JOINT FINGERPRINT EMBEDDING AND DECRYPTION FOR VIDEO DISTRIBUTION

Shiguo Lian, Zhongxuan Liu, Zhen Ren, Haila Wang

SAMI Lab, France Telecom R&D Beijing
Beijing, 100080, P.R China
shiguo.lian@orange-ftgroup.com

ABSTRACT

A secure video distribution scheme is proposed, which embeds a fingerprint code into the video content during decryption process. At the server side, the video content is scrambled by motion vector (MV) encryption. At the customer side, the video content is decrypted and fingerprinted simultaneously under the control of both the key and the fingerprint. For MV decryption and fingerprint embedding are both based on MV modification, they are combined into homogenous operations. Thus, it is difficult for attackers to get the clear video content from the gap between the decryption operation and the embedding operation. To counter collusion attacks, the fingerprint can be encoded with collusion-resistant codes before being embedded. Furthermore, by improving the watermarking strength, the colluded copy's quality will be reduced greatly, which makes collusion attacks out of work.

1. INTRODUCTION

Secure multimedia distribution becomes more and more important and urgent with the wide spread of multimedia content. It transmits media data to customers and can trace illegal distributors. Till now, two kinds of distribution schemes have been proposed: the broadcasting encryption scheme and the fingerprint based scheme.

The broadcasting encryption scheme [1] implements secure media distribution over broadcasting networks. It partitions media data into segments, encrypts each segment into two cipher-segments under the control of two sub-keys, and then sends all the encrypted cipher-segments to customers. The scheme reduces the server's loading, while it cannot solve the Super Distribution problem [2]: the decrypted copy may be distributed without control.

The fingerprint-based scheme [3,4,5] has the potential property to solve the Super Distribution problem. For each customer, the fingerprint (a unique watermark, i.e., customer ID) is embedded into the media content. Thus, each customer receives different copy with a unique watermark. The key problem is to embed the fingerprint in secure and efficient ways. The multicast media distribution scheme [3] embeds the fingerprint at the server side, which needs to transmit double size of the media content. The WaterCasting scheme [4] embeds watermarks with the routers, which distributes the server's loading to the routers, but needs to modify transmission protocols. Another scheme [5] embeds fingerprints into media content at the receiver side, which reduces the server's loading greatly, but cannot confirm the security. It is because that the clear media may be released from the gap between decryption and fingerprint embedding.

As an alternative, the joint fingerprint embedding and decryption (JFD) scheme decrypts and marks the media content simultaneously at the receiver side. Different decryption key produces different copy. For example, Anderson et al [6] proposed the scheme based on a stream cipher, which encrypts an image with a stream cipher and embeds different watermarks into the LSBs of the image. This scheme is efficient, while not robust to signal processing (recompression, adding noise, etc). Kundur et al [7] proposed the scheme based on partial decryption, which scrambles the sign bit of the DCT coefficients and decrypts only part of the sign bits in decryption. This scheme is robust to some signal processing operations, but its perceptual security is not high enough, and the security against collusion attacks is not confirmed. Lemma et al [8] proposed the scheme based on selective encryption. The scheme is efficient, while large size of key needs to be transmitted, and the security against collusion attacks is not confirmed.

In this paper, we present a new JFD scheme in order to obtain better performances. The encryption algorithm and watermarking algorithm based on homogeneous operations are used to encrypt and mark media content, which keep their properties, such as security and robustness, unchanged. Additionally, according to watermarking algorithms' properties, it is easy to implement watermark detection and traitor tracing. The rest of the paper is arranged as follows. In Section 2, the secure distribution scheme is proposed. The example based on motion vector encryption and watermarking is presented in Section 3. In Section 4, its performances are analyzed. Conclusions are drawn and future work is given in Section 5.

2. THE PROPOSED SECURE DISTRIBUTION SCHEME

Only one encrypted stream is transmitted, and different copy is recovered by different key. At the server side, the original media content P is encrypted into C with the encryption algorithm E under the control of the key K. That is,

$$C = \mathrm{E}(P, K).$$

At the receiver side, different customer decrypts the media content C into different copy P_j (j=0,1,…,M-1) (M is the number of customers) with the homogeneous decryption and watermarking algorithm under the control of the decryption key K_j. That is,

$$\begin{cases} P_j = \mathrm{D}(C, K_j) \\ K_j = K \,||\, F_j \end{cases}.$$

Here, D() is the homogeneous decryption or watermarking algorithm, F_j denotes the fingerprint of the j-th customer, and "||" denotes the combination between decryption and watermarking.

3 THE SCHEME BASED ON MOTION VECTOR ENCRYPTION AND WATERMARKING

Motion vector encryption and watermarking [9,10] both modify motion vectors in order to realize video encryption and video watermarking. By combining the homogeneous operations, the decryption and watermarking can be implemented in a seamless way. Fig. 1 shows the encryption, watermarking and JFD operations. Here, $\vec{V}$ is the original motion vector (OA), $\vec{V}'$ is the watermarked motion vector (OA'), $\vec{V}''$ is the encrypted motion vector (OA''), S_W denotes the watermarked motion vector set corresponding to $\vec{V}$, S_E denotes the encrypted motion vector set corresponding to $\vec{V}$, K is the encryption/decryption key, and $F_j\ (j = 0, 1, \cdots, M-1)$ is the fingerprint.

Intuitively, the motion vector is decrypted and watermarked according to the following steps: 1) the motion vector $\vec{V}''$ (OA'') is decrypted into $\vec{V}$ (OA), 2) the motion vector $\vec{V}$ (OA) is marked and produces $\vec{V}'$ (OA'). Differently, in this scheme, $\vec{V}''$ (OA'') is decrypted into $\vec{V}'$ (OA') directly. And the process is controlled by both the decryption key K and the fingerprint F_j.

3.1 Motion Vector Encryption

Scrambling motion vector reduces videos' quality, and can be used to encrypt videos, together with DCT encryption [10]. In order to reduce the effect on compression ratio, we partition MVs into 8 sets according to the VLC length (H.264/AVC), as shown in Table 1. Here, each set is composed of no less than 2 MVs, and each MV is scrambled in the corresponding set. Additionally, in each set, all the MVs are even or odd. This condition keeps the scrambling operation and watermarking operation homogeneous.

An example of MV scrambling is presented as follows. If the original vector is $\vec{V} = [v_x, v_y] = [-6, 11]$ (v_x and v_y are the horizontal and vertical vector, respectively), then it will be encrypted into $\vec{V}'' = [v_x'', v_y'']$. Here, v_x'' varies in Set 2={4,-4,6,-6}, and v_y'' varies in Set 4={9,-9,11,-11,13,-13,15,-15}.

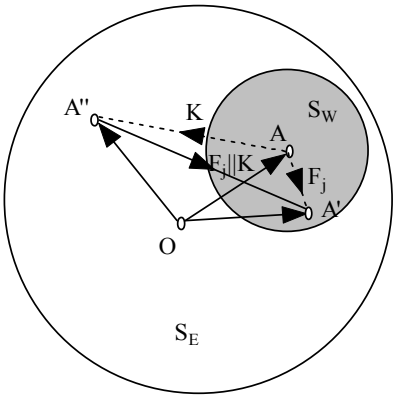


Fig. 1. The proposed JFD scheme based on MV encryption

Table 1 The Motion Vector Sets

Matched Set	VLC Length	Number of Vectors	Motion Vectors
0	3	2	± 1
1	5	2	± 2
2	5	2	± 3
3	7	4	$\pm 4, \pm 6$
4	7	4	$\pm 5, \pm 7$
5	9	8	$\pm 8, \pm 10, \pm 12, \pm 14$
6	9	8	$\pm 9, \pm 11, \pm 13, \pm 15$
7	11	2	± 16

3.2 Joint Fingerprint Embedding and Decryption

The fingerprint is embedded into the MVs during MV decryption. Set F_j the fingerprint bit, and $\vec{V}' = [v_x', v_y']$ the decrypted and fingerprinted MV. Then, the JFD scheme is presented as follows.

If F_j=1, then

$$\begin{cases} v_x' = \mathrm{D}(v_x'', K), v_y' = \mathrm{D}(v_y'', K), & v_x''\%2 = 1 \text{ and } v_y''\%2 = 0 \\ v_x' = \mathrm{D}(v_x'', K) + 1, v_y' = \mathrm{D}(v_y'', K) + 1, & v_x''\%2 = 0 \text{ and } v_y''\%2 = 1 \\ v_x' = \mathrm{D}(v_x'', K) + 1, v_y' = \mathrm{D}(v_y'', K), & v_x''\%2 = 0 \text{ and } v_y''\%2 = 0 \\ v_x' = \mathrm{D}(v_x'', K), v_y' = \mathrm{D}(v_y'', K) + 1, & v_x''\%2 = 1 \text{ and } v_y''\%2 = 1 \end{cases}$$

If F_j=0, then

$$\begin{cases} v_x' = \mathrm{D}(v_x'', K) - 1, v_y' = \mathrm{D}(v_y'', K) - 1, & v_x''\%2 = 1 \text{ and } v_y''\%2 = 0 \\ v_x' = \mathrm{D}(v_x'', K), v_y' = \mathrm{D}(v_y'', K), & v_x''\%2 = 0 \text{ and } v_y''\%2 = 1 \\ v_x' = \mathrm{D}(v_x'', K), v_y' = \mathrm{D}(v_y'', K) - 1, & v_x''\%2 = 0 \text{ and } v_y''\%2 = 0 \\ v_x' = \mathrm{D}(v_x'', K) - 1, v_y' = \mathrm{D}(v_y'', K), & v_x''\%2 = 1 \text{ and } v_y''\%2 = 1 \end{cases}$$

Here, % denotes the module operation, and D() is the inverse scrambling operation.

3.3 Fingerprint Extraction

The fingerprint bit F_j can be extracted as follows.

$$F_j = \begin{cases} 1, & v_x'\%2 = 1 \text{ and } v_y'\%2 = 0 \\ 0, & v_x'\%2 = 0 \text{ and } v_y'\%2 = 1 \end{cases}$$

4 PERFORMANCE ANALYSIS

4.1 Security of the Encryption Scheme

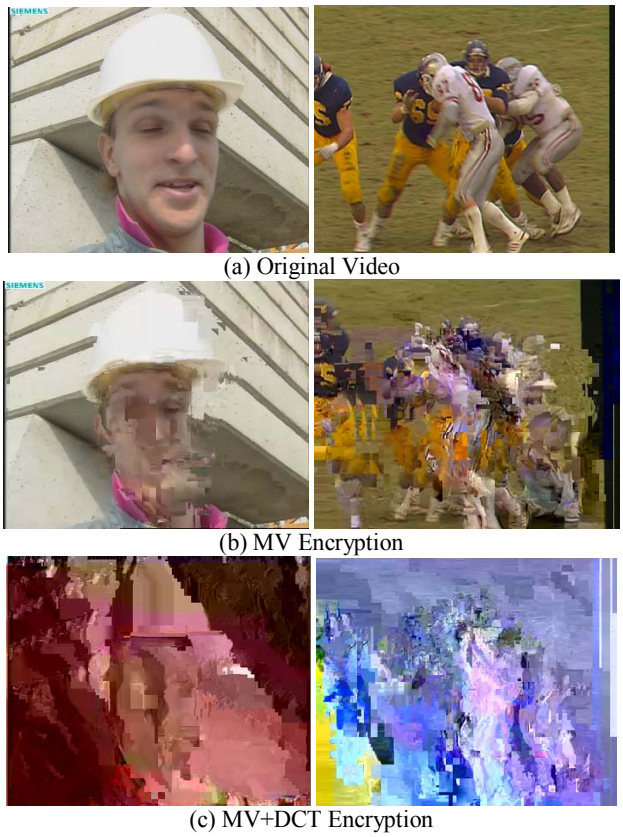
As a media encryption algorithm, the security includes two aspects: cryptographic security and perceptual security [10]. Cryptographic security denotes the security against cryptographic attacks, while perceptual security means the perceptibility of the encrypted media data.

In perception, encrypting only MVs degrades the video quality, but cannot protect the media content completely. Fig. 2 gives the experimental results on two sample video clips. As can be seen, the video content Fig. 2(b) is still intelligible especially when the video contains more background than motion objects. To improve the security, DCT coefficients can also be encrypted, as shown in Fig. 2(c).

From cryptographic viewpoint, brute-force attack is the basic method to break a cryptosystem. In this scheme, MVs are scrambled within each MV set. Set H the size of a MV set. If multi-keys are used, the brute-force space of N MVs is H^N. According to Table 1, H is no smaller than 2. Thus, the space is no smaller than 2^N. As long as N is big enough, the security against brute-force attack can be confirmed. The security against some other attacks as known-plaintext or select-plaintext attack can be improved by combining with DCT encryption.

4.2 Collusion Resistance

This scheme embeds fingerprints into the video content according to a watermarking algorithm. Thus, the fingerprint is easy to be detected. The system's collusion resistance depends on two aspects: 1) the fingerprint's collusion resistance, and 2) the quality degradation caused by collusion attacks. For the first aspect, the fingerprint is encoded with the fingerprint code [11,12] that produces the fingerprint resistant to some collusion attacks. For the second aspects, by improving the embedding strength, the collusion attacks can be forbidden, because the colluded videos' quality is often reduced greatly. Based on fingerprint code [12], the scheme's correct detection rate (Cdr) is tested and shown in Fig. 3. Here, the x-label denotes the prediction resolution in motion vector modification. As can be seen, Cdr decreases with the rise of prediction resolution. On the other hand, the colluded video's quality decreases with the rise of prediction resolution, as shown in Fig. 4. The colluded video is slightly blurry in 0.5-pixel prediction resolution, while is apparently blurry in 1-pixel prediction resolution. Thus, for this scheme, the collusion often happens below 0.5-pixel prediction mode, otherwise the colluded copy will lose the practical value. When the prediction resolution is no bigger than 0.5, Cdr may be acceptable (no smaller than 80%).



(a) Original Video

(b) MV Encryption

(c) MV+DCT Encryption

Fig. 2. Results of video encryption

5 DISCUSSIONS AND FUTURE WORK

In this paper, we present a secure media distribution scheme based on homogeneous encryption and watermarking operations. Compared with the existing schemes [6,7], the proposed scheme has some good properties: 1) The homogeneous encryption and watermarking operations both keep their properties, 2) The fingerprint is embedded with watermark embedding methods, which makes it easy to extract the fingerprint, and 3) The fingerprint can be encoded with some fingerprint encoding methods that keep

resistant to some collusion attacks. However, some means need to be taken to improve its practicality, such as avoiding the error propagation caused by modifying motion vectors. Additionally, some other homogeneous encryption and watermarking algorithms will be considered, which may obtain better performances.

ACKNOWLEDGEMENT

This work was supported by France Telecom project "Tatouage" through the grant code PEK06-ILAB-008.

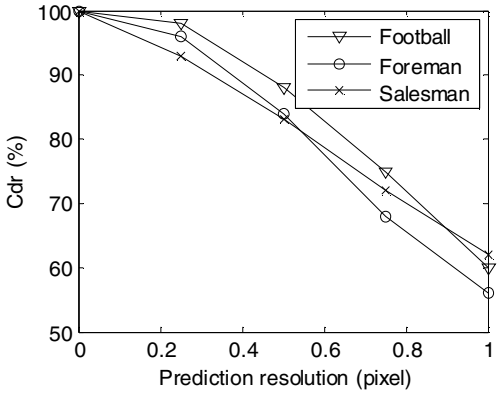


Fig. 3. Correct detection rate after collusion attacks

(a) Fingerprinted copy

(b) Colluded copy 0 (0.5p)

(c) Colluded copy 1 (1p)

Fig. 4. Perceptual quality of colluded video copies

REFERENCES

[1] B. M. Macq and J. J. Quisquater. Cryptology for digital TV broadcasting. Proceedings of the IEEE, 83(6): 944-957, 1995.

[2] D. Boneh, J. Shaw. Collusion-secure fingerprinting for digital data. In Proceeding of Advances in Cryptology - CRYPTO'95, LNCS 963, pp. 452-465, 1995.

[3] R. Parnes and R. Parviainen, "Large scale distributed watermarking of multicast media through encryption," in Proc. IFIP Int. Conf. Communications and Multimedia Security Issues of the New Century, pp. 17, 2001.

[4] I. Brown, C. Perkins, and J. Crowcroft. Watercasting: Distributed watermarking of multicast media. In Proceedings of International Workshop on Networked Group Communication, Springer-Verlag LNCS, 1736, 1999.

[5] J. Bloom, "Security and rights management in digital cinema," in Proc. IEEE Int. Conf. Acoustic, Speech and Signal Processing, Vol. 4, pp. 712-715, 2003.

[6] R. Anderson and C. Manifavas, "Chameleon – A new kind of stream cipher," in Lecture Notes in Computer Science, Fast Software Encryption, Springer-Verlag, pp. 107-113, 1997.

[7] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proceedings of the IEEE, Vol. 92, No. 6, pp. 918-932, 2004.

[8] A. N. Lemma, S. Katzenbeisser, M. U. Celik, M. V. Veen. Secure Watermark Embedding Through Partial Encryption. Proceedings of International Workshop on Digital Watermarking (IWDW 2006), Springer LNCS, 4283, 433-445, 2006.

[19] Y. Bodo, N. Laurent, J. Dugelay, "Watermarking video, hierarchical embedding in motion vectors," In IEEE International Conference on Image Processing, Spain, 2003.

[10] S. Lian, Z. Liu, Z. Ren and H. Wang. Secure Advanced Video Coding Based on Selective Encryption Algorithms. IEEE Transactions on Consumer Electronics, Vol. 52, No. 2, pp. 621-629, 2006.

[11] D. Boneh, J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Trans. Inform. Theory, Vol. 44, pp. 1897-1905, Sept. 1998.

[12] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, Anti-collusion fingerprinting for multimedia, IEEE Trans. Signal Processing, Vol. 51, pp. 1069-1087, Apr. 2003.