ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

An Efficient Steganographic Approach for H.264/AVC Compressed Videos

[1] Saurabh Anand, [2] Anand Singh Jalal
[1][2] Department of Computer Engineering & Applications, GLA University, Mathura, India

***Abstract* - Steganography is the art and science of communication which hides the presence of secret information. In this paper, a novel approach to hide the secret information in videos has been proposed for H.264/AVC compressed videos. H.264/AVC is known to be highly efficient and network friendly coding technique. In the proposed approach, we have utilized the F5 algorithm for preventing statistical attacks and improving embedding efficiency. Perceptual quality has been taken into consideration while using the Steganographic technique as well as after the compression by the H.264 method. Firstly, the videos are compressed and then the Steganographic method is applied. From the results, it is evident that F5 method gives the better PSNR values as far as perceptual quality is concerned.**

Keywords— Steganography, H.264/AVC, PSNR, Perceptual Quality, F5.

I. INTRODUCTION

Data hiding deals with the ability of embedding data into a digital cover with a minimum amount of perceivable degradation which makes the hidden data invisible to a human observer [1]. Due to all these facilities Steganography have thrilled the digital era. Many interesting Steganographic techniques have been created and its continuing evolution is guaranteed by a growing need for information security. There are several requirements in steganography, including the high payload of hidden information, imperceptible distortion, security and reliability [1]. To achieve the practical covert communication, digital video files can serve as good hosts, especially when these files are available to most of the people and their transmission is increasingly popular.

H.264/Advanced Video Coding (AVC) is the state-of-the-art video codec and its decent coding performance lends itself to become the major coding mechanism in various applications [2]. The most popular digital video formats/containers for file sharing nowadays, including FLV (Flash Video), MKV (Matroska Multimedia Container), AVI (Audio Video Interleave) and MP4, etc., support H.264/AVC so we choose the video files employing H.264/AVC as the "stego" host. First, a user may acquire a video file compressed by a popular video codec, such as MPEG2 or MPEG4, and will use this video content as the stego host. The stego video will then be transmitted to the trusted party and the hidden information should be extracted efficiently and reliably from the partially decoded bit-stream.

In [1] the author has proposed the modern research work in the area of Steganography technique deployed in transform, spatial, and compression domains of digital images. Transform domain techniques alters the frequency coefficients instead of manipulating directly the image pixels, thus keeping distortion at minimum level and that is what makes them preferred over spatial domain techniques. But in case of embedding capacity, spatial domain techniques have proved to give better results.

In [2] author has implemented Steganography in Multi Media Services (MMS) using image over mobile communication. It is secure because data which needs to be hidden is encrypted first and then embed in to message in both image and text as well [2].

In [3] the author has discussed Steganography and its types. They laid due emphasis on Line and Word Shift Coding, Feature Coding techniques as different methods of it. In [4] the author introduced a new Steganography technique to provide better protection to digital data content. They did a comparative study of the current literature in digital audio Steganography techniques and also discussed its strengths and weaknesses. In general, the temporal domain techniques, aim to maximize the hiding capacity, transform domain methods by exploiting the masking properties in order to make the noise generated by embedded data indiscernible. On the other hand, encoded domain methods endeavor to ensure the veracity of hidden data against challenging environment, such as the real time applications. To better approximate the sturdiness of the presented techniques, a classification based on their occurrence in the voice

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

encoder is given. They have also presented a comparison along with a performance evaluation for the reviewed techniques. They elucidate that the frequency domain is much preferred over the temporal domain.

In this paper, to achieve the Steganography while maintaining the perceptual quality of the original audio/visual data, we investigate combinations of embedding methods to satisfy most of the requirements or restrictions.

II. PROPOSED METHOD

H.264 compression standard is based on motion compensated and DCT like transform coding, where each picture are compressed by partitioning the image into one or more slices, and each slices consists of macroblocks and each macroblocks consists of blocks of 16*16 luma samples with corresponding chroma samples. Further each macroblocks are divided into sub-macroblocks partitions for motion prediction. Allowed sizes for prediction partitions are 16*16, 16*8, 8*16, 8*8, 8*4, 4*8 and 4*4. At this point, the H.264/AVC encoding process integrated with our video since the quantization, intra prediction and motion estimation procedures have modified [5]. To reduce the prediction residuals H.264/AVC employs the inter prediction which is to be further processed by the entropy coding [6].

In our proposed scheme, F5 processing scheme is used to process both intra and inter residuals in Luma and Chroma. The advantages of using F5 technique is that a careful steganalysis will not reveal the existence of hidden information. To achieve the higher degree of security in F5 algorithm, one may skip some quantized coefficients given that both the embedder and detector know the rule. This is eventually a trade-off between the security and payload of hidden information. In video coding the magnitude of resultant coefficients tends to become smaller, which is the result of using F5 technique. This means that if we will use a constant Quantization Parameter (QP) to encode a video, the size of the video gets reduced after the information embedding [7]. So will be able to save some bits in the current frame so that the following frames can be assigned with smaller QP values, and this frame may not only preserves the frame content better but will also generate more number of nonzero indices to raise the payload of hidden information.

H.264/AVC gives advantages of using four 16*16 or nine 4*4 intra prediction modes which can be applied on the luma while four 8*8 prediction modes for chroma. In the proposed approach, we only utilize the nine 4*4 intra prediction modes for information hiding [10].
Enough work has been done on text Steganography, image Steganography as well as on Video Steganography. Here, in this work, aim is to do video Steganography-using the concept of F5 algorithm which is considered better than the F4 algorithm.
The idea behind the Steganography algorithm is that a secret message is embedded into an image in order to alter the quantization step, the algorithm embeds more zeroes than ones, and this is detectable statistically. It is evident that, the histogram of the coefficients has got enough odd as compared to even coefficients. We can also embed text using text Steganography.

Algorithm 1: F4 Algorithm
Input:
Message bit = [0 1 1 1 0]
1: Get the RGB image and convert it to YCbCr.
2: Calculate the 8*8 DCT of input image
3: Quantize the DCT coefficient by a constant value
4: if quantized coefficient==0
Continue; % skips all zeros
else if Quantized coefficient<0 && message bit~=0
increase the value by 1
else if Quantized coefficient>0 && message bit~=0
decrease the value by 1
end
end
end

F4 Embeds secret message data continuously resulting in changes to concentrate on the start of the file, and unused rest resides on the end. This phenomenon is called Continuous embedding. For a very short secret message comprising of 217 byes (1736 bits), F4 changes 1157 places. This shows that the number of bits changed is significantly more which is not a good feature for attack proof Steganographic algorithm. A new mechanism is required to decrease the number of bit changes.

The F5 algorithm is almost same as F4 algorithm. The only difference is that F5 is an enhanced version of F4 algorithm with respect to 2 main features stated below which help in preventing statistical attacks and improving embedding efficiency: Permutative Straddling, Matrix Encoding

Permutative Straddling - To prevent the Continuous Embedding problem in which the changes concentrate on

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

the start of the file, and unused rest resides on the end. F5 algorithm uses a technique called Permutative Straddling for scattering the secret message over the whole carrier medium.

The straddling mechanism used in F5 shuffles all coefficients using a permutation first. Then, F5 embeds into the permuted sequence. The shrinkage does not change the number of coefficients (only their values) .The permutation depends on key derived from a password. F5 delivers the steganographically changed coefficients in its original sequence to the Huffman coder. With correct key, receiver will be able to repeat the permutation.

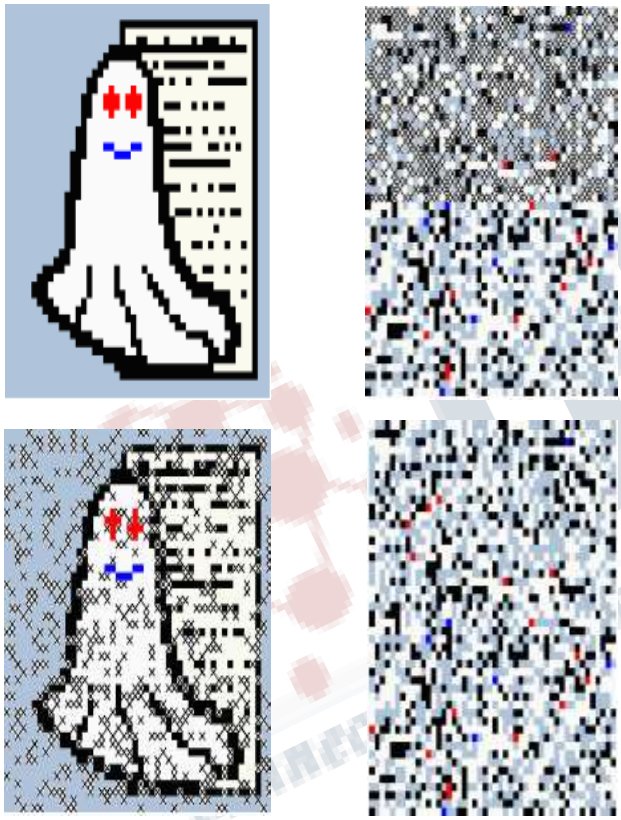

Fig 1: Permutative Straddling scatters the changes

Matrix Encoding - Suppose we want to embed 2 bits x1, x2 in three modifiable bit places a1, a2, a3 changing one place at most. We have following 4 cases:

$$x1 = a1 \oplus a3, x2 = a2 \oplus a3 \Rightarrow \textit{change nothing}$$
$$x1 \neq a1 \oplus a3, x2 = a2 \oplus a3 \Rightarrow \textit{change } a1$$
$$x1 = a1 \oplus a3, x2 \neq a2 \oplus a3 \Rightarrow \textit{chnage } a2$$
$$x1 \neq a1 \oplus a3, x2 \neq a2 \oplus a3 \Rightarrow \textit{chnage } a3$$

In all 4 cases, we do not change more than one bit. General case: If we have a code word 'a' with 'n' modifiable bit places for 'k' secret message bits 'x', Matrix encoding technique embeds 'k' secret message bits by changing one of n= 2^k-1 places.

F5 Implementation Steps:

- Start JPEG compression. Stop after the quantisation of coefficients.
- Initialise a cryptographically strong random number generator with the key derived from the password.
- Instantiate a permutation (two parameters: random generator and number of coefficients).
- Determine the parameter *k* from the capacity of the carrier medium, and the length of the secret message.
- Calculate the code word length *n = 2^k − 1.*
- Embed the secret message with (1, *n, k)* matrix encoding (Hash based embedding).
- Implement inverse permutation.
- Continue JPEG compression (Huffman coding etc.)

III. RESULTS AND ANALYSIS

To measure the performance for image distortion due to hiding of messages, we have used the well known peak-signal-to noise ratio (PSNR) which can be applied to stego images. PSNR is categorized under different distortion metrices. With help of PSNR (Peak-Signal-To-Noise Ratio) we can make the comparison between the qualities of stego images compared to cover images. PSNR is defined as;

where Imax = 255, maximum gray level for any grayscale image. The Mean Squared Error MSE is defined as

$$PSNR = 10 \times \log_{10}\left(\frac{I_{\max}^2}{MSE}\right)(dB)$$

where M and N represent the number of pixels of the payload in horizontal and vertical directions respectively.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(|\, C(i,j) - S(i,j)\,|)^2$$

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

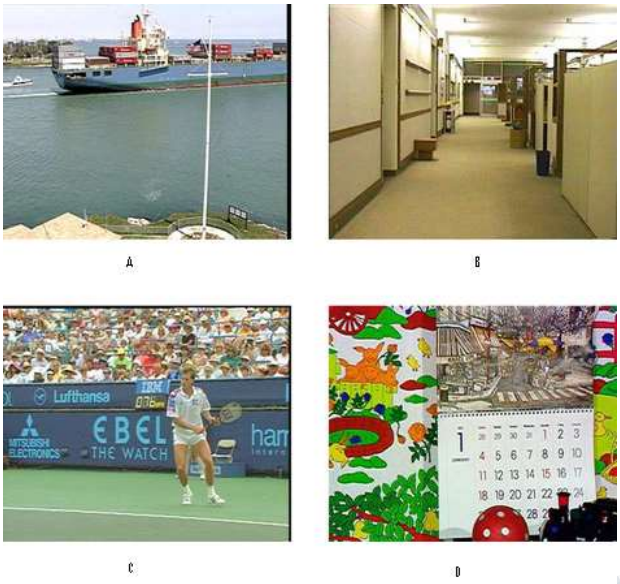

Fig 2: The four test videos: a Container, b Hall monitor, c Stefan and d Mobile

ORIGINAL PSNR	F4 PSNR	F5 PSNR
36.2158	35.0042	34.5966
36.1363	34.9361	34.5213
34.0203	33.2502	32.9594
31.7442	31.231	31.0852
29.8245	39.5151	29.3896

Table 1: Results of container video

ORIGINAL PSNR	F4 PSNR	F5 PSNR
37.2715	35.7673	36.8177
37.1141	35.3631	36.7418
33.3641	32.5266	33.2084
32.8451	32.1184	32.7039
33.4549	32.7333	33.2957

Table 2: Results of hall monitor video

ORIGINAL PSNR	F4 PSNR	F5 PSNR
34.4311	33.5897	34.3271
34.5802	33.7196	34.3666
14.6346	14.6249	14.6326
13.7481	13.7403	13.7465
13.0441	13.0380	13.0437

Table 3: Results of Stefan video

ORIGINAL PSNR	F4 PSNR	F5 PSNR
34.1982	33.4012	33.4017
34.2302	33.4146	33.5151
20.6977	20.6511	20.6636
16.4378	16.4154	16.4250
14.7404	14.7306	14.7317

Table 4: Results of Mobile video

IV. CONCLUSION

In this work, it is possible to pass the information from source to destination in such a manner that the perceptual quality does not get affected. In this work, the advantages of H.264/AVC technique have been taken for compressing the frames of the videos in which the secret data is to be embedded. F5 algorithm is used for hiding the information. The proposed data hiding algorithm i.e. F5, is better than the earlier used methods as evident from the PSNR calculation.

REFERENCES

[1] B. Saha and S. Sharma, "Steganographic Techniques of Data Hiding Using Digital Images", Defence Science Journal, vol. 62, pp. 11-18, 2012.

[2] S. Mohanapriya, "Design and implementation of steganography along with secured message services in mobile phones," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250-2459, 2012.

[3] M. Hariri, R. Karimi and M. Nosrati, "An introduction to steganography methods," World Applied Programming, vol. 1, no. 3, pp. 191-195, 2011.

[4] F. Djebbar, B. Ayad, K.A. Meraim and H. Hamam, "Comparative study of digital audio steganography techniques," EURASIP Journal on Audio, Speech, and Music Processing, vol. 2012, pp. 1-16, 2012.

[5] H. Zhu, R. Wang, D. Xu and X. Zhou, "Information Hiding Algorithm for H. 264 Based on the predition difference of Intra_4× 4," in Image and Signal Processing (CISP), 2010 3rd International Congress on, pp. 487-490, 2010.

[6] 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, 2007., pp. 373-376, 2007.

[7] P. Su, M. Lu and C. Wu, "A practical design of high-volume steganography in digital video files," Multimedia Tools and Application, vol. 66, pp. 247-266, 2013.