract the hidden message as a special decoder and our proposal is straightforward. After data extraction from the consecutive GOPs the hidden message is reconstructed back by concatenation of the extracted bit stream.

Video with secret message hidden
Data Extraction
Hidden secret message bit stream

Fig 3.4 Input and Output of Phase 3

3.4 Calculation of Motion Vector

If the reconstructed prediction error maintains the same criterion, then identify the data extractor for the given value. If any macro block associated with fails to maintain the criterion (line 5 of Algorithm 2), then will not be identified by the data extract or and the message will not be extracted correctly. Hence, we propose to use an adaptive threshold by iteratively decrementing by 1 decibel (dB) for this frame until either the criterion is satisfied for all macro blocks or the stopping value is reached for which we embed no data in this frame (line 19 in Algorithm 1). Since the threshold used for each frame is different, we hide their eight values for that GOP in the I-frame using any robust image data-hiding technique or sending them on a separate channel based on the application.

Algorithm 1

```
Input: $E^h$,$T_{key}$ ,$\bar{d}$
Output: Key found, $T_{key}$
Compress $E^h$ using JPEG compression to
produce $E^{-h}$
Decompress $E^{-h}$ to obtain lossy $E_T^h$
Set key found =true
While key found &(i,j)∈ $d_{i,j}(x)$ do
If 10 $log_{10}(b^2/\sum B_{i,j}\ E_t^h(x)) > T_{key}$ then
key found =false
decrement $T_{key}$
end
end
```

Algorithm 2

```
input:GOP($d^{th}$ ,$E^{\sim h}$),K
Output: message bit stream m
Extract the threshold $T_{key}$ for all frames in GOP form
I-frame or use them for other channel
For each frame P and B do
Decompress $E^{\sim h}$ to obtain $E^h$ and identify the
Candidate motion vectors:$d_{i,j(x)=\{d_{i,j}^h,x\}}$ :10 $log_{10}(b^2/$
$\sum B_{i,j}\ E_t^h(x)) \leq T_{key}$
For each (i,j) ∈ $d_{i,j}(x)$,do)
Extract two message bits m(k)=LSB $d_{i,j}^x$
```

```
m(k+1)=LSB($d_{i,j}^{x}$ )
K=k+2
If B-frame then
Extract from backward compensation
Motion vectors 2message bits m(k)= $d_{i,j}^{y}$
m(K+1=$d_{i,j}^{y}$)
k=k+2
end
end
end.
```

IV. Experimental Analyses

The experimental analysis describes the implementation of proposed approach and its comparison with existing approach. The proposed approach is implemented using Mat lab software.

Video Size In MB	PSNR ratio in Existing System(in dbs)	PSNR ratio in Proposed System(in dbs)
3MB	0.4	0.27
6MB	0.61	0.42
10MB	0.93	0.65

Table1: Comparison of PSNR ratio between existing system and Proposed System

Clearly from table 1 the PSNR (Peak Signal To Noise Ratio) from existing system Approach to the proposed system decreased.

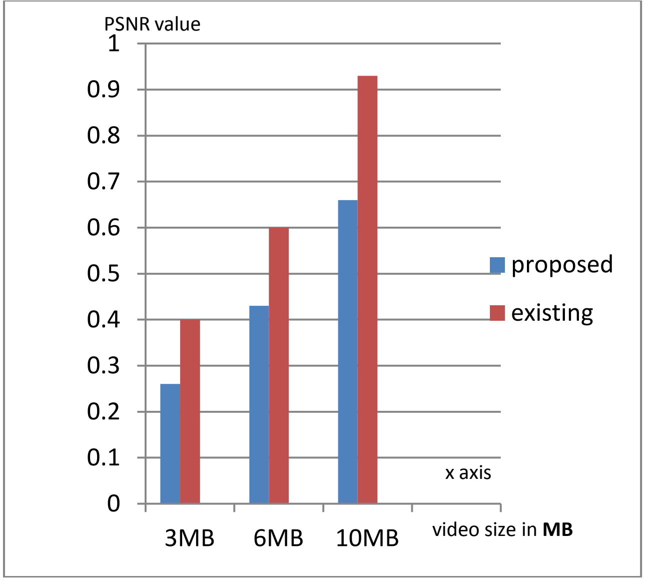

Figure 4.1 Comparison of PSNR ratio with varied size of video with existing and proposed system.

V. Conclusion and Future Work

The Quantization algorithm is a symmetric-key algorithm, which uses the same key for both encrypting and decrypting the data. 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 macro blocks prediction error is high (low PSNR) to be the candidates for hiding a bit in each of their horizontal and vertical components for achieving low distortion in quality and size. 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. In future work we can use any other encryption standards for more security else define any Steganography techniques."

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.2004.

[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] 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.

[4] 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.

[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] B. Chen and G. W. Wornell, "Quantization index modulation for digitalwatermarking and information embedding of multimedia," *J. VLSI Signal Process.*, vol. 27, pp. 7–33, 2001.