Secured Reversible Data Transmission by Using Gzip Deflector Algorithm for Encoded AVC Video

[1,]Gokiladeepa.G, [2,]Gayathri.S, [2,]Heeba.S.D, [2,]Pavithra.R
[1]Assistant Professor, Department Of Information Technology, SNS College of Engineering, TamilNadu, India
[2]UG Scholar, Dept. of Information Technology, SNS College of Engineering ,TamilNadu, India

Abstract

Reversible data transmission, visible watermarking and steganography schemes that can be employed along with multimedia applications. However, these methods are susceptible to quantization errors provided by standard image/video compression standards. In this work we present a secured data transmission using novel reversible visible watermarking scheme for H.264/AVC encoded video sequences. The proposed approach reversibly embeds the residual information that will then be used by the decoder to recover the original image or video frame. The residual information is losslessly compressed using the Gzip Deflector algorithm to minimize the information to be embedded and reduce the distortion provided by RCM. The compressed information is then encrypted using the 128–bit Advanced Encryption Standard (AES). Furthermore we add security in this work if the key does not match we provide irrelevant information or unwanted data's to the decoder. And finally we compared our proposed work with existing state of art.

Index Terms – Information embedding, data compression, lossless recovery, reversible watermarking scheme, DCT, AES, GZip Deflector algorithm.

1. INTRODUCTION

The recent growth of computer networks and multimedia systems has contributed to the proliferation of multimedia con-tent. However, the availability of multimedia editing software has raised the issue of increased distortion level[1]unauthorized manipulation of proprietary material. Visible watermarking techniques have been extensively used to protect copyrighted material. However, traditional approaches, such as [2] are not able to recover the original image/video quality after watermarking extraction.The methods proposed for removable visible watermarking schemes where authenticated users are allowed to approximate the visible watermark. Nonetheless, these methods only manage to recover an approximate version of the original image after watermark extraction [12] and are therefore unsuitable for military, law and medical applications.There are several reversible visible watermarking schemes that can be employed for many applications [3]. However, these methods are susceptible to quantization errors provided by standard image/video compression standards. Therefore, these methods are not suitable for most Internet applications where multimedia content needs to be compressed prior transmission. In previous work, the same author has presented a reversible watermarking scheme for JPEG image compression . However, this method cannot be directly integrated within current video compression standards, mainly due to the spatio-temporal prediction mechanisms being employed by video standards.

This paper presents secured data transmission by an adaptation of the reversible visible watermarking scheme presented, for H.264/AVC video coding. The proposed method computes the residual error caused by the embedded watermark which is losslessly compressed using the GZip Deflector algorithm and then encrypted using the Advanced Encryption Standard (AES). The resulting information is embedded within the trans-form coefficients of every macroblock (MB) pair using the Reversible Contrast Mapping (RCM).The simulation results clearly show that the proposed mechanism outperforms the state of the art approach where Peak Signal-to-Noise Ratio (PSNR) gains of up to 7 dB were registered. The structure of this paper is as follows. Section II provides a detailed description of each component involved in the Reversible Visible Watermarking Embedding process while the Reversible Visible Watermark Extraction process is described in section III. Section IV presents the testing environment and presents the simulation results. The final comments and conclusion are delivered in section V.

2. Information Embedding

A High level description of the proposed Reversible Visible Watermark Embedding process for video content is illustrated in Fig.1. The original frame I is first fed to the information Embedding process which inserts a visible watermark within its Region of Interest (ROI) to generate the frame I_W. Given that the embedded watermark directly affects the image content, it makes this process irreversible.The resulting watermarked frame I_W is then compressed using the Video Encoder 1 process which employs motion estimation

and spatial prediction of the standard H.264/AVC encoder [4] to minimize the residual error E_{WC} to be entropy coded. The motion vectors and modes selected for each Macro block (MB) are registered in the Control Information module. This information is then used by the video encoder to compress the original image I which outputs the residual error E_C. This process computes neither motion estimation nor mode decision, but relies solely on the information contained within the Control Information module, thus significantly reduce the complexity of the system.

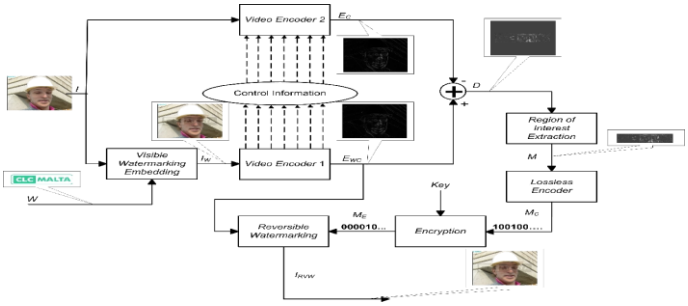

Fig.1 Schematic diagram of Information Embedding process.

The difference between the residual errors of the compressed watermarked image E_{WC} [5]and the compressed image EC provides the discrepancy image D. This image contains 0 values outside the ROI, while having low magnitude values within the ROI. Therefore, in order to minimize the information to be embedded within the image, only the message M encompassing the Region of Interest within D is losslessly encoded and encrypted. The encrypted message M_E is then embedded within the watermarked image I_W using a re-visible watermarking approach. More information about each individual module is provided in the following sub-sections.

2.1 Data Embedding

The Visible Watermarking Embedding process is used to perceptibly insert a watermark W into a primary image I so that the watermark is visible by the human eye. The purpose of these watermarks is to be noticeable without significantly reducing the quality of the image. The method adopted in this work considers the human vision system (HVS model) and the image content to insert the watermark without significantly degrading the perceptual quality of the image/video content. This process dissects the host image I into non-overlapping 8× 8 blocks. The watermark pattern W is then adaptively embedded into the host image using

$$I_n^W(i,j) = \begin{cases} [\alpha_n I_n(i,j)], & \text{if } W(i,j)=1 \\ I_n(i,j), & \text{otherwise} \end{cases} \quad (1)$$

where [ ] represents the floor function, I_n^W and I_n denote the n^{th} 8×8 block of the watermarked image I_W and the host image I respectively, i and j are spatial coordinates within the block and $_n$ is the n^{th} adaptive scaling coefficient. The scaling coefficients $_n$ are dependent on both the human perception and image content and determine the visibility of the watermark pattern. More information about the derivation of these scaling coefficients can be found in [8] and [12].

2.2 Video Encoder and DCT

The Video Encoder process employs the standard H.264/AVC encoder [6] to compress the supplied video content.This process employs spatial prediction and motion estimation to minimize the residual error to be encoded. The encoder derives the residual information to be encoded by subtracting the predicted frame from the original frame. The resulting residual information is de-correlated using the discrete cosine transform (DCT) transformation [10][9] and quantized to keep the least amount of information while still achieving an acceptable level of image quality. The quantized transform coefficients are then inverse quantized and inverse transformed to recover the residual error E which also includes the quantization error introduced by the lossy nature of the standard video codec.

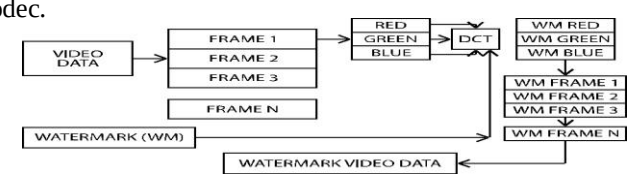

Fig. 2. DCT Based Watermark Technique.

The proposed method employs two Video Encoder pro-cesses. The Video Encoder 1 process receives the watermarked frame I_W and computes motion estimation and spatial pre-diction to compress the video. The resulting modes selected and motion vectors are then stored in the Control Information module while the resulting residual error E_{WC} is outputted. On the other hand, the Video Encoder to process receives the original video stream I and compresses it using the motion vectors and mode selected available in the Control Information module. This is done to ensure synchronization between the two processes and to minimize the computational complexity of the proposed system.

2.3 Data Compression and Encryption

The discrepancy message D is derived by subtracting the residual E_C from the residual E_{WC}. As it can be seen from Fig. 1, the non-zero coefficients reside only within the Region of Interest. Therefore, in order to minimize the data to be embedded, the Region of Interest is extracted from the discrepancy message D to generate the message M and this information is then passed through the Lossless Encoder process.The Lossless Encoder process adopts a simple encoding strategy, where each pixel in M is represented by a 10–bit codeword. The Most Significant Bit (MSB) is used to flag whether the pixel is a watermark (1) or not (0). The second MSB represents the polarity of the coefficient where negative coefficients are marked by a 1. The remaining 8–bits represent the magnitude of the coefficients of the residual error message M. Given that the decoder needs some extra information to be able to decode the encoded message (e.g. watermark dimensions and coordinates of the ROI), this information is concatenated to M prior to lossless encoding. The resulting 10–bit code words are then compressed using the public do-main lossless Gzip Deflector algorithm [14].

2.4 AES (Advanced Encryption Standard*)*

To enhance the security, a 128–bit Advanced Encryption Standard (AES) [13] is used to encrypt the information to be embedded so that only authenticated users can recover the original image.The AES algorithm is a symmetric key algorithm which means the same key is used to both encrypt and decrypt a message. Also, the cipher text produced by the AES algorithm is the same size as the plain text message. Most of the operations in the AES algorithm take place on bytes of data or on words of data 4 bytes long, which are represented in the field GF(28), called the Galois Field. AES is based on a design principle known as a Substitution permutation network. AES operates on a 4×4 matrix of bytes, termed the state. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. The AES algorithm loops through certain sections Nr times. It is fast in both software and hardware.AES Algorithm have following steps

1) Key Expansion—Round keys are derived from the cipher key using Rijndael's key schedule.

2) Initial Round
   a) *Add Round Key*—each byte of the state is combined with the round key using bitwise XOR.

3) Rounds
   a) *Sub Bytes*—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   b)*Shift Rows*—A transposition step where each row of the state is shifted cyclically a certain number of steps.
   c) *Mix Columns*—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   d) *Add Round Key*

4) Final Round (no Mix Columns)
   a) Sub Bytes
   b) Shift Rows
   c) Add Round Key

Advantages of using AES algorithm*:*
1) Very Secure.
2) Reasonable Cost.
3) Main Characteristics
   i) Flexibility, ii) Simplicity

2.5 Reversible Contrast Mapping (RCM)

The Reversible Watermarking process adopts the Reversible Contrast Mapping (RCM) mechanism presented in [15] to embed the encrypted information M_E within the watermarked image I_W . The RCM algorithm was used since it is reported to provide high-capacity data embedding without the requirement of the transmission of any additional side information.The RCM algorithm considers x and y to be a pair of coefficients whose values [11] reside in the range [0; L]. The forward RCM algorithm transforms the pixel pairs according to

$$x = 2x - y; \quad y = 2y - x \qquad (2)$$

In order to prevent overflow and underflow, the transformed pixel pairs are restricted within the range

$$0 \leq x \leq L,\ 0 \leq y \leq L \qquad (3)$$

The original coefficients can be recovered using the following inverse transformation

$$x = [(2/3)\ x + (1/3)\ y],\ Y = [(1/3)\ x + (2/3)\ y)] \qquad (4)$$

Where [ ] is the ceil function.

The RCM method substitutes the Least Significant Bit (LSB) of x and y. The LSB of x is set to 1 to indicate a transformed pair while 0 otherwise. The information bit b is then embedded within the LSB of y. More information about this method can be found in [15].The method proposed in [8], which is considered as the state of the art method, applies the RCM algorithm in the spatial domain. However, the RCM method cannot be applied in the spatial domain when considering compressed images since the embedded information will be distorted by the Quantization process of the image/video codec. It was further shown that the RCM method can modify the transformed coefficients prior entropy coding, thus mak-ing recovery of the original transform coefficients possible. However, the transform coefficients provide different levels of distortions, and therefore it is more desirable to embed the information within high frequency coefficients which provide the least distortion to the human vision system.

Therefore, considering a P Q image, the Reversible Watermarking scans the blocks column-wise and grabs the first two neighbouring 4 4 transformed blocks. It embeds the first bit within the coordinate (3,3) which corresponds to the highest frequency coefficient. The remaining $^{P}_{32}{}^{Q}$ 1 bits are then stored within the coefficient with coordinates (3,3) of the remaining neighbour blocks. Once all the blocks have been used this process goes back to the first two neighbouring blocks and embeds the second $^{P}_{32}{}^{Q}$ bits within the coefficient coordinate (3,2). This process proceeds until either the whole bit stream is embedded or else when all the transform coefficients are used. It is important to notice that the RCM algorithm can be used to embed information more than once within the same coefficients. However, this will contribute to major distortions within the image. Therefore, the transform coefficients were only used once for embedding. The Reversible Watermarking process then outputs the image $I_{RV\,C}$ which is then entropy encoded and transmitted.

3. Information Extraction

The Information Extraction process in-verts the computations performed by the Reversible Visible Watermark Embedding process. It receives the entropy coded information and decodes it to recover the image $I_{RV\,W}$ .The Reversible Data Extraction process then computes the inverse RCM function[13] to extract the encrypted message M_E and the visible watermarked residual E_W . The message M_E is then decrypted and decoded to derive the message M. The message M contains the residual watermark within a Region of Interest together with additional information suitable to reconstruct the discrepancy image D. The im-ages D and E_{WC} are then summed to generate E_C. The Video Decoder then is able to recover the original compressed video sequence I_C.

4. Simulation Result

The proposed Reversible Visible Watermarking Scheme was implemented using the C++ programming language. The raw video sequences considered in these simulation results were encoded using a Common Intermediate Format (CIF) resolution at 30fps with a format IPPP using the Baseline Profile of H.264/AVC. The video was encoded using only the 4 4 transform size. The Quantization Parameter is set to a default of 20 unless otherwise specified. The logos employed in these experiments included some of the logos.

TABLE I

Performance Analysis of the Proposed Reversible Visible Watermarking Embedding Process

TABLE I

Performance Analysis of the Proposed Reversible Visible Watermarking Embedding Process

Logo	**Width**	**Height**	M_E **Size (Bytes)**	**Comp. Ratio**	I_W **PSNR (dB)**
ATLSS	163	216	14408	2.4436	26.2887
DARPA	130	263	16461	2.0770	26.9543
Censcir	82	225	8747	2.1093	30.1921
Robotics	130	108	5623	2.4969	31.4413
CIT	82	225	8472	2.1778	31.7764
HCII	65	65	2253	1.8753	37.4408

Table I illustrates the performance of the proposed Re-versible Visible Watermarking Embedding mechanism. It can be clearly seen that the compression efficiency provided by the Lossless Encoder process is between 1.8 and 2.5. This compression efficiency is almost constant and thus not affected by the logo size. It can be further noticed that the larger the size of the logo to be embedded the lower is the quality of the Watermarked Video I_W . This is quite intuitive since larger logos need to modify more DCT coefficients thus inevitably reducing the perceptual quality of the Watermarked Video.The proposed system was compared to the Yang method which was adapted for compressed video. As it can be seen from Fig. 2, the quality of the proposed method is superior to the method adopted in [8]. In fact, it can be seen that no matter how much information is reversible embedded the proposed system manages to recover the original quality for authenticated users. This is mainly due to the fact that the information is being embedded on the compressed transform coefficients. On the other hand, the performance of the state of the art approach degrades with increasing embedding information since the information is hidden within the spatial domain which is corrupted by the Quantization process.

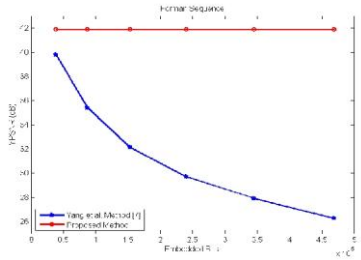

Fig. 3. Performance of the Yang method [8] and the proposed method at different number of embedded bits

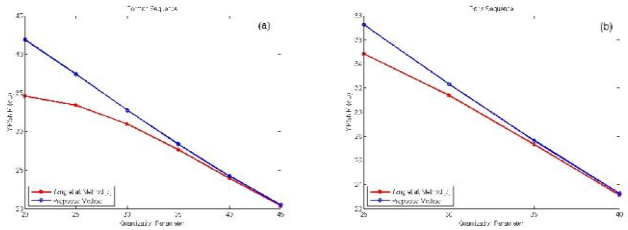

Fig. 4. Performance of the Yang [8] and the proposed method at different Quantization Parameters (a) Foreman

(b) Paris Sequence

Fig. 5. Subjective results when using the (a) method proposed by Yang [8] and the (b) Proposed method. QP was set to 30.

The performance of the proposed scheme was further analysed using different Quantization Parameters. As

shown in Fig. 3, the proposed system clearly outperforms the method presented in [7] where PSNR gains of up to 7 dB were achieved. The superiority of the proposed method is more evident in Fig. 4 where it can be seen that the method proposed by Yang does not manage to extract the reversible information since it was corrupted by quantization errors induced by the lossy Video Encoder process. The quantization errors generally provide syntax and semantic violations in the De-Encryption and Lossless Decoding processes which are thus not able to recover the original embedded information. On the other hand the proposed method manages to recover the original compressed video when the user is authenticated.

5. Comments And Conclusion

This paper has presented a secured data Transmission with Advanced Encryption Standard (AES) using novel reversible visible water-marking scheme for H.264/AVC encoded video. The proposed method computes the information required by the decoder to recover the original compressed video when receiving the watermarked video sequence. The additional information is reversibly embedded within the transform coefficients of the watermarked video. The authenticated users are then enabled to extract the information hidden within the transform coefficients to recover the original compressed image.The experimental results have shown the superiority of the proposed system where PSNR gains of up to 7 dB was registered relative to the state of the art approach. It was further shown that the information to be hidden can be compressed with compression efficiency between 1.8 and 2.5.And the distortion provided by the RCM method is reduced. Furthermore, watermark estimation functions can be employed in order to reduce the energy within the message D to be decoded.

References

[1] Reuben A.Farrugia "Reversible Visibe Watermarking for H.264/AVC Encoded Video" IEEE Conference,May 2011

[2] A.Watson,"Visually Optimal DCT Quantization Matrices for Individual Images", in Data Compression Conference, 1993. DCC '93., 1993, pp. –187.

[3] S.-K. Yip, O. Au, C.-W. Ho, and H.-M. Wong, "Lossless Visible Water-Marking" , in Multimedia and Expo, 2006 IEEE International Conference on, 9-12 2006, pp. 853 –856

[4] Xiao Zeng, Zhen-YongChen, MingChen and Zhang Xiong," Reversible Video Watermarking Using Motion Estimation and Prediction Error Expansion,"journal of information science and engineering 27,465-479(2011)

[5] R. A. Farrugia, "A Reversible Visible Watermarking Scheme for Com-pressed Images", ", in MELECON 2010 - 2010 15th IEEE Mediterranean Electrotechnical Conference, , 26-28 2010, pp. 212 –217

[6] T. Wiegand, G. Sullivan, G. Bjontegaard, and A. Luthra, "Overview of the H.264/AVC Video Coding Standard," IEEE Transactions on, Vol. 13, no. 7, pp. 560 –576, July 2003

[7] S.P.Mohanty ,K.R.Ramakrishnan, and M.S. Kankanhalli,"A DCT Domain Visible Watermarking Technique for Images," in Multimedia andExpo, 2000, IEEE International Conference on, NewYork, USA, pp. 1029–1032

[8] D. Coltuc and J.-M. Chassery, "Very Fast Watermarking by Reversible Contrast Mapping," Signal Processing Letters, IEEE, Vol. 14, no. 4, pp.255-258,April 2007

[9] A. Watson, "Visually Optimal DCT Quantization Matrices for Individual Images", ," in Data Compression Conference, 1993. DCC '93, 1993, pp. 178–187

[10] Y.Yang, X. Sun, H. Yang, and C.-T. Li, , "Removable Visible Image Watermarking Algorithm in the Discrete Cosine Transform Domain," Expo, 2000. ICME 2000. 2000 IEEE International Conference on, New York, NY , USA, pp. 1029–1032

[11] A. Alattar, "Reversible of a Generalized Integer Transform ," Image Processing, IEEE Transactions on, Vol. 13,no.8,pp. 1147-1156,Aug.2004

[12] Y. Hu and B. Jeon, "Reversible Visible Watermarking and Lossless Recovery of Visible Watermarking and Original Images,"Circuits and Systems for Video Technology IEEE Transactions on,Vol.16,no.11,pp.1423-1429,Nov.2006

[13] Advanced Encryption Standard (AES), FIPS PUB Std.197,2001

[14] (2010)Thezlibwebsite.[Online].Available http://www.zlib.net/

[15] B.-B. Huang and S.-X. Tang, "A Contrast-Sensitive Visible Water- MarkingScheme,"IEEE MultiMedia,vol.13,no.2 pp. 60– 66, 2006.