On the Security of an MPEG-Video Encryption Scheme Based on Secret Huffman Tables

Shujun Li[1], Guanrong Chen[2], Albert Cheung[2], Kwok-Tung Lo[3], Mohan Kankanhalli[4]

1 Universität Konstanz 2 香港城市大學 City University of Hong Kong 3 The Hong Kong Polytechnic University 香港理工大學 4 NUS National University of Singapore

Abstract

This paper re-studies the security of an MPEG-video encryption scheme based on secret Huffman tables proposed in [1]. The present cryptanalysis shows that: 1) the key space of the encryption scheme is not sufficiently large against divide-and-conquer (DAC) ciphertext-only attack; 2) its security against the chosen-plaintext attack is very weak. The insecurity is mainly due to the separated use of different Huffman tables for different sets of syntax elements. A brief discussion on how to improve this MPEG-video encryption scheme is also given.

MPEG-Video Encryption Scheme under Study

Figure 1: *The encryption-encoding and the decryption-decoding processes.*

Table 1: *The key space was estimated by enumerating all "good" encryption methods of the wo encryption operations performed on selected significant (NOT all) VLC codewords.*

Huffman table	Number of good encryption methods
B-10	$3!$
B-12	$7! \cdot 2^6$
B-13	$6! \cdot 2^8$
B-14	$6!$
B-15	$16!$
Total	$(3!) \cdot \left(7! \cdot 2^6\right) \cdot \left(6! \cdot 2^8\right) \cdot (6!) \cdot (16!) \approx 2^{92}$

An **optional** measure to enhance security against plaintext attack: re-encrypting the Huffman tables after a number of frames.

Cryptanalysis #1: Ciphertext-Only Attack

- *What the attacker can do*: observe a number of ciphertexts.
- *How the attack works*: exhaustively search for the five secret Huffman tables one by one among all possible ones.

Syntax Errors Indicate Wrong Huffman Tables

For the MPEG-video encryption scheme under study, the occurrence of syntax errors as follows can serve as a criterion for detecting wrong keys.

- Loss of synchronization due to incorrect bit size of any VLC codeword.
- Invalid VLC codewords.
- All stuffing bits at the end of a slice: must be 0s.
- Marker bits: must be "1" to avoid "start code emulation".
- Semantic constraints.
- Existence of EOB VLC codewords, and a maximal number of decoded DCT coefficients in each block (64).
- The number of MBs within each picture should not be greater than a maximal value.
- Skipped slice headers may be forbidden.

Breaking Five Huffman Tables One by One

The five Huffman tables are used for coding different sets of syntax elements, so it is possible to separatedly break them one by one with a **Divide-and-Conquer (DAC)** attack.

Breaking Table B-10 Following the MPEG-2 standard, Tables B-12/13/14/15 are all independent of the decoding of the first MB header in a slice, which makes the separated reconstruction of Table B-10 possible. When B-10 cannot be separatedly broken, one has to exhaustively search for Tables B-10 and B-14 together.

Breaking Table B-14 All DCT coefficients in a non-intra MB are coded with Table B-14. Thus, syntax errors may occur when a wrong Table B-14 is used to decode a non-intra MB. Since most MBs in a P/B-picture are non-intra ones, the probability of such syntax errors is practically high.

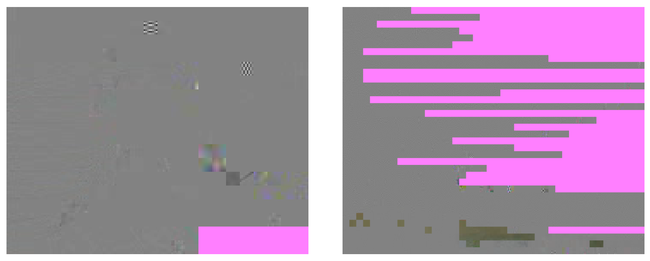

Figure 2: *Decoding an MPEG-1 video "Carphone" and an MPEG-2 video "Tennis", when two VLC codewords, "00101" and "000110", were exchanged. Note: the pink areas denote syntax errors.*

Breaking Table B-12 Once Table B-14 is reconstructed, Table B-12 can be further exhaustively searched for in intra MBs with *intra_vlc_format* = 0. If all intra MBs are encoded with *intra_vlc_format* = 1, Table B-12 has to be exhaustively searched for together with Table B-15.

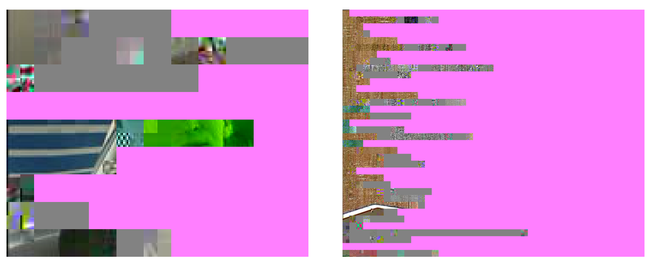

Figure 3: *Decoding the MPEG-1 video "Carphone" and the MPEG-2 video "Tennis", when two VLC codewords, "00" and "01", were exchanged.*

Breaking Table B-15 If Table B-12 has been broken, Table B-15 can be exhaustively searched for in luminance blocks of intra MBs with *intra_vlc_format* = 1, just like Table B-14.

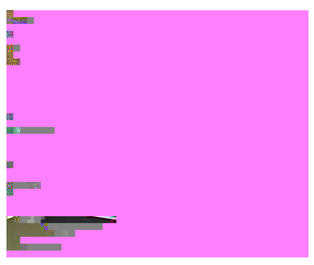

Figure 4: *Decoding the MPEG-2 video "Tennis", when two VLC codewords, "00101" and "000110", were exchanged.*

Breaking Table B-13 After Tables B-12/14/15 are broken, Table B-13 can be exhaustively searched for in chrominance blocks of intra MBs. If there are intra MBs with *intra_vlc_format* = 0, it can be exhaustively broken immediately after Table B-14 is broken, without knowing Table B-15.

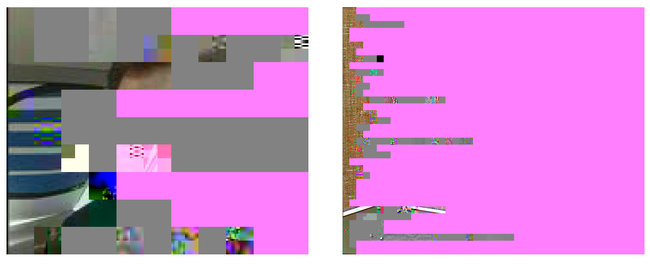

Figure 5: *Decoding the MPEG-1 video "Carphone" and the MPEG-2 video "Tennis", when two VLC codewords, "01" and "10", were exchanged.*

Computational Complexity

B-10	B-12	Complexity
Yes	Yes	$(3!) + (7! \cdot 2^6) + (6! \cdot 2^8) + (6!) + (16!) \approx 2^{44.3} \ll 2^{92}$
No	Yes	$(3!) \cdot (6!) + (7! \cdot 2^6) + (6! \cdot 2^8) + (16!) \approx 2^{44.3} \ll 2^{92}$
Yes	No	$(3!) + (7! \cdot 2^6) \cdot (16!) + (6! \cdot 2^8) + (6!) \approx 2^{62.5} \ll 2^{92}$
No	No	$(3!) \cdot (6!) + (7! \cdot 2^6) \cdot (16!) + (6! \cdot 2^8) \approx 2^{62.5} \ll 2^{92}$.
Note: "B-10"/"B-12" = B-10/B-12 separatedly broken.		

Cryptanalysis #2: Chosen-Plaintext Attack

- *What the attacker can do*: choose a number of plaintexts and observe the corresponding ciphertexts.
- *How the attack works*: the plaintexts are chosen to trigger syntax errors for each Huffman table.

Breaking Huffman Tables One by One

Breaking Table B-10 Choose a P-picture, in which there are a number of consecutive slices that contains only one "Not Coded" non-intra MB. The values of *motion_residuals*, *dmvectors*, the sign bits of the motion vectors, and even *f_code*[*r*][*s*] can be chosen to uniquely distinguish the VLC codeword corresponding to each value of *motion_code*.

Breaking Table B-14 After breaking Table B-10, choose one or more blocks in a non-intra MB with the following pattern until all VLC codewords are obtained:
"(run_1, $level_1$), (run_e, $level_e$), $\cdots$, (run_i, $level_i$), (run_e, $level_e$), $\cdots$, EOB",
where (run_i, $level_i$) is the i-th entry in the secret Table B-14 and (run_e, $level_e$) is an Escape RLE codeword.

Breaking Tables B-12/13 To break the entry corresponding to *dct_dc_size* = *s*, choose an intra-block as follows: "*level*, EOB", where the DC coefficient *level* has *s* significant bits. Then, the video bitstream corresponding to this block will be "*dct_dc_size* = *s*, *dc_dct_differential*, EOB".

Breaking Table B-15 After breaking Tables B-12 and B-13, one can break Table B-15 by choosing some intra-blocks, in the same way of breaking Table B-14.

The Number of Chosen Plaintexts

As a whole, to completely break all the secret Huffman table, at most 4 intra MBs in an I-picture and 3 non-intra MBs in a P-picture (or 2 non-intra MBs in a B-picture) are needed. Note that only one chosen picture is enough to recover all secret Huffman tables needed for decoding the same type of pictures (and part of other types of pictures).

Two More Points

- A very frequent and thus very heavy re-encryption of the Huffman tables have to be employed to resist the proposed attacks, which may not be practical in some real applications.
- Using multiple Huffman tables (MHT) [7] with a stream cipher can be another solution, but the performance may not be better than simply using the stream cipher for encryption without secret Huffman tables.

References

[1] Kankanhalli, M.S., Guan, T.T.: Compressed-domain scrambler/descrambler for digital video. IEEE Trans. Consumer Electronics **48**(2) (2002) 356–365
[2] ISO/IEC, ITU-T: Information technology – generic coding of moving pictures and associated audio information: Video. MPEG-2 standard: ISO/IEC 13818-2 and ITU-T Rec. H.262 (2000)
[3] Schneier, B.: Applied Cryptography – Protocols, Algorithms, and Souce Code in C. Second edn. John Wiley & Sons, Inc., New York (1996)
[4] Wu, C.P., Kuo, C.C.J.: Fast encryption methods for audiovisual data confidentiality. In: Multimedia Systems and Applications III. Volume 4209 of Proc. SPIE. (2001) 284–295
[5] Wu, C.P., Kuo, C.C.J.: Efficient multimedia encryption via entropy codec design. In: Security and Watermarking of Multimedia Contents III. Volume 4314 of Proc. SPIE. (2001) 128–138
[6] Xie, D., Kuo, C.C.J.: An enhanced MHT encryption scheme for chosen plaintext attack. In: Internet Multimedia Management Systems IV. Volume 5242 of Proc. SPIE. (2003) 175–183
[7] Wu, C.P., Kuo, C.C.J.: Design of integrated multimedia compression and encryption systems. IEEE Trans. Multimedia **7**(5) (2005) 828–839
[8] Zhou, J., Liang, Z., Chen, Y., Au, O.C.: Security analysis of multimedia encryption schemes based on multiple Huffman table. IEEE Signal Processing Letters **14**(3) (2007) 201–204
[9] Jakimoski, G., Subbalakshmi, K.P.: Cryptanalysis of some multimedia encryption schemes. IEEE Trans. Multimedia **10**(3) (2008) 330–338

Corresponding author is Shujun Li. Contact him via his personal web site: `http://www.hooklee.com`.