A hybrid scheme for encryption and watermarking

Xiaowei Xu,[1α] Scott Dexter[2β] and Ahmet M. Eskicioglu[3β]
[α]The Graduate Center of the City University of New York
365 Fifth Avenue, New York City, NY 10016
[β]Department of Computer and Information Science, CUNY Brooklyn College
2900 Bedford Avenue, Brooklyn, NY 11210

ABSTRACT

Encryption and watermarking are complementary lines of defense in protecting multimedia content. Recent watermarking techniques have therefore been developed independent from encryption techniques. In this paper, we present a hybrid image protection scheme to establish a relation between the data encryption key and the watermark. Prepositioned secret sharing allows the reconstruction of different encryption keys by communicating different activating shares for the same prepositioned information. Each activating share is used by the receivers to generate a fresh content decryption key. In the proposed scheme, the activating share is used to carry copyright or usage rights data. The bit stream that represents this data is also embedded in the content as a visual watermark. When the encryption key needs to change, the data source generates a new activating share, and embeds the corresponding watermark into the multimedia stream. Before transmission, the composite stream is encrypted with the key constructed from the new activating share. Each receiver can decrypt the stream after reconstructing the same key, and extract the watermark from the image. Our presentation will include the application of the scheme to a test image, and a discussion on the data hiding capacity, watermark transparency, and robustness to common attacks.

Key words: multimedia security, encryption, watermarking, secret sharing, singular value decomposition.

1. INTRODUCTION

Encryption and watermarking each provide a different *line of defense* in protecting content. Recent research has therefore followed two different avenues resulting in encryption techniques that are independent from watermarking techniques:

- *Encryption* makes the content unintelligible through a reversible mathematical transformation based on a secret key [1,2]. In secure multimedia content distribution, the audio/visual stream is compressed, packetized and encrypted [3]. One of the most challenging problems in distribution architectures is the delivery of the decryption key.
- *Watermarking (data hiding)* [4,5,6,7] is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia element for different purposes such as copyright protection, access control, and broadcast monitoring.

One possible avenue of research is to establish a relation between the data encryption key and the watermark. A recent method for delivering the keying information in secure multimedia multicast applications suggests the use of a *media dependent* channel [8]. The rekey messages are embedded in the multimedia stream rather than being sent in a separate channel. In a previous work, we proposed a secret sharing scheme to carry the both the rekeying information and copyright/usage rights data as a bit sequence in the transport stream and as a watermark [9]. This paper will present an implementation of this scheme to protect digital images in distribution. We start with a brief introduction to secret sharing.

Secret sharing is an approach for developing multi-party protocols for key establishment [1]. Schemes based on secret sharing not only provide a reliable mechanism for the protection of cryptographic keys without increased risk of disclosure but they also facilitate distributed trust or shared control for critical activities.

[1]xuxw76@yahoo.com, [2]dexter@sci.brooklyn.cuny.edu, [3]eskicioglu@sci.brooklyn.cuny.edu

Definition 1: A (*t, n*) *threshold scheme* ($t \le n$) is a method that enables a trusted dealer to divide a secret S into n secret shares S_i, ($1 \le i \le n$) in such a way that at least t shares are required to reconstruct S. It is assumed that each S_i is securely distributed to user P_i and stored as confidential information.

Definition 2: A *perfect* threshold scheme is a threshold scheme in which the knowledge of (t-1) or fewer shares does not provide any advantage to the opponent to find the secret S.

In Shamir's (*t, n*) threshold scheme [10], the secret S is defined to be the coefficient a_0 of a random (t-1)-degree polynomial $f(x) = (a_{t-1}x^{t-1} + \ldots + a_1x + a_0) \bmod p$ over the finite Galois Field GF(p). The trusted party is responsible for the following tasks in order to divide the secret among n users:

1. Choose a prime p larger than n and the secret S.
2. Construct $f(x)$ by selecting (t-1) random coefficients $a_1, \ldots, a_{t-1}$.
3. Compute the shares S_i by evaluating $f(x)$ at n distinct points.
4. Securely distribute S_i to user P_i ($1 \le i \le n$).

The secret S can be obtained by constructing the polynomial $f(x) = \sum_{i=0}^{t-1} y_i \prod_{0 \le j \le t-1, j \ne i} (x - x_j)/(x_i - x_j)$ from any t of the n shares, and computing $f(0)$.

Definition 3: A *prepositioned secret sharing scheme* is a threshold scheme in which some secret shares are stored by the participants in advance of the activation of the scheme with the added property that even if all of the pieces are exposed in violation of the protocol, the secret key cannot be recovered until some additional information is provided [11,12]. In our implementation of the hybrid scheme, we store t-1 shares as prepositioned information in the receivers to enable the reconstruction of a secret using one more secret share (i.e., the "activating" share).

2. HYBRID SCHEME

Encryption and watermarking are two primary technologies for protecting multimedia content. In the proposed scheme, the basic tasks performed by the sender and receiver are as follows:

Sender side (The sender has the prepositioned secret shares $s_1, s_2, s_{3, \ldots,} s_n$, where $s_i \in Z^+$):

1. Generate s_0, the activating share, and construct K as the shared secret from $s_0, s_1, s_2, s_{3, \ldots,} s_n$.
2. I_W = Embed_WM (I, W), where Embed_WM ( ) is the watermarking embedding function, I is the image, and W is the watermark.
3. C = Encrypt (I_W, K), where Encrypt () is a robust symmetric cipher, and C is the ciphertext message.
4. Send (s_0, C) over the communication channel.

Receiver side (The receiver has the prepositioned secret shares $s_1, s_2, s_{3, \ldots,} s_n$, where $s_i \in Z^+$):

1. Receive (s_0, C) over the communication channel.
2. Reconstruct K from $s_0, s_1, s_2, s_{3, \ldots,} s_n$.
3. I'_W = Decrypt (C, K), where Decrypt () is the symmetric cipher to recover the watermarked image I'_W.
4. W' = Extract_WM (I'_W), where Extract_WM () is the watermark extraction function.

The above tasks require three tools: a key generator, a cipher, and a watermarking scheme. In our experiments, we used the following software:

- For the construction of a shared secret symmetric cipher, the solution of a linear system of equations is needed in finite arithmetic. NTL [13], an appropriate tool for this purpose, is free software that can be used according to the terms of the GNU General Public License. It is a portable C++ library that provides data structures and algorithms

for arbitrary length integers; for vectors, matrices, and polynomials over the integers and over finite fields; and for arbitrary precision floating point arithmetic.

- The Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS) (FIPS Publication 197) that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. The AES algorithm is a symmetric block cipher that is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. A public-domain implementation of the 128-bit AES cipher is written by Szymon Stefanek [14].
- A watermarking algorithm consists of the watermark structure, an embedding algorithm and an extraction, or a detection, algorithm. Watermarks can be embedded in the pixel domain or a transform domain such as the DCT or discrete wavelet. Singular Value Decomposition (SVD) is a recent approach used in watermarking. Software for SVD is available at Numerical Recipes [15].

There are several uses of the proposed hybrid scheme. In copyright or content protection systems, the most critical information that needs to be carried from the source to the receivers includes *time stamps*, *Copy Control Information (CCI)*, and *copyright ownership data*. If this information needs to change from one multimedia element (image, video, etc.) to another, how can this change be induced? Secret sharing offers a solution, providing a means to change the watermark in the multimedia content be sending a new activating share to the population of receivers.

Example: Assume that we have the 3 pieces of information given in Figure 1. Each piece needs to be carried with a different image that will be delivered. We carry the information as a bit sequence in the activating share, and also embed the same information in the content as a visual watermark.

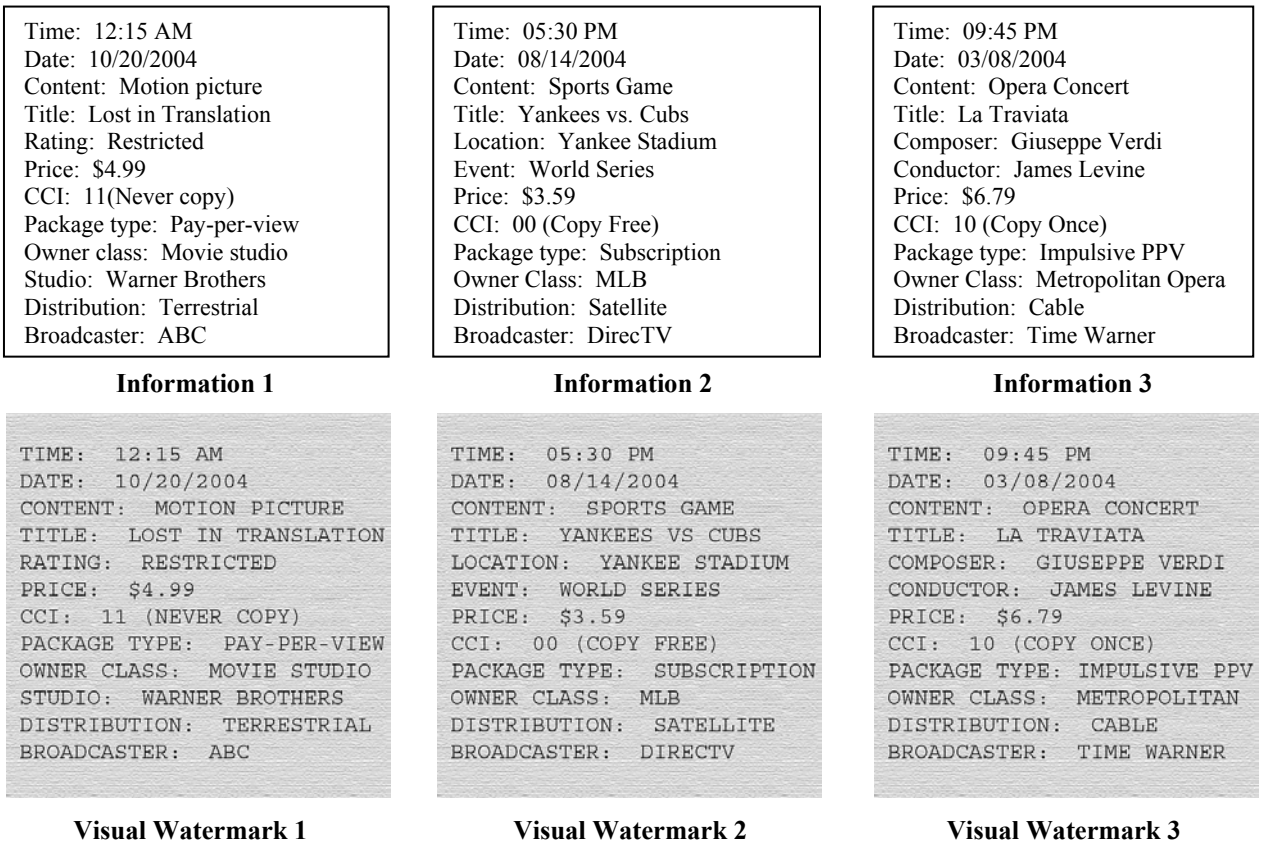


Figure 1. Copyright/usage rights information and corresponding visual watermarks

A similar approach is used in the Digital Transmission Content Protection (DTCP) Specification [16] that defines a cryptographic protocol for protecting audio/visual entertainment content from illegal copying, intercepting and tampering as it traverses digital buses such as the IEEE 1394 interface. For the transfer of the CCI from a source device to a sink device, two methods can be used:

- The Encryption Mode Indicator (EMI): The Copy Generation Management System (CGMS) bits are carried via the most significant two bits of the synch field of the isochronous packet header defined by the interface specification. The EMI allows immediate access to CGMS information without extracting embedded CCI. The CGMS information is used as an argument in the key exchange protocol to generate the keys for encrypting the content across the interface. Modifying the EMI bits in an unauthorized way will result in erroneous decryption of the content.
- Embedded CCI: The CCI is carried as part of the multimedia content stream. Some transport formats (including MPEG) include fields allocated for the CCI associated with the stream. The CCI can also be embedded as a watermark directly into the content.

3. SVD-BASED WATERMARKING SCHEME

Although any other watermark embedding and extraction algorithm can be used, we implemented an SVD-based watermarking scheme.

Every real matrix A can be decomposed into a product of 3 matrices $A = U\Sigma V^T$, where U and V are orthogonal matrices, $U^TU = I$, $V^TV = I$, and Σ = diag (λ_1, λ_2, ...). The diagonal entries of Σ are called the singular values (SVs) of A, the columns of U are called the left singular vectors of A, and the columns of V are called the right singular vectors of A. This decomposition is known as the *Singular Value Decomposition* of A, and can be written as

$$A = \sum_{i=1}^{r} \lambda_i U_i V_i^T$$

where r is the rank of matrix A. Note that each SV specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image.

The SVD is one of the most useful tools of linear algebra with several applications to multimedia including image compression [17,18,19,20,21,22,23,24,25], signal processing [26,27,28,29], and watermarking [30,31,32].

The SVD of the cover image A and the visual watermark W are, respectively, $A = U_a \Sigma_a V_a^T$ and $W = U_W \Sigma_W V_W^T$. $\lambda_i, i = 1,..., k$ denote the SVs of the cover image, and $\lambda_{wi}, i = 1,..., l$ denote the SVs of the visual watermark. The scaling factor α is chosen to be the constant 0.1.

Watermark Embedding

The watermark is embedded by using the SVs of the watermark to modify the corresponding SVs of the cover image, yielding distorted SVs λ_i^d:

$$\lambda_i^d = \lambda_i + \alpha\lambda_{wi}$$

The watermarked image is then constructed as:

$$A^d = U_A \Sigma_A^d V_A^T$$

Because the watermark W is embedded in A, the size of W should be less than or equal to the size of A, but the rank of W may be smaller, equal to, or greater than the rank of A.

Watermark Extraction

The watermark extraction process is the inverse of the embedding process:

$$\lambda_{wi}^{d} = \frac{\lambda_i^{d} - \lambda_i}{\alpha}.$$

The extracted singular values are used with the orthogonal matrices U_W and V_W to construct the visual watermark:

$$W_{extracted} = U_W \Sigma_W^{d} V_W^{T}.$$

4. WATERMARKING AND ENCRYPTION OF IMAGES

Our experiments included several cover images and visual watermarks. We will present the results for one cover image and one visual watermark. In this experiment, we used three 128-bit shares (the activating share, and 2 prepositioned shares) to construct the encryption key. The shares and the constructed key are given in Table 1. The encryption key is computed as part of the solution of the linear system of three equations with three unknowns, i.e.,

$$f(x) = (a_2x^2 + a_1x + a_0) \mod p$$

$$y_0 = a_2(x_0)^2 + a_1x_0 + a_0 \mod p$$
$$y_1 = a_2(x_1)^2 + a_1x_1 + a_0 \mod p$$
$$y_2 = a_2(x_2)^2 + a_1x_2 + a_0 \mod p$$

To find the solution (a_2, a_1, a_0), the NTL generates an appropriate value of p. Once the coefficients of the 2nd degree polynomial are determined, we obtain $f(0)=a_0$.

Table 1. Shares and secret encryption key

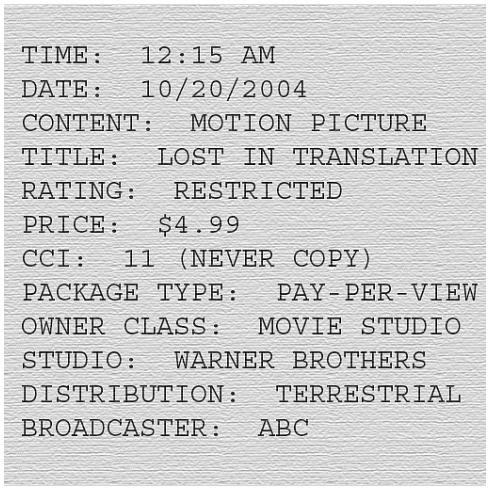
Share	Value
Activating (x_0,y_0)	61 f4 a7 d4 a8 72 70 e0 04 09 8f 64 96 2d 14 be
Prepositioned 1 (x_1,y_1)	01 3c 75 48 98 59 71 c9 46 c1 71 da a6 40 08 b4
Prepositioned 2 (x_2,y_2)	0c 02 52 fd 68 fc 80 68 82 82 a4 51 ed 8b 73 e0
Encryption key (a_0)	ed 66 05 2b 23 ea 21 48 4e 6a 82 c0 83 dd 77 8f

Figure 2 shows the 512x512 gray scale cover image Lena, the 512x512 gray scale Visual Watermark 1, the watermarked Lena, and the extracted visual watermark before any attacks. The information contained in Visual Watermark 1 is carried in the activating share.

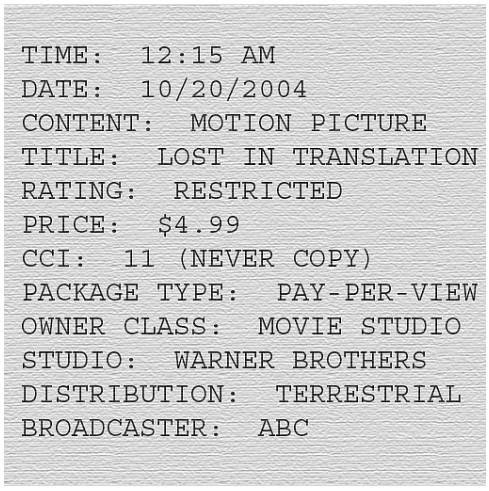
The length and binary representation of each piece of information (time, date, content, etc.) is included in Table 2. As there is no industry standard, the binary values are arbitrarily chosen to guarantee uniqueness in each field.

(a)

(b)



(c)



(d)

Figure 2. (a) Cover image Lena, (b) Watermarked Lena, (c) Visual watermark, (d) Extracted watermark.

Table 2. Representation of information in Visual Watermark 1

Field	Value	# of allocated bits	Binary representation
Time/Day/Month/Year	12:15/20/10/2004	32	01100001111101001010011111010 10
Content	Motion picture	8	10101000
Title	Lost in Translation	28	0111001001110000111000000000
Rating	R	4	0100
Price	4.99	14	00001001100011
CCI	11	2	11
Package type	Pay-per-view	8	011001000
Owner class	Movie studio	8	10010110
Studio	Warner brothers	8	00101101
Distribution	Terrestrial	8	00010100
Broadcaster	ABC	8	10111110

The encryption key in Table 1 was used to protect the watermarked Lena in transmission. The watermarked and encrypted image is shown in Figure 3.

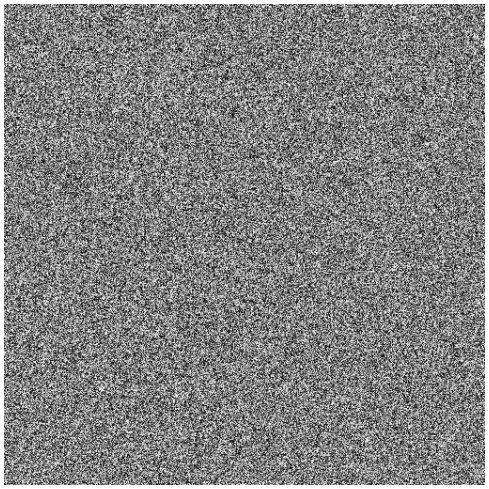
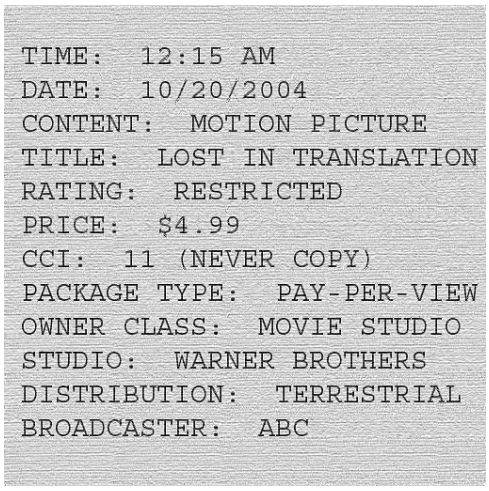


Figure 3. Watermarked and encrypted Lena

5. ATTACKS ON WATERMARKED IMAGES

The SVD-based watermarking scheme was tested using seven attacks. The chosen attacks were JPEG compression, JPEG 2000 compression, Gaussian blur, Gaussian noise, rescaling, rotation and cropping. All the attacks were performed using the freeware *xnview* software.

Figure 4 shows the first attack (i.e., JPEG compression) on the cover image, and the watermark extracted after the attack. The attack was to compress Lena at 30:1 ratio.



(a) (b)

Figure 4. (a) JPEG compressed Lena (30:1), (b) Extracted watermark

Figure 5 shows the second attack (i.e., JPEG 2000 compression) on the cover image, and the watermark extracted after the attack. The attack was to compress Lena at 50:1 ratio.

(a) (b)

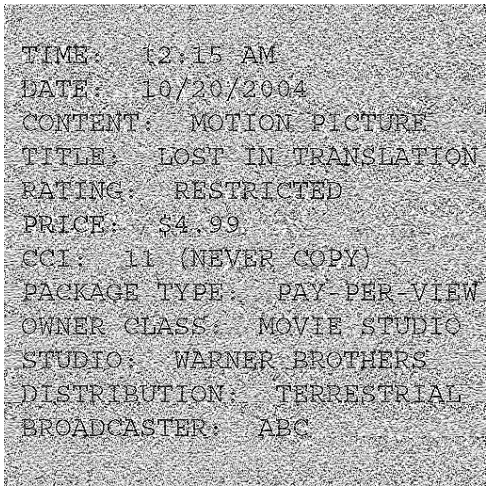
Figure 5. (a) JPEG 2000 compressed Lena (50:1), (b) Extracted watermark

Figure 6 shows the third attack (i.e., Gaussian blur) on the cover image, and the watermark extracted after the attack. The attack was to blur Lena using a radius of 3.

(a) (b)

Figure 6. (a) Gaussian blurred Lena (radius=3), (b) Extracted watermark

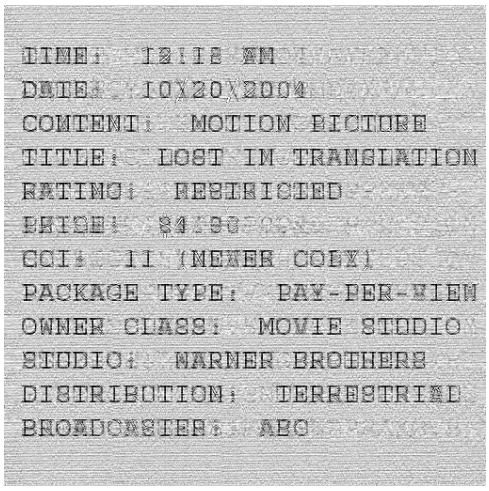
Figure 7 shows the fourth attack (i.e., Gaussian noise) on the cover image, and the watermark extracted after the attack. The attack was to introduce noise to Lena using the parameter 0.2.



(a) (b)

Figure 7. (a) Gaussian noisy Lena (0.2), (b) Extracted watermark

Figure 8 shows the fifth attack (i.e., rescaling) on the cover image, and the watermark extracted after the attack. The attack was to rescale Lena to quarter of its size, and then back to its original size using bilinear interpolation.

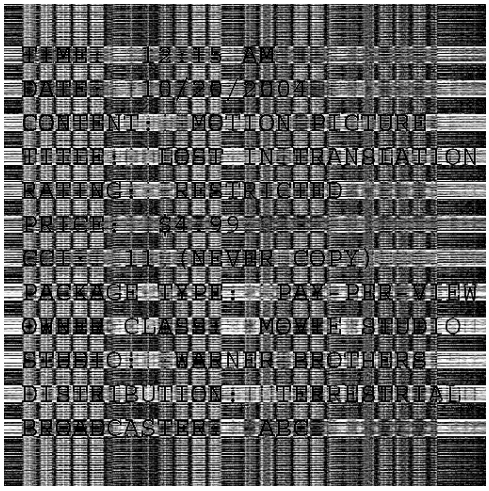


(a) (b)

Figure 8. (a) Rescaled Lena (512x512 → 256x256 → 512x512), (b) Extracted watermark

Figure 9 shows the sixth attack (i.e., rotation) on the cover image, and the watermark extracted after the attack. The attack was to rotate Lena 20 degrees clockwise first, and then to rotate it back to its original position using bilinear interpolation.

(a)

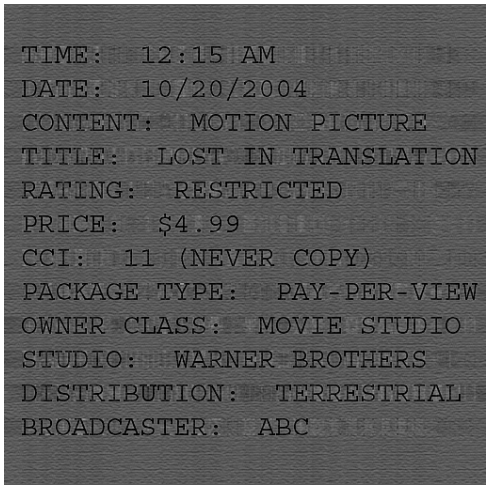


(b)

Figure 9. (a) Rotated Lena (20 degrees), (b) Extracted watermark

Figure 10 shows the seventh attack (i.e., cropping) on the cover image, and the watermark extracted after the attack. The attack was to crop the right half of Lena. In watermark extraction, the missing half was replaced with the right half of unwatermarked Lena.

(a)



(b)

Figure 10. (a) Cropped Lena (right half), (b) Extracted watermark

Although the image loses its entire commercial value after each attack, the watermark is extracted in a reliable way. The worst attack appears to be the rotation of the image, which results in a very noisy visual watermark. Even in this case, the information is still legible.

6. CONCLUSIONS

We presented a hybrid image protection scheme that integrates encryption and watermarking. It can be used in unicast, broadcast and multicast applications of multimedia. Encryption is needed to prevent unauthorized access to multimedia content, and watermarking is used for copyright protection. The scheme is based on prepositioned secret sharing that allows the construction of fresh encryption keys by communicating different activating shares. A part of the activating share can be used to carry copyright or usage rights data. In our experiments, we used the entire 128-bit activating share for this purpose. This data was also embedded into multimedia content as a watermark. On receipt of the activating share and the encrypted content, each receiver can construct the decryption key, decrypt the content and extract the watermark.

The SVD-based watermarking algorithm was resistant to seven attacks (JPEG compression, JPEG 2000 compression, Gaussian blur, Gaussian noise, rescaling, rotation and cropping) commonly used to evaluate the robustness of watermarking schemes. The embedded watermark may include the time and date of broadcast, a brief description of content, the CCI, and information about the package type, owner, broadcaster and distribution mechanism.

Each new activating share provides the opportunity to change the watermark in the content. In some broadcast systems, the decryption key changes every few seconds. In such systems, as the watermark does not need to change at that frequency, there needs to be a different mechanism to trigger the change in the watermark.

The watermarking scheme used in our implementation (or any other SVD-based algorithm) can be primarily used for copyright protection purposes. Watermark extraction requires the value of the scaling factor, the singular values of the unwatermarked cover image, and the left and right singular vectors of the visual watermark. For different images and watermarks, this information cannot be stored in receivers with limited storage capacity.

In watermarking schemes, either the embedded watermark or its representation needs to be a secret. For example, when a new movie is released on a DVD, its CCI would normally be "never copy." This information is known but the way it is represented as a watermark should be securely kept. As the activating share contains full information about the watermark, several methods can be considered to hide the mapping between the copyright and usage rights information and the actual watermark. A visual watermark serves as one method of hiding this information.

REFERENCES

[1] J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[2] B. Schneier, *Applied Cryptography*, John Wiley and Sons, Inc, 1996.

[3] A. M. Eskicioglu, J. Town and E. J. Delp, "Security of Digital Entertainment Content from Creation to Consumption," *Signal Processing: Image Communication, Special Issue on Image Security*, Vol. 18, Issue 4, pp. 237-262, April 2003.

[4] S. Katzenbeisser and F. A. P. Petitcolas (Editors), *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, Inc., 2000.

[5] N. F. Johnson, Z. Duric, S. Jajodia, *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures*, Kluwer Academic Publishers, 2000.

[6] I. J. Cox, M. L. Miller and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2001.

[7] M. Arnold, M. Schmucker and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*, Artech House, Inc., 2003.

[8] J. Song, R. Poovendran, W. Trappe, K. J. R. Liu, "A Dynamic Key Distribution Scheme Using Data Embedding for Secure Multimedia Multicast," *Proceedings of SPIE Security and Watermarking for Multimedia Contents III*, Vol. 4314, San Jose, CA, January 22-25, 2001, pp. 618-628.

[9] A. M. Eskicioglu, E. J. Delp and M. R. Eskicioglu, "New Channels for Carrying Copyright and Usage Rights Data in Digital Multimedia Distribution," *Proceedings of the International Conference on Information Technology: Research and Education*, pp. 94-98, Newark, NJ, August 11-13, 2003.

[10] A. Shamir, "How to share a secret," *CACM*, 22(11), pp. 612-613, November 1979.

[11] G. J. Simmons, "How to (really) share a secret," *Advances in Cryptology – CRYPTO '88 Proceedings*, pp. 390-448, Springer-Verlag, 1990.

[12] G. J. Simmons, "Prepositioned shared secret and/or shared control schemes," *Advances in Cryptology – EUROCRYPT '89 Proceedings*, pp. 436-467, Springer-Verlag, 1990.

[13] Available at http://shoup.net/ntl

[14] Available at http://www.esat.kuleuven.ac.be/~rijmen/rijndael

[15] Available at http://www.nr.com

[16] Available at www.dtcp.com

[17] H. C. Andrews and C. L. Patterson, "Outer Product Expansions and Their Uses in Digital Image Processing," *IEEE Transactions on Computers,* 25(2), February 1976, pp. 140-148.

[18] H. C. Andrews and C. L. Patterson, "Singular value Decomposition (SVD) Image Coding," *IEEE Transactions on Communications*, 24(4), April 1976, pp. 425-432.

[19] N. Garguir, "Comparative Performance of SVD and Adaptive Cosine Transform in Coding Images," *IEEE Transactions on Communications*, 27(8), August 1979, pp. 1230-1234.

[20] D. P. O'Leary and S. Peleg, "Digital Image Compression by Outer Product Expansion," *IEEE Transactions on Communications*, 31(3), March 1983, pp. 441-444.

[21] T. Saito, T. Komatsu and H. Harashima, "Improvement on Singular Value Decomposition Vector Quantization," *Electronics and Communications in Japan*, Part 1, 73(2), 1990, pp. 11-20.

[22] C. S. McGoldrick, W. J. Dowling and A. Bury, "Image Coding Using the Value Decomposition and Vector Quantization," *5th International Conference on Image Processing and Its Applications*, London, UK, July 4-6, 1995, pp. 296-300.

[23] J. F. Yang and C. L. Lu, "Combined Techniques of Singular Value Decomposition and Vector Quantization," *IEEE Transactions on Image Processing*, 4(8), August 1995, pp. 1141-1146.

[24] P. Waldemar and T. A. Ramstad, "Hybrid KLT-SVD Image Compression," *1997 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 4, Munich, Germany, April 21-24, 1997, pp. 2713-2716.

[25] S. O. Aase, J. H. Husoy and P. Waldemar, "A Critique of SVD-Based Image Coding Systems," *1999 IEEE International Symposium on Circuits and Systems VLSI*, Vol. 4, Orlando, FL, May 1999, pp. 13-16.

[26] K. Konstantinides and G. S. Yovanof, "Improved Compression Performance Using SVD-Based Filters for Still Images, *SPIE Proceedings*, Vol. 2418, San Jose, CA, February 7-8, 1995, pp. 100-106.

[27] K. Konstantinides and G. S. Yovanof, "Application of SVD-Based Spatial Filtering to Video Sequences," *1995 IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 4, Detroit, MI, May 9-12, 1995, pp. 2193-2196.

[28] K. Konstantinides, B. Natarajan and G. S. Yovanof, "Noise Estimation and Filtering Using Block-Based Singular Value Decomposition, *IEEE Transactions on Image Processing*, 3(3), March 1997, pp. 479-483.

[29] R. Karkarala and P. O. Ogunbona, "Signal Analysis Using a Multiresolution Form of the Singular Value Decomposition, *IEEE Transactions on Image Processing*, 10(5), May 2001, pp. 724-735.

[30] V. I. Gorodetski, L. J. Popyack, V. Samoilov and V. A. Skormin, "SVD-based Approach to Transparent Embedding Data into Digital Images," *International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001)*, St. Petersbug, Russia, May 21-23, 2001.

[31] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, 4(1), March 2002, pp.121-128.

[32] D. V. S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition," *Proceedings of 45th IEEE Midwest Symposium on Circuits and Systems*, Tulsa, OK, August 2002, pp. 264-267.