A Novel Reversible Robust Steganography Method Based on H.264/AVC (Postprint)

Authors: Liu Shuyang, Chen Liang

Date: 2018-05-02T00:00:00+00:00

Abstract

A novel reversible robust video steganography method based on H.264/AVC is proposed. The method first employs (t, n) threshold secret sharing technology to distribute the secret information to be embedded via polynomial distribution to obtain sub-secrets, then encodes the sub-secrets using BCH codes, selects embedding locations through H.264 prediction modes, and finally embeds the encoded sub-secrets into various frames of the video. During extraction, t encoded sub-secrets from the video are utilized to recover the secret information. Experimental results demonstrate that the method can completely recover the original video during secret information extraction, exhibits strong robustness against bit errors and frame errors, can fully recover the secret information when the random frame loss rate is less than or equal to 15%, effectively controls intra-frame distortion drift, and achieves favorable visual quality.

Full Text

Preamble

Title: A New Reversible Robust Steganography Method Based on H.264/AVC

Authors: Liu Shuyang[1], Chen Liang[2]
[1]Lanzhou University, Lanzhou 730000, China
[2]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China

Abstract: This paper proposes a new reversible robust video steganography method based on H.264/AVC. The method first employs a (t, n) threshold secret sharing technique to distribute the secret information to be embedded, obtaining sub-secrets through polynomial distribution. It then encodes these sub-secrets using BCH codes and selects embedding locations through H.264 prediction modes. Finally, the encoded sub-secrets are embedded into various

frames of the video. During extraction, the secret information is recovered using t encoded sub-secrets from the video frames.

Experimental results demonstrate that this method can completely restore the original video when extracting secret information, exhibits strong robustness against bit errors and frame errors, and can fully recover secret information when the random frame loss rate is less than or equal to 15%. The method effectively controls intra-frame distortion drift and achieves good visual quality.

Keywords: H.264/AVC; reversible steganography; robustness; intra-frame distortion drift

CLC Number: TP309.2
DOI: 10.3969/j.issn.1001-3695.2017.11.0999

Abstract (English): This paper proposes a new reversible robust steganography method for H.264/AVC. The method first distributes the secret data to be embedded using a specific polynomial to obtain a series of sub-secrets. It then uses BCH codes to encode each group of sub-secrets and embeds the encoded sub-secrets into each video frame using prediction modes. The hidden data is recovered using t encoded sub-secrets from the video frames. Experimental results show that the method can completely recover the original video and exhibits high robustness against bit errors and frame errors. When the random frame loss rate is less than or equal to 15%, the method can completely recover the secret data. Additionally, the method can avoid intra-frame distortion drift and provides better visual concealment.

Keywords (English): H.264/AVC; reversible steganography; robustness; intra-frame distortion drift

0 Introduction

Video steganography is a technique that hides secret information within video content, making it imperceptible to unauthorized parties. The H.264/AVC video compression standard has become the most popular video compression standard due to its high compression ratio, strong error recovery capability, and wide applicability, and has been rapidly deployed across various domains [1]. When H.264 videos containing hidden secret information are transmitted over networks, they may suffer from bit errors, frame loss, and packet loss due to harsh physical environments (unintentional attacks) and network attacks (intentional attacks), resulting in video corruption and inability to recover the secret information.

Research on H.264 video steganography began in 2005, with most studies selecting the transform domain and heavily relying on DCT coefficients [2-6]. However, research on robust video steganography algorithms remains scarce [7]. Esen et al. [8] achieved robust video steganography using forbidden zone data

hiding and selective embedding, while Liu et al. [4-6] utilized BCH codes for H.264 videos to recover from bit errors. Nevertheless, these algorithms cannot recover secret information under frame loss or packet loss scenarios.

Typically, the embedding and extraction processes of secret information modify the original carrier to a certain extent, which is unacceptable for applications such as medical imaging, legal evidence, and other domains that do not tolerate permanent distortion. Reversible steganography can address this issue. Generally, steganographic methods that can completely restore the original carrier after secret information extraction are called reversible steganography. Currently, research on reversible steganography primarily focuses on reversibility [10], and studies on reversible steganography algorithms for H.264 video are still limited [12].

References [10, 11] utilize prediction mode selection to choose embedding blocks for information hiding. Reference [10] only considers algorithm reversibility, while reference [11] builds upon [10] to solve bit error problems and improve robustness, but cannot address frame errors and frame loss caused by packet loss. Reference [12] employs secret sharing to achieve robustness, but the algorithm cannot resolve bit error and loss issues. Reference [13] implements reversible video steganography for 3D H.264/AVC using histogram modification.

This paper proposes a novel reversible robust video steganography method for H.264 video. The method can completely restore the original video during information extraction while simultaneously recovering from bit loss, bit errors, frame loss, and frame errors caused by harsh physical environments and network attacks. It also effectively controls intra-frame distortion drift and achieves good visual quality.

1.1 Intra-frame Distortion Drift Prevention

In the H.264 video compression standard, 4×4 blocks have 9 intra prediction modes (0–8) and 16×16 blocks have 4 intra prediction modes (0–3). During intra prediction, the prediction block is calculated based on previously encoded blocks and the current block to be encoded. As shown in Figure 1 [Figure 1: see original paper], assuming the current block is B_i,j, its predicted value is calculated from the gray portions of its encoded left neighbor block B_i,j-1, upper-left neighbor block B_i-1,j-1, upper neighbor block B_i-1,j, and upper-right neighbor block B_i-1,j+1, according to the intra prediction mode adopted by the current block. If secret information is embedded in the gray portions shown in the figure, the embedding-induced errors will inevitably propagate to the current block through the aforementioned calculation, causing intra-frame distortion drift. If the edge pixels of neighboring blocks containing embedded secret information are not used for predicting the current block, intra-frame distortion drift can be prevented.

1.2 BCH Codes

BCH codes are a class of cyclic error-correcting codes. For a BCH(n, k, t) code, where n is the code length, k is the number of information bits, and t is the error-correcting capability, the code can correct up to t errors. The parity-check matrix of a BCH(n, k, t) code is constructed using primitive elements in GF(2^m).

1.3 Secret Sharing

Secret sharing is a technique for distributing a secret among participants, where only a certain number of participants can reconstruct the secret. In 1979, Shamir [9] proposed a threshold secret sharing method based on Lagrange interpolation. Assume the secret information to be divided is S. Construct a t-1 degree polynomial:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \pmod{p}$$

where $a_0 = S$ and p is a large prime number. For n participants, compute the values $y_i = f(x_i)$ at n distinct points x_i and distribute them as sub-secrets to the n participants. If t sub-secrets (x_i, y_i) are collected, the secret can be recovered using the Lagrange interpolation formula:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{\substack{1 \le j \le t \\ j \ne i}} \frac{x - x_j}{x_i - x_j}$$

The constant term $a_0 = f(0)$ is the recovered secret message.

For convenience, we define three conditions as shown in Figure 2 [Figure 2: see original paper]. If the current block satisfies Condition 1, embedding information in this block will not propagate errors to its right neighbor through the rightmost column. If the current block satisfies Condition 2, embedding will not propagate errors to its lower-left and bottom neighbors through the bottom row. If the current block satisfies Condition 3, embedding will not propagate errors to its lower-right neighbor through the bottom-right sub-block. Therefore, using Conditions 1, 2, and 3 can control intra-frame distortion drift.

2.1 Embedding Process

Since the video content in 16×16 blocks is relatively smooth, embedding secret information can easily cause visual distortion. Therefore, this algorithm uses quantized 4×4 block DCT coefficients for embedding. Figure 3 [Figure 3: see original paper] shows the flowchart of the embedding process. First, the original H.264 video is entropy decoded to obtain the decoded DCT coefficients and

4×4 intra luminance prediction modes. Based on the absolute value of DC coefficients in the DCT blocks and a custom threshold parameter, suitable embedding blocks are selected. Blocks with non-zero coefficients and $|DC| >$ threshold are chosen as candidate embedding blocks because modulation of non-zero coefficient blocks causes less noticeable distortion. Then, among the candidate blocks, those simultaneously satisfying Conditions 1, 2, and 3 are selected as final embedding blocks. The BCH-encoded sub-secrets are embedded into the DCT coefficients of these blocks using the modulation method. Finally, all DCT coefficients containing embedded information are re-entropy-coded to obtain the target H.264 video with secret information.

The modulation method is described as follows. Let N be a positive integer and $Y_{i,j}$ be the coefficient at position (i, j) where $i, j = 0, 1, 2, 3$:

- If the bit to embed is 1 and $|Y_{i,j}| \geq 0$, modify according to equation (6):

$$\tilde{Y}_{i,j} = Y_{i,j} + N + 1$$

- If the bit to embed is 0 and $|Y_{i,j}| < 0$, modify according to equation (7):

$$\tilde{Y}_{i,j} = Y_{i,j} - (N + 1)$$

- If the bit to embed is 0 and $|Y_{i,j}| \geq 0$, no modification is made.

2.2 Extraction Process

Figure 4 [Figure 4: see original paper] shows the flowchart of the extraction process. First, the received H.264 video is entropy decoded to obtain the decoded DCT coefficients and 4×4 intra prediction modes. Based on the absolute value of DC coefficients, the custom threshold, and whether the neighboring blocks' prediction modes simultaneously satisfy Conditions 1, 2, and 3, the 4×4 blocks containing embedded secret information are selected. The encoded secret information M' is extracted from the quantized DCT coefficients:

- If $|Y_{i,j}| = N + 1$, extract bit 1 and modify according to equation (8):

$$\tilde{Y}_{i,j} = Y_{i,j} - (N + 1)$$

- If $|Y_{i,j}| = N$, extract bit 0 and no modification is made.

After extracting the information M', BCH decoding and secret sharing processing are applied to recover the secret information M.

3 Experimental Analysis

The proposed method was implemented on the H.264 reference codec software JM 16.0. Each test video was encoded at 30 fps for 300 frames, with an I-frame

interval of 15, quantization parameter of 28, and resolution of 176×144. The test video sequences included standard videos such as container, news, coastguard, and mobile. The PSNR (Peak Signal-to-Noise Ratio) was calculated as the average of PSNR values for I, B, and P frames between the original YUV video file and the embedded video file. The original video refers to the H.264 video file before secret information embedding. Frame loss rate is defined as the ratio of lost frames to total tested frames, and survival rate is the ratio of correctly extracted embedded bits to total embedded bits.

Table 1 presents the recovery performance of embedded secret information under different frame loss rates for test videos using BCH(63,7,15) and (t,n) threshold secret sharing of (3,8). The results show that the four videos achieve an average PSNR of 36.71 dB and an average embedding capacity of 7,812 bits. At random frame loss rates of 5%, 10%, and 15%, the survival rate of embedded secret information reaches nearly 100%, demonstrating good visual quality, embedding capacity, and strong robustness. Under normal network packet loss rates (10%), the method is fully suitable for secure secret information transmission. Furthermore, the embedding capacity can be adjusted by modifying the secret sharing threshold to meet requirements, and the infinite number of video frames can be utilized to accommodate the secret information to be embedded.

Table 2 compares the embedding performance of different (t,n) threshold values for the container video at a 15% network frame loss rate. The results indicate that when t remains constant and n increases, the survival rate increases; when n remains constant and t increases, the survival rate decreases. This is consistent with theoretical analysis of secret sharing. Figures 5 [Figure 5: see original paper] and 6 [Figure 6: see original paper] further verify this conclusion. Figure 5 shows the variation of secret information survival rate under different frame loss rates when t is fixed and n varies. Figure 6 shows the variation when n is fixed and t varies.

Figures 7 [Figure 7: see original paper] through 11 [Figure 11: see original paper] illustrate the survival rate variation of embedded secret information under different network frame loss rates across multiple experiments. The results demonstrate that when the network frame loss rate is no greater than 10%, the survival rate of embedded bits reaches 100% in all experiments.

Figures 12 [Figure 12: see original paper] through 14 [Figure 14: see original paper] display frames from the original News video, the embedded video, and the video after information extraction. The results show that the algorithm achieves good visual quality.

Table 3 provides a performance comparison between the proposed algorithm and algorithms [2] and [3]. Under network frame loss rates of 5%, 15%, and 20%, the average survival rates of algorithm [2], algorithm [3], and the proposed algorithm are 83.25%, 76.13%, and 97.63%, respectively. At a 15% frame loss rate, the proposed video steganography algorithm can completely recover secret information under normal network transmission conditions and exhibits high

robustness.

Figure 15 [Figure 15: see original paper] compares the performance of the proposed algorithm with algorithm [11] using the NEWS video sequence. The results show that the proposed algorithm achieves a 100% survival rate, significantly outperforming algorithm [11]. This is because algorithm [11] lacks the bit error correction capability provided by BCH codes.

4 Conclusion

This paper proposes a reversible robust video steganography method based on H.264. The method enables recovery of original secret information and restoration of the original video carrier at the receiver end even when videos containing secret information suffer from one or multiple intentional or unintentional attacks during transmission. The method can be applied to remote medical services, cloud computing, video transmission, reversible image authentication, and 2D vector maps. Since both secret sharing and BCH coding techniques are used before embedding and after extraction, the algorithm has relatively low complexity. If m_1 is the number of bits in the original secret information and m_2 is the number of original secret messages, the complexity of both embedding and extraction processes is $O(\log m_1 + m_2)$, making it suitable for real-time video applications.

References

[1] Bi Houjie. New Generation Video Compression Coding Standard H.264/AVC [M]. Beijing: People' s Posts and Telecommunications Press, 2005: 97-129.

[2] Ma X J, Li Z T, Tu H, et al. A data hiding algorithm for H.264/AVC video streams without intraframe distortion drift [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2010, 20(10): 1320-1330.

[3] Ma X J, Li Z T, Lvy J, et al. Data hiding in H.264/AVC streams with limited intra-frame distortion drift [C]// Proceedings of Computer Network and Multimedia Technology. 2009: 1-5.

[4] Liu Y X, Li Z T, Ma X J, et al. A robust without intra-frame distortion drift data hiding algorithm based on H.264/AVC [J]. Multimedia Tools and Applications, 2014, 72(1): 613-636.

[5] Liu S, Liu Y X, Feng C, et al. A reversible data hiding method based on HEVC without distortion drift [C]// Proceedings of International Conference on Intelligent Computing. 2017: 613-624.

[6] Liu Y X, Liu S Y, Zhao H G, et al. A data hiding method for H.265 without intra-frame distortion drift [C]// Proceedings of International Conference on Intelligent Computing, Intelligent Computing Methodologies. 2017: 642-651.

[7] Liu Y X, Li Z T, Ma X J, et al. A robust data hiding algorithm for H.264/AVC video streams [J]. Journal of Systems and Software, 2013, 86(8): 2174-2183.

[8] Esen E, Alatan A A. Robust video data hiding using forbidden zone data hiding and selective embedding [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2011, 21(8): 1130-1138.

[9] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[10] Liu Y X, Ma X J, Li Z T. A reversible data hiding scheme based on H.264 without distortion drift [J]. Journal of Software, 2012, 7(5): 1059-1066.

[11] Liu Y X, Ju L M, Hu M S, et al. A robust reversible data hiding scheme for H.264 without distortion drift [J]. Neurocomputing, 2015, 151(1): 1053-1060.

[12] Liu Y X, Ju L M, Hu M S, et al. A new data hiding method for H.264 based on secret sharing [J]. Neurocomputing, 2016, 188: 113-119.

[13] Zhao J, Li Z T, Feng B. A novel two-dimensional histogram modification for reversible data embedding into stereo H.264 video [J]. Multimedia Tools and Applications, 2016, 75(10): 5959-5980.

Author Information

Fund Project: National Natural Science Foundation of China (61272407)

Biographies:
Liu Shuyang (1998-), male, from Zhoukou, Henan, undergraduate student, research interests include information security (liushy2016@lzu.edu.cn).
Chen Liang (1983-), male, from Ji' an, Jiangxi, senior engineer, PhD, research interests include information security.

Note: Figure translations are in progress. See original paper for figures.