An Optical Video Cryptosystem with Adaptive Steganography

Cheng-Hung Chuang
Dept. of Computer Sci. and Information Eng.
Asia University
Taichung County 41354, Taiwan
chchuang@asia.edu.tw

Guo-Shiang Lin
Dept. of Computer Sci. and Information Eng.
Da-Yeh University
Changhua County 51591, Taiwan
khlin@mail.dyu.edu.tw

Abstract

In this paper, an optical cryptosystem with adaptive steganography is proposed for video sequence encryption and decryption. The optical cryptosystem employs a double random phase encoding algorithm to encrypt and decrypt video sequences. The video signal is first transferred to RGB model and then separated into three channels: red, green, and blue. Each channel is encrypted by two random phase masks generated from session keys. For higher security, an asymmetric method is applied to cipher session keys. The ciphered keys are then embedded into the encrypted video frame by a content-dependent and low distortion data embedding technique. The key delivery is accomplished by hiding ciphered data into the encrypted video frame with a specific hiding sequence generated by the zero-LSB sorting technique. Experimental results show that the adaptive steganography has a better performance than the traditional steganography in the video cryptosystem.

1. Introduction

Due to the fast development of communication technology, it is convenient to acquire multimedia data. Unfortunately, the problem of illegal data access occurred everywhen and everywhere. Hence, it is important to protect the content and the authorized use of multimedia data against the attackers. Data encryption is a strategy to make the data unreadable, invisible or incomprehensible during transmission by scrambling the content of data [1]. In an image cryptosystem, it uses some reliable encryption algorithms or secret keys to transform or encrypt secret images into ciphered images. Only the authorized users can decrypt secret images from the ciphered images. The ciphered images are meaningless and non-recognizable for any unauthorized users who grab them without knowing the decryption algorithms or the secret keys.

Dissimilarly, steganographic techniques refer to methods of embedding secret data into cover data in such a way that people can not discern the existence of the hidden data. The image steganographic methods (or called virtual image cryptosystems) [2-5] are proposed to hide the secret images into readable but non-critical cover images. They are designed to reduce the notice of illegal users. Common methods for data hiding can be categorized into spatial and transform domain methods. In the spatial domain, secret data is directly embedded into the values of image pixels. Contrarily, in the transform domain, e.g., discrete cosine transform (DCT), Fourier transform, or wavelets, transformed coefficients of cover signals can be manipulated to hide messages. The earliest method, which is simple and has high embedding capacity, embedded data into least significant bits (LSBs) of image pixel values or quantized transform coefficients.

For high speed optical system application, many optical image encryption algorithms have been developed for transmission security [6-10]. The double random phase encoding [6] is a famous and widely used algorithm which employs two random phase masks in the input plane and the Fourier plane to encrypt images into stationary white noise. In [7], an optical image cryptosystem based on the double random phase encryption and a public-key type of data embedded technique is proposed. In [8], the optical encryption is performed using the fractional Fourier transform. In [9], the encryption method using wavelength multiplexing and lensless Fresnel transform hologram is proposed for color image application. In [10], the optical color image encryption scheme is performed in the fractional Fourier transform domain. However, the input data is limited to still images in those cryptosystems.

Since video data security is very important for multimedia application, e.g. video surveillance, pay-TV, video-on-demand, and videoconference, it is essential to develop video encryption techniques. Most video encryption methods are operated on MPEG compressed domain [11-14]. Nevertheless, very few optical methods have been proposed or published for video encryption. In this paper, we propose an optical video cryptosystem based on the double random phase encryption and the adaptive steganographic method. The session keys of random phase masks are encrypted by the asymmetric encryption method, e.g. Rivest-Shamir-Adleman (RSA) algorithm [15]. This ciphered data is embedded into LSBs of the encrypted video frame, in which a zero-LSB sorting technique is applied to find the hiding sequence. Simulation and experimental results show that the proposed video cryptosystem has a good performance in secure data embedding, hiding capacity, and visual quality.

2. The Proposed Method

In the double random phase encoding [6] of the optical system, an image I is multiplied by a random phase mask P_s in the input plane and transformed to Fourier domain. It is multiplied by another random phase mask P_f and converted to the spatial domain for obtaining the encrypted image I_e. In the decoding step, the encrypted image is transformed to the Fourier plane, multiplied by the conjugate of mask P_f, converted to spatial field, and multiplied by the conjugate of mask P_s to obtain its decrypted image I_d. The equations are defined as follows.

$$I_e = F^{-1}\left\{F\{I\exp(i2\pi P_s)\}\exp(i2\pi P_f)\right\} \tag{1}$$

$$I_d = F^{-1}\left\{F\{I_e\}\exp(i2\pi P_f^*)\right\}\exp(i2\pi P_s^*) \tag{2}$$

where F denotes the Fourier transformation, F^{-1} indicates its inverse transformation, and P_s*, P_f* are the conjugate masks of P_s, P_f. Figure 1 shows the optical setup of the double random phase encryption and decryption.

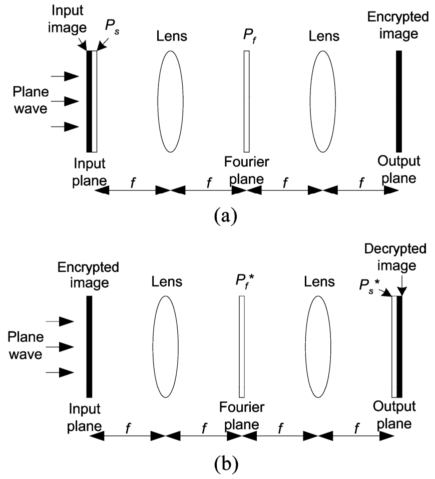
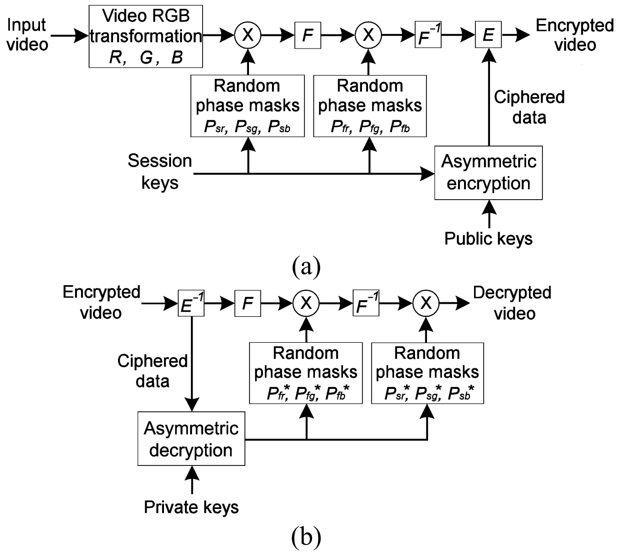


Figure 1. Schematic diagram for optical implementation of double random phase (a) encryption and (b) decryption (*f* is focal length of the lens).

For a video sequence, it is first transformed to RGB model and separated into three channels: red, green, and blue in each video frame. The three channels are coded by the double random phase algorithm, i.e. multiplied by masks P_{sr}, P_{sg}, P_{sb}, and P_{fr}, P_{fg}, P_{fb}. Session keys are used to generate these phase masks and then ciphered by the asymmetric encryption algorithm for higher security. The ciphered data is embedded into the encrypted video frame for the delivery of session keys. The receiver, who owns the private keys of the encryption algorithm, can decipher session keys using the secret data extracted from the encrypted video frame. Then the session keys are used to decrypt and reconstruct the video frame. Figure 2 shows the schema of the proposed optical video cryptosystem.

The ciphered data is embedded into LSBs of the quantized encrypted video frame. Hence, the quantization and embedding processes will cause the loss in visual quality. Based on the LSB algorithm, the important issue is how to select the hidden regions or positions that result in low distortion. It is a simple way to hide the data in fixed positions of the encrypted video frame. Nevertheless, due to the different video content, the fixed positions are not always suitable for hiding data. To improve the visual quality of the decrypted video sequences and safely convey the session keys, a low distortion, adaptive, and content-dependent data embedding technique is applied to hide the secret data. In our strategy, the transformation coefficients with smaller absolute values are preferable to hide data due to smaller energy and quantization step size. To keep the embedding and decoding sequences invariant, the LSBs are set to zero and a sorting technique is employed.



Input video
Video RGB transformation R, G, B
X
F
X
F^{-1}
E
Encrypted video
Random phase masks P_{sr}, P_{sg}, P_{sb}
Random phase masks P_{fr}, P_{fg}, P_{fb}
Ciphered data
Session keys
Asymmetric encryption
Public keys
(a)
Encrypted video
E^{-1}
F
X
F^{-1}
X
Decrypted video
Ciphered data
Random phase masks P_{fr}^*, P_{fg}^*, P_{fb}^*
Random phase masks P_{sr}^*, P_{sg}^*, P_{sb}^*
Asymmetric decryption
Private keys
(b)

Figure 2. Schema of the proposed video cryptosystem. (a) Encryption, (b) Decryption (X: multiplication, E and E^{-1}: the embedding and decoding functions).

Assume that there are n bits in the ciphered data, i.e. $B=\{b_1, b_2, \ldots, b_n\}$. Since the transformation coefficients in the encrypted video frame in the optical system are complex numbers, the real and imaginary parts can be selected to embed data. In this paper, the real part is chosen for the hidden site. The detailed embedding and decoding procedures are described as follows.

2.1. Embedding Procedure

1. The absolute values of real part of the transformation coefficients are sorted in ascending order. The set of the first n+2 numbers except the maximum and the minimum is chosen and defined as Λ, i.e. $\Lambda=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, where $|\alpha_i| \leqq |\alpha_{i+1}|$, α_i and $\alpha_{i+1} \in \Lambda$. Note that the maximum and minimum in the first n+2 numbers are not used to be quantized and hidden data, since the quantization step size should be computed from them.
2. The set Λ is quantized to be $\Lambda_Q=\{\alpha_{q1}, \alpha_{q2}, \ldots, \alpha_{qn}\}$ with a quantization level denoted as QL.
3. All LSBs of Λ_Q are modified to zero to obtain the zero-LSB set $\Lambda_{QZ}=\{\alpha_{qz1}, \alpha_{qz2}, \ldots, \alpha_{qzn}\}$. Then all elements in Λ_{QZ} are sorted in ascending order with their absolute values to obtain the sorted zero-LSB set $\Lambda_{QZS}=\{\alpha_{qzs_1}, \alpha_{qzs_2}, \ldots, \alpha_{qzs_n}\}$, where $\left|\alpha_{qzs_i}\right| \leqq \left|\alpha_{qzs_{i+1}}\right|$, α_{qzs_i} and $\alpha_{qzs_{i+1}} \in \Lambda_{QZS}$. The set of numbers $S=\{s_1, s_2, \ldots, s_n\}$, where $s_i \in \{1, 2, \ldots, n\}$ and i=1, 2, …, n, is used to be the hiding sequence.
4. The ciphered data B is successively embedded into LSBs of the set Λ_Q with sequence S, i.e. $\Lambda_{QS}=\{\alpha_{qs_1}, \alpha_{qs_2}, \ldots, \alpha_{qs_n}\}$, where $\alpha_{qs_i} \in \Lambda_Q$. The embedding rule is defined as
$$\alpha_{qs_i}^e = \alpha_{qs_i} + \operatorname{sgn}(b_i - \operatorname{mod}(\alpha_{qs_i}, 2)) \tag{3}$$
where $\operatorname{sgn}(\cdot) \in \{-1, 0, 1\}$ is the signum function, i=1, 2, …, n. Thus the set with hidden data becomes $\Lambda_{QS}^E = \{\alpha_{qs_1}^e, \alpha_{qs_2}^e, \ldots, \alpha_{qs_n}^e\}$.
5. Finally, the set Λ_{QS}^E is de-quantized to get Λ_S^E =

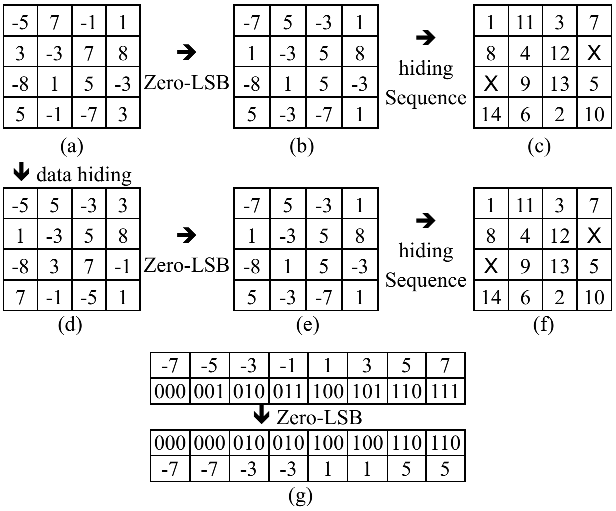
$\{\alpha^e_{s_1}, \alpha^e_{s_2}, ..., \alpha^e_{s_n}\}$.

2.2. Decoding procedure

1. This step is the same as the 1st step in embedding procedure. The set is defined as $\Lambda^E=\{\alpha_1{}^e, \alpha_2{}^e, \ldots, \alpha_n{}^e\}$, where $|\alpha^e_i| \leqq |\alpha^e_{i+1}|$, α^e_i and $\alpha^e_{i+1} \in \Lambda^E$. The sequence in Λ^E is different from that in Λ.
2. The set Λ^E is quantized with QL to be $\Lambda^E_Q = \{\alpha^e_{q1}, \alpha^e_{q2}, ..., \alpha^e_{qn}\}$.
3. All LSBs of Λ^E_Q are set to zero to obtain the zero-LSB set $\Lambda^E_{QZ} = \{\alpha^e_{qz1}, \alpha^e_{qz2}, ..., \alpha^e_{qzn}\}$. The elements in Λ^E_{QZ} are sorted in ascending order with their absolute values to obtain $\Lambda^E_{QZS} = \{\alpha^e_{qzs_1}, \alpha^e_{qzs_2}, ..., \alpha^e_{qzs_n}\}$, where $|\alpha^e_{qzs_i}| \leqq |\alpha^e_{qzs_{i+1}}|$, $\alpha^e_{qzs_i}$ and $\alpha^e_{qzs_{i+1}} \in \Lambda^E_{QZS}$.
4. Now, the set Λ^E_{QZS} is equal to the set Λ_{QZS} with the same sequence, $S=\{s_1, s_2, \ldots, s_n\}$. The hidden data $B=\{b_1, b_2, \ldots, b_n\}$ is correctly extracted from LSBs of the set $\Lambda^E_{QS} = \{\alpha^e_{qs_1}, \alpha^e_{qs_2}, ..., \alpha^e_{qs_n}\}$, i.e.

$$b_i = \begin{cases} 0, \text{ if } \mathrm{mod}(\alpha^e_{qs_i}, 2) = 0 \\ 1, \text{ if } \mathrm{mod}(\alpha^e_{qs_i}, 2) = 1 \end{cases} \tag{4}$$

Figure 3 shows a 4×4 example of data hiding and decoding where numbers in (a) are real part values of the transformation coefficients, (b) is the zero-LSB set of (a), (c) is the hiding sequence computed from (b), (d) is results of (a) after data hiding, (e) is the zero-LSB set of (d), (f) is the hiding sequence computed from (e), and (g) is the corresponding binary list. It is clear that the zero-LSB sets in (b) and (e) are matched and sequences in (c) and (f) are equal, although (a) and (d) are different.



(a)

-5	7	-1	1
3	-3	7	8
-8	1	5	-3
5	-1	-7	3

(b)

-7	5	-3	1
1	-3	5	8
-8	1	5	-3
5	-3	-7	1

(c)

1	11	3	7
8	4	12	X
X	9	13	5
14	6	2	10

(d)

-5	5	-3	3
1	-3	5	8
-8	3	7	-1
7	-1	-5	1

(e)

-7	5	-3	1
1	-3	5	8
-8	1	5	-3
5	-3	-7	1

(f)

1	11	3	7
8	4	12	X
X	9	13	5
14	6	2	10

(g)

-7	-5	-3	-1	1	3	5	7
000	001	010	011	100	101	110	111
000	000	010	010	100	100	110	110
-7	-7	-3	-3	1	1	5	5

Figure 3. A simple example of data hiding and decoding (QL=8; hidden data=11001110100011).

3. Experiment

In our experiment, 18 YUV video sequences in QCIF format (selected from [16]) are examined. The PSNR given by Eq. (5) and (6) is applied to evaluate the visual quality of the decrypted video sequences, i.e.

$$PSNR = \frac{1}{k}\sum_{i=1}^{k} PSNR_i, \tag{5}$$

$$PSNR_i = 10\log_{10}\frac{255^2}{MSE_i}, \tag{6}$$

where $PSNR_i$ and MSE_i are the PSNR and the mean square error of the ith video frame, respectively. MSE_i is computed by the average MSE values of the R, G, and B channels of the ith video frame. The conventional steganographic algorithm [7], where the ciphered data is hidden into the central square area in the encrypted video frame, and the adaptive steganographic method are performed for comparison.

First, the visual quality of video sequences is evaluated with different quantization levels. The hidden data size in each video frame is set to a fixed value, i.e. 19200 bits. Table 1 shows the maximal, minimal, and average PSNR values of the 18 decrypted video sequences with different quantization levels, i.e. QL=8, 16, 32, 64, 128, and 256. It is obvious that the PSNR values increase over 20 dB between the results of the conventional method and the adaptive one. Figure 4 plots the PSNR values of the 18 decrypted video sequences with QL=8. The top and bottom lines are the results using the adaptive and the conventional methods, respectively. Figure 5 shows some sample original, encrypted, and decrypted video frames, where the decrypted results by using the conventional and adaptive steganography are shown in the 3rd and 4th columns, respectively. In these 4 sample video sequences (from top to bottom), PSNR values are 22.10, 21.69, 19.38, and 25.93 dB by the conventional method, while they are 43.28, 42.87, 40.67, and 47.12 dB by the adaptive one.

Table 1. Visual quality evaluation list of the 18 decrypted video sequences with different QL values.

QL	$PSNR$ (dB)					
	Conventional method [7]			Adaptive method		
	Max.	Min.	Avg.	Max.	Min.	Avg.
8	25.93	17.85	21.37	47.16	39.10	42.60
16	31.91	23.82	27.33	53.19	45.12	48.62
32	37.93	29.86	33.34	59.21	51.14	54.63
64	43.97	35.88	39.35	65.23	57.14	60.65
128	49.93	41.83	45.37	71.25	63.18	66.67
256	56.00	47.86	51.39	77.27	69.19	72.69

To evaluate the visual quality of the decrypted video sequences versus the hidden data size, the encrypted video sequences are embedded with different size of data ranged from 108 to 62,208 bits/frame. The QL is set to 8. Figure 6 shows the curves of the average PSNR of the 18 decrypted video sequences versus the hidden data size, where the top and bottom curves are the results using adaptive and conventional methods, respectively. When the PSNR is set to a value not less than 30 dB, the hidden data size is not more than about 3,400 bits/frame in the conventional method while it is about 47,200 bits/frame in the adaptive one. It is about 14 times the data size of the conventional one. Therefore, it is demonstrated that the adaptive steganography-based optical video cryptosystem has a better performance than the conventional steganography-based one.

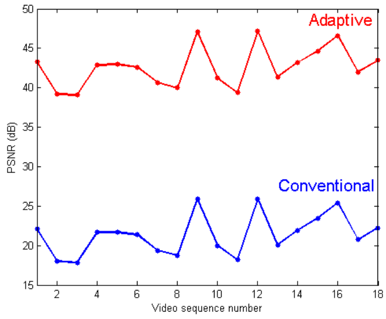


Figure 4. Curves of the PSNR values of the 18 decrypted video sequences (*QL*=8; hidden data=19200 bits/frame).

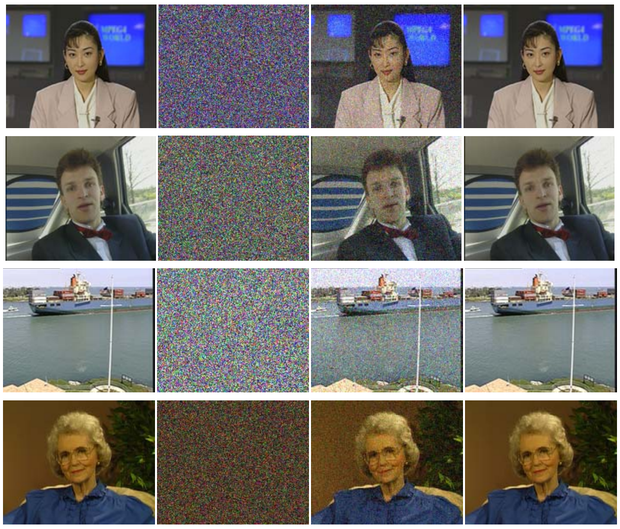


Figure 5. Sample original (the 1st column), encrypted (the 2nd column), and decrypted (the 3rd and 4th columns are using conventional [7] and adaptive methods, respectively) video frames (*QL*=8; hidden data=19200 bits/frame).

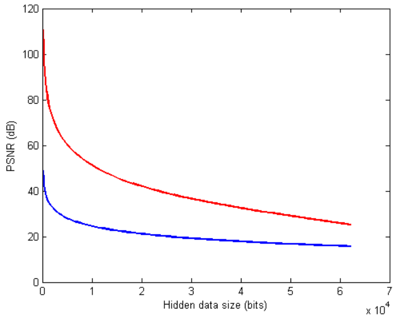


Figure 6. Curves of the average PSNR of the 18 decrypted video sequences versus the hidden data size.

4. Conclusion

In this paper, the optical video cryptosystem based on the adaptive steganography is presented. The double random phase encoding algorithm, the asymmetric encryption method, and the adaptive steganographic data embedding technique are applied in the proposed video cryptosystem. The video sequences are encrypted by the double random phase encoding algorithm. The session keys are ciphered by the asymmetric encryption method. This ciphered data of session keys is embedded into the encrypted video frame by the adaptive steganographic data hiding method. Thus, the session key delivery is achieved by using the adaptive steganography technique. In comparison with the conventional technique, a higher data embedding capacity and visual quality are performed. It is verified that the proposed video cryptosystem provides data hiding characteristics of content-dependence, low distortion, and security. Moreover, the proposed adaptive steganographic technique can be applied to any field that data hiding is needed.

Acknowledgment

This research was supported by the National Science Council, Taiwan, under the grant of NSC97-2221-E-468-006.

References

[1] M. Yang, et al.: "Data-image-video encryption," *IEEE Potentials*, vol. 23, no. 3, pp. 28-34, 2004.

[2] Y.-C. Hu: "High-capacity image hiding scheme based on vector quantization," *Pattern Recognition*, vol. 39, no. 9, pp. 1715-1724, 2006.

[3] C.-C. Chang, et al.: "New image steganographic methods using run-length approach," *Information Sciences*, vol. 176, no. 22, pp. 3393-3408, 2006.

[4] W.-Y. Chen: "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation," *Applied Mathematics and Computation*, vol. 185, no. 1, pp. 432-448, 2007.

[5] Y.-H. Yu, et al.: "A new steganographic method for color and grayscale image hiding," *Computer Vision and Image Understanding*, vol. 107, pp. 183-194, 2007.

[6] P. Refregier and B. Javidi: "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, pp. 767-769, 1995.

[7] G.-S. Lin, et al.: "A public-key-based optical image cryptosystem based on data embedding techniques", *Optical Engineering*, vol. 42, no. 8, pp. 2331-2339, 2003.

[8] R. Tao, et al.: "Double image encryption based on random phase encoding in the fractional Fourier domain," *Optics Express*, vol. 15, pp. 16067-16079, 2007.

[9] L. Chen and D. Zhao: "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Optics Express*, vol. 14, pp. 8552-8560, 2006.

[10] M. Joshi, et al.: "Color image encryption and decryption using fractional Fourier transform," *Optics Communications*, vol. 279, pp. 35-42, 2007.

[11] S. G. Lian, et al.: "Secure advanced video coding based on selective encryption algorithms," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 2, pp. 621-629, 2006.

[12] J. Huang and H. Qian: "Video Encryption for Security Surveillance," *Proc. IEEE International Carnahan Conference on Security Technology*, pp. 207-211, 2007.

[13] C.N. Raju, et al.: "A novel video encryption technique based on secret sharing," *Proc. IEEE International Conference on Image Processing*, pp. 3136-3139, 2008.

[14] R. Iqbal, et al.: "Compressed-Domain Video Processing for Adaptation, Encryption, and Authentication," *IEEE Multimedia*, vol. 15, no. 2, pp. 38-50, 2008.

[15] B. Schneier: *Applied Cryptography*, 2nd ed., Wiley, New York, 1996.

[16] Video Traces Research Group, Arizona State University: http://trace.eas.asu.edu/