# Authenticating Cropped and Resized Images Using Distributed Source Coding and Expectation Maximization

Yao-Chung Lin, David Varodayan, and Bernd Girod

Information Systems Laboratory, Stanford University, Stanford, CA 94305

## ABSTRACT

Media authentication is important in content delivery via untrusted intermediaries, such as peer-to-peer (P2P) file sharing. Many differently encoded versions of a media file might exist. Our previous work applied distributed source coding not only to distinguish the legitimate diversity of encoded images from tampering but also localize the tampered regions in an image already deemed to be inauthentic. The authentication data supplied to the decoder consisted of a Slepian-Wolf encoded image projection.

We extend our scheme to authenticate cropped and resized images using an Expectation Maximization algorithm. Experimental results demonstrate that the proposed algorithm can distinguish legitimate encodings of authentic cropped and resized images from illegitimately modified versions using authentication data of less than 250 bytes.

**Keywords:** Image authentication, distributed source coding, Expectation Maximization

## 1. INTRODUCTION

Media authentication is important in content delivery via untrusted intermediaries, such as peer-to-peer (P2P) file sharing or P2P multicast streaming. In these applications, many differently encoded versions of the original file might exist. Moreover, transcoding and bitstream truncation at intermediate nodes might give rise to further diversity. But intermediaries might also tamper with the media for many reasons, such as interfering with the distribution of a particular file, piggybacking unauthentic content, or generally discrediting a distribution system. In previous work, we applied distributed source coding (DSC) to image authentication to distinguish the diversity of legitimate encodings from malicious manipulation[1] and demonstrated that the same framework can localize tampering in images deemed to be inauthentic.[2,3] In this paper, we extend our image authentication scheme to be robust to cropping and resizing. Our approach is to let the authentication decoder learn stretching and shifting parameters using an Expectation Maximization[4] (EM) algorithm.

Past media authentication approaches fall into two groups: watermarks and media hashes. A "fragile" watermark can be embedded into the host signal waveform without perceptual distortion.[5,6] Users can confirm the authenticity by extracting the watermark from the received content. The watermark should survive lossy compression, but should "break" as a result of malicious manipulation. Unfortunately, watermarking authentication is not backward compatible with previously encoded contents; unmarked contents cannot be authenticated later. Embedded watermarks might also increase the bit-rate required when compressing a media file.

Media hashing[7,8] achieves authentication of previously encoded media by using an authentication server to supply authentication data to the user. Media hashes are inspired by cryptographic digital signatures,[9] but unlike cryptographic hash functions, media hash functions offer proof of perceptual integrity. Using a cryptographic hash, a single bit difference leads to an entirely different hash value. If two media signals are perceptually indistinguishable, they should have identical hash values. A common approach of media hashing is extracting features which have perceptual importance and should survive compression. The authentication data are generated by compressing the features or generating their hash values. The user checks the authenticity of the received content by comparing the features or their hash values to the authentication data.

Further author information: E-mail: {yao-chung.lin, varodayan, bgirod}@stanford.edu, Telephone: +1 650 723 3476, Fax: +1 650 724 3648.

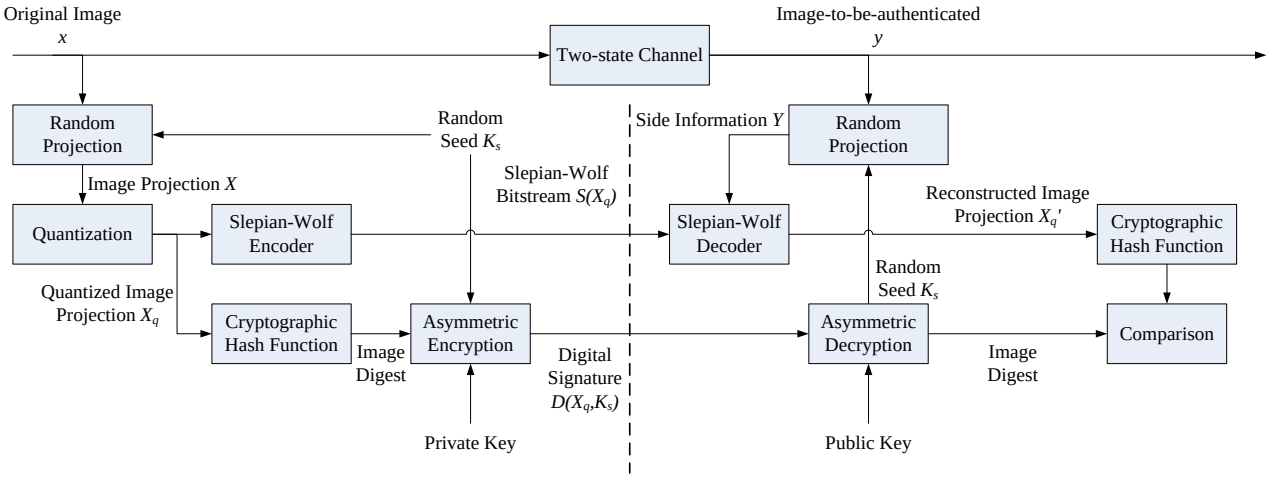



Figure 1. Image authentication system based on distributed source coding.

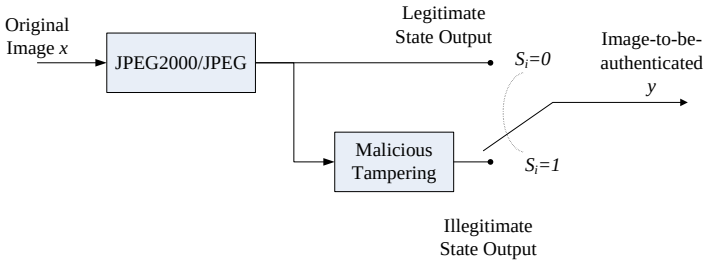



Figure 2. Space-varying two-state lossy channel.

Section 2 reviews our image authentication system using distributed source codes,[1] an extension of media hashing. It has similarities with secure biometric authentication[10,11] and some semi-fragile watermarking schemes.[12] In Section 3, we describe a model for cropping and resizing and introduce our extension for image authentication with parameter learning. The EM algorithmic details are given in Section 4. Simulation results in Section 5 show that the proposed scheme can distinguish between authentic encodings of cropped and resized images and illegitimately modified versions.

## 2. REVIEW OF IMAGE AUTHENTICATION WITH DSC

Fig. 1 is the block diagram for our earlier image authentication scheme[1] as well as the current work. We denote the source image as $x$. We model the image-to-be-authenticated $y$ by way of the space-varying two-state lossy channel in Fig. 2. The legitimate state of the channel performs lossy JPEG2000 or JPEG compression and reconstruction with peak signal-to-noise ratio (PSNR) of 30 dB or better. The illegitimate state additionally includes malicious tampering. The channel state variable $S_i$ is defined per nonoverlapping 16x16 block of image $y$. If any pixel in block $B_i$ is tampered, $S_i = 1$; otherwise, $S_i = 0$.

We now review the authentication system. The left-hand side of Fig. 1 shows that a pseudorandom projection (based on a randomly drawn seed $K_s$) is applied to the original image $x$ to produce projection coefficients $X$, which are quantized to $X_q$. The authentication data comprise two parts, both derived from $X_q$. The Slepian-Wolf bitstream $S(X_q)$ is the output of a Slepian-Wolf encoder based on rate-adaptive low-density parity-check (LDPC) codes.[13] The much smaller digital signature $D(X_q, K_s)$ consists of the seed $K_s$ and a cryptographic hash value of $X_q$ signed with a private key. The authentication data are generated by a server upon request. Each response uses a different random seed $K_s$, which is provided to the decoder as part of the authentication data. This prevents an attack which simply confines the tampering to the nullspace of the projection. Based on the random seed, for each 16x16 nonoverlapping block $B_i$, we generate a 16x16 pseudorandom matrix $P_i$ by

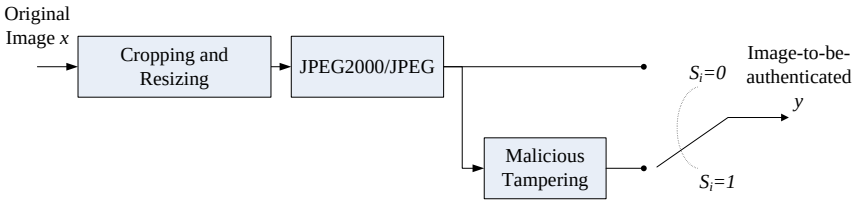



Figure 3. Space-varying two-state lossy channel with cropping and resizing.

drawing its elements independently from a Gaussian distribution $\mathcal{N}(1, \sigma^2)$ and normalizing so that $||P_i||_2 = 1$. We choose $\sigma = 0.2$ empirically. The inner product $\langle B_i, P_i \rangle$ is an element of $X$, quantized to an element of $X_q$.

The authentication decoder, in the right-hand side of Fig. 1, seeks to authenticate the image $y$ with authentication data $S(X_q)$ and $D(X_q, K_s)$. It first projects $y$ to $Y$ in the same way as during authentication data generation. A Slepian-Wolf decoder reconstructs $X_q{}'$ from the Slepian-Wolf bitstream $S(X_q)$ using $Y$ as side information. Decoding is via joint bitplane LDPC belief propagation[14] initialized according to the known statistics of the legitimate channel state at the worst permissible quality for the given original image. Then the image digest of $X_q{}'$ is computed and compared to the image digest, decrypted from the digital signature $D(X_q, K_s)$ using a public key. If these two image digests are not identical, the receiver declares image $y$ to be inauthentic. If they match, then $X_q$ has been recovered. To confirm the authenticity of $y$, the receiver verifies that the empirical conditional entropy $H_{\text{emp}}(X_q|Y)$ (based on the legitimate channel model) is less than a certain threshold.

Since this second-pass comparison uses all available information, the threshold for $H_{\text{emp}}(X_q|Y)$ specifies how statistically similar the image-to-be-authenticated must be to the original to be declared authentic. But the rate of the Slepian-Wolf bitstream $S(X_q)$ determines whether the quantized image projection $X_q$ is recovered at all.[15] Accordingly, at the encoder, we select a Slepian-Wolf bit-rate just sufficient to successfully decode with both legitimate 30 dB JPEG2000 and JPEG reconstructed versions of $x$. At the decoder, we choose a threshold for $H_{\text{emp}}(X_q|Y)$ for the second-pass comparison to distinguish between the different joint statistics induced in the images by the legitimate and illegitimate channel states.

## 3. CROPPING AND RESIZING MODEL

In this paper, we replace the two-state lossy channel in Fig. 2 with the one in Fig. 3. Now both the legitimate and illegitimate states of the channel are affected by a cropping and resizing adjustment. In the legitimate state, we model the channel as

$$\begin{aligned} y(m_1, m_2) &= x(n_1, n_2) + z(m_1, m_2), \\ \text{with } n_1 &= \alpha_1 m_1 + \beta_1, \\ n_2 &= \alpha_2 m_2 + \beta_2, \end{aligned}$$

where $(\alpha_1, \alpha_2)$ and $(\beta_1, \beta_2)$ are stretching and shifting parameters, respectively, and $z$ is noise introduced by compression and reconstruction. Fig. 4(a) gives an example for source image "Lena" at 8-bit 512x512 original resolution. The legitimate $y$ in Fig. 4(b) is first cropped to 480x480 resolution starting at pixel (25,25) from the top left corner, then resized to 512x512, and finally JPEG2000 compressed and reconstructed at 30 dB PSNR. In this case, $\alpha_1 = \alpha_2 = \frac{480}{512} = 0.94$ and $\beta_1 = \beta_2 = 24$. The illegitimate $y$ in Fig. 4(c) additionally includes malicious tampering. Fig. 4(d) shows the illegitimate $y$ realigned to the original, with channel states $S_i$ labeled red if illegitimate and blue if cropped out in $y$. The remainder are legitimate cropped-in states.

The image authentication system described in Section 2 cannot authenticate legitimate images subject to the cropping and resizing adjustment just described, because the side information is not synchronized with the corresponding authentication data. Other approaches in prior art involve generating geometric-distortion resilient features that serve as authentication data.[16,17] These features are usually derived from large portions of the image or even the whole image. Therefore, the authentication is less precise, i.e. a small amount of tampering cannot be detected. We instead propose that the authentication decoder estimate the stretching and shifting parameters directly from the Slepian-Wolf bitstream $S(X_q)$ and the image-to-be-authenticated $y$ using

(a) (b) (c) (d)

Figure 4. Test image "Lena" (a) $x$ original, white box indicates the cropping boundary (b) $y$ in legitimate state, (c) $y$ in illegitimate state, (d) channel states $S_i$ (red: illegitimate, blue: cropped-out) associated with the 16x16 blocks of aligned output in (c).

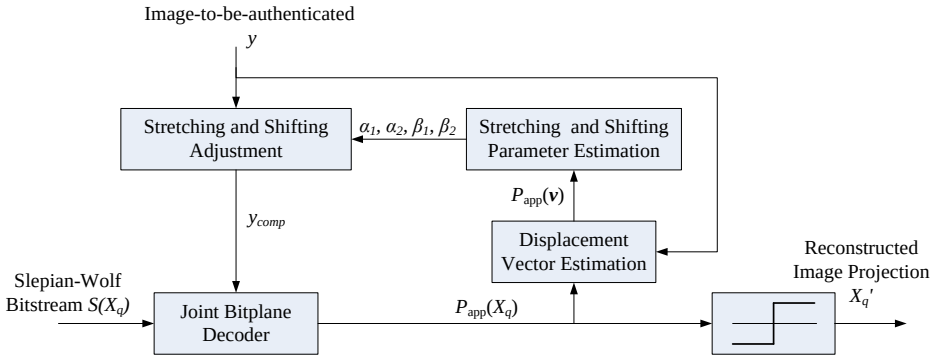



Figure 5. Stretching and shifting parameter learning Slepian-Wolf decoder.

an EM algorithm. This combination of unsupervised learning with distributed source decoding is closely related to the learning of motion vectors in distributed video coding.[18]

## 4. EXPECTATION MAXIMIZATION

The introduction of learning to the system in Fig. 1 requires a modification of the Slepian-Wolf decoder block from a joint-bitplane LDPC decoder[14] to the stretching-and-shifting-learning Slepian-Wolf decoder shown in Fig. 5. As before, it takes the Slepian-Wolf bitstream $S(X_q)$ and the image-to-be-authenticated $y$ and yields the reconstructed image projection $X_q{}'$. But it now does this via an EM algorithm. The E-step updates the *a posteriori* probability mass functions (pmf) $P_{\text{app}}(X_q)$ using the joint bitplane decoder and also estimates displacement vectors for a subset of reliably-decoded projection pixels. The M-step updates the stretching and shifting parameters based on the displacement vector distributions, denoted $P_{\text{app}}(\mathbf{v})$ in Fig. 5. This loop of EM iterations terminates when hard decisions on $P_{\text{app}}(X_q)$ satisfy the constraints imposed by $S(X_q)$.

In the E-step, we fix stretching parameters $(\alpha_1, \alpha_2)$ and shifting parameters $(\beta_1, \beta_2)$ at their current hard estimates. Inverse stretching and shifting is applied to the image $y$ to obtain a compensated image $y_{\text{comp}}$. If the stretching and shifting parameters are accurate, $y_{\text{comp}}$ would be closely aligned to the original image $x$ in the cropped-in region. We derive intrinsic pmfs for the image projection pixels $X_q$ as follows. In the cropped-in region, we use Gaussian distributions centered at the random projection values of $y_{\text{comp}}$, and in the cropped-out region, we use uniform distributions. Then, we run three iterations of joint bitplane LDPC decoding on the intrinsic pmfs with the Slepian-Wolf bitstream $S(X_q)$ to produce extrinsic pmfs $P_{\text{app}}([X_q]_i = x_q)$.

We estimate displacement vectors for those projection pixels for which $\max_{x_q} P_{\text{app}}([X_q]_i = x_q) > T = 0.995$, denoting this set of reliably-decoded projection indices as $\mathcal{C}$. We also denote the maximizing reconstruction value $x_q$ to be $[x_q^{\max}]_i$. (To guarantee that $\mathcal{C}$ is nonempty, we make sure to encode a small portion of the quantized image projection $X_q$ with degree-1 syndrome bits. The decoder knows those values with probability 1 and

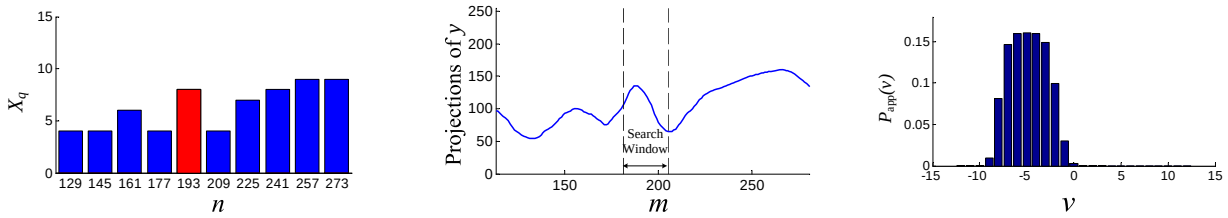



Figure 6. Example of displacement vector estimation in 1-D.

includes their indices in $\mathcal{C}$.) We obtain displacement vector pmfs $P_{\text{app}}(\mathbf{v}^{(i)})$ for these pixels by maximizing the following log-likelihood function:

$$\begin{aligned} L(\alpha_1,\alpha_2,\beta_1,\beta_2) &\equiv \sum_{i\in\mathcal{C}} \log P([x_q^{\max}]_i, \mathbf{n}^{(i)}, y; \alpha_1,\alpha_2,\beta_1,\beta_2) \\ &= \sum_{i\in\mathcal{C}} \log \left( \sum_{\mathbf{m}^{(i)}} P([x_q^{\max}]_i, \mathbf{n}^{(i)}, y|\mathbf{m}^{(i)}; \alpha_1,\alpha_2,\beta_1,\beta_2) P(\mathbf{m}^{(i)}) \right), \end{aligned}$$

where $\mathbf{n}^{(i)} = (n_1^{(i)}, n_2^{(i)})$ is the set of top-left co-ordinates of the 16x16 projection blocks $B_i$ in the original image $x$, and the latent variable $\mathbf{m}^{(i)} = (m_1^{(i)}, m_2^{(i)})$ represents the corresponding set of co-ordinates in $y$. Note that $P([x_q^{\max}]_i, \mathbf{n}^{(i)}, y; \alpha_1,\alpha_2,\beta_1,\beta_2)$ is the joint probability of observations $[x_q^{\max}]_i, \mathbf{n}^{(i)}$, and $y$, parameterized by $\alpha_1,\alpha_2,\beta_1$, and $\beta_2$. The latent variable update can be written as

$$\begin{aligned} Q_i(\mathbf{m}) &:= P(\mathbf{m}^{(i)} = \mathbf{m}|[x_q^{\max}]_i, y, \mathbf{n}^{(i)}; \alpha_1,\alpha_2,\beta_1,\beta_2) \\ &= P(\mathbf{v}^{(i)} = \mathbf{m} - \mathbf{n}^{(i)}|[x_q^{\max}]_i, y, \mathbf{n}^{(i)}; \alpha_1,\alpha_2,\beta_1,\beta_2) \\ &\equiv P_{\text{app}}(\mathbf{v}^{(i)} = \mathbf{m} - \mathbf{n}^{(i)}). \end{aligned}$$

In this way, we associate a displacement vector pmf $P_{\text{app}}(\mathbf{v}^{(i)})$ with each projection pixel $[X_q]_i$ in $\mathcal{C}$, in a process similar to learning motion vectors in distributed video coding.[18] For the projection pixel $[X_q]_i$, we produce the pmf $P_{\text{app}}(\mathbf{v}^{(i)} = \mathbf{v})$ by matching the pixel to projections obtained from $y$ through vectors $\mathbf{v}$ over a small search window. Specifically, $P_{\text{app}}(\mathbf{v}^{(i)} = \mathbf{v})$ is proportional to the integral over the quantization interval of $[x_q^{\max}]_i$ of a Gaussian centered at the projection of a block displaced by vector $\mathbf{v}$ in the image $y$. Fig. 6 gives a 1-D example of the resulting distribution of $Q_i(\mathbf{m})$ for the projection pixel at $\mathbf{n}^{(i)} = 193$. The quantized projection pixel shown as red bar in Fig. 6(a) is matched against the projections of $y$ in Fig. 6(b) over the search window to obtain $P_{\text{app}}(\mathbf{v}) \propto \int_{x:Q(x)=[x_q^{\max}]_i} P(x|y(\mathbf{n^{(i)}} + \mathbf{v}))dx$ in Fig. 6(c).

In the M-step, we re-estimate the parameters $(\alpha_1,\alpha_2)$ and $(\beta_1,\beta_2)$ by holding the displacement vector pmfs $P_{\text{app}}(\mathbf{v}^{(i)})$ fixed and maximizing a lower bound of the log-likelihood function $L(\alpha_1,\alpha_2,\beta_1,\beta_2)$:

$$\begin{aligned} (\alpha_k,\beta_k) &:= \arg\max_{\alpha_k,\beta_k} \sum_{i\in\mathcal{C}} \sum_{m_k^{(i)}} Q_i(m_k^{(i)}) \log P([x_q^{\max}]_i, n_k^{(i)}, y|m_k^{(i)}; \alpha_k,\beta_k) \\ &= \arg\max_{\alpha_k,\beta_k} \sum_{i\in\mathcal{C}} \sum_{m_k^{(i)}} Q_i(m_k^{(i)}) \left( \log P(n_k^{(i)}|m_k^{(i)}, [x_q^{\max}]_i, y; \alpha_k,\beta_k) + \log P([x_q^{\max}]_i, y|m_k^{(i)}) \right), \end{aligned}$$

for $k = 1, 2$. The lower bound is due to Jensen's inequality and concavity of $\log(.)$. Note also that $P([x_q^{\max}]_i, y|m_k^{(i)})$ does not depend on the parameters $(\alpha_1,\alpha_2)$ and $(\beta_1,\beta_2)$ and can be thus ignored in the maximization. We model $P(n_k^{(i)}|m_k^{(i)}, [x_q^{\max}]_i, y; \alpha_k,\beta_k)$ as a Gaussian distribution, i.e. $(\alpha_k n_k^{(i)} + \beta_k - m_k^{(i)}) \sim \mathcal{N}(0,\sigma^2)$. Taking partial

derivatives with respect to each parameter and setting to zero, we obtain the optimal updates:

$$\alpha_k^* := \frac{|\mathcal{C}| \sum_{i\in\mathcal{C}} n_k^{(i)} E[m_k^{(i)}] - \sum_{i\in\mathcal{C}} n_k^{(i)} \sum_{i\in\mathcal{C}} E[m_k^{(i)}]}{|\mathcal{C}| \sum_{i\in\mathcal{C}} E[(m_k^{(i)})^2] - (\sum_{i\in\mathcal{C}} E[m_k^{(i)}])^2}$$

$$\beta_k^* := \frac{1}{|\mathcal{C}|} \sum_{i\in\mathcal{C}} (n_k^{(i)} - \alpha_k^* E[m_k^{(i)}]),$$

for $k = 1, 2$, and where the expectations $E[.]$ are taken over $Q_i(m_k^{(i)})$.

## 5. SIMULATION RESULTS

Our experiments use "Barbara","Lena","Mandrill" and "Peppers" of size 512x512 at 8-bit gray resolution. The two-state channel in Fig. 3 crops the image randomly to resolution between 480x480 and 511x511 and then resizes it to 512x512 resolution. Then JPEG2000 or JPEG compression and reconstruction is applied at 30 dB reconstruction PSNR. In the illegitimate state, the malicious attack overlays a 20x122 pixel text banner randomly in the image. The text color is white or black, whichever is more visible, to avoid generating trivial attacks, such as white text on a white area. The image projection $X$ is quantized to 4 bits, and the Slepian-Wolf encoder uses a 4096 bit LDPC code with 400 degree-1 syndrome nodes.

Fig. 7 compares the minimum rates for decoding $S(X_q)$ with legitimate test images using three different decoding schemes: the proposed EM decoder that learns the parameters, an oracle decoder that knows the parameters, and a fixed decoder that always assumes no cropping and resizing. The EM decoder requires minimum rates only slightly higher than the oracle decoder, while the fixed decoder requires higher and higher rate as the cropped-out area increases.

For the next experiment, we set the authentication data size to 220 bytes and measure false acceptance and rejection rates. The acceptance decision is made based on the empirical conditional entropy of $X_q$ of the estimated cropped-in blocks. The channel settings remain the same except that the JPEG2000/JPEG reconstruction PSNR is selected from 30-42 dB. With 4000 trials each on "Barbara", "Lena", "Mandrill", and "Peppers," Fig. 8 shows the receiver operating characteristic curves created by sweeping the decision threshold of the empirical conditional entropy. The EM decoder performs very closely to the oracle decoder, while the fixed decoder rejects authentic test images with high probability. In the legitimate case, the EM decoder estimates the stretching and shifting parameters with mean squared error $5.7 \times 10^{-6}$ and 0.65, respectively.

## 6. CONCLUSIONS

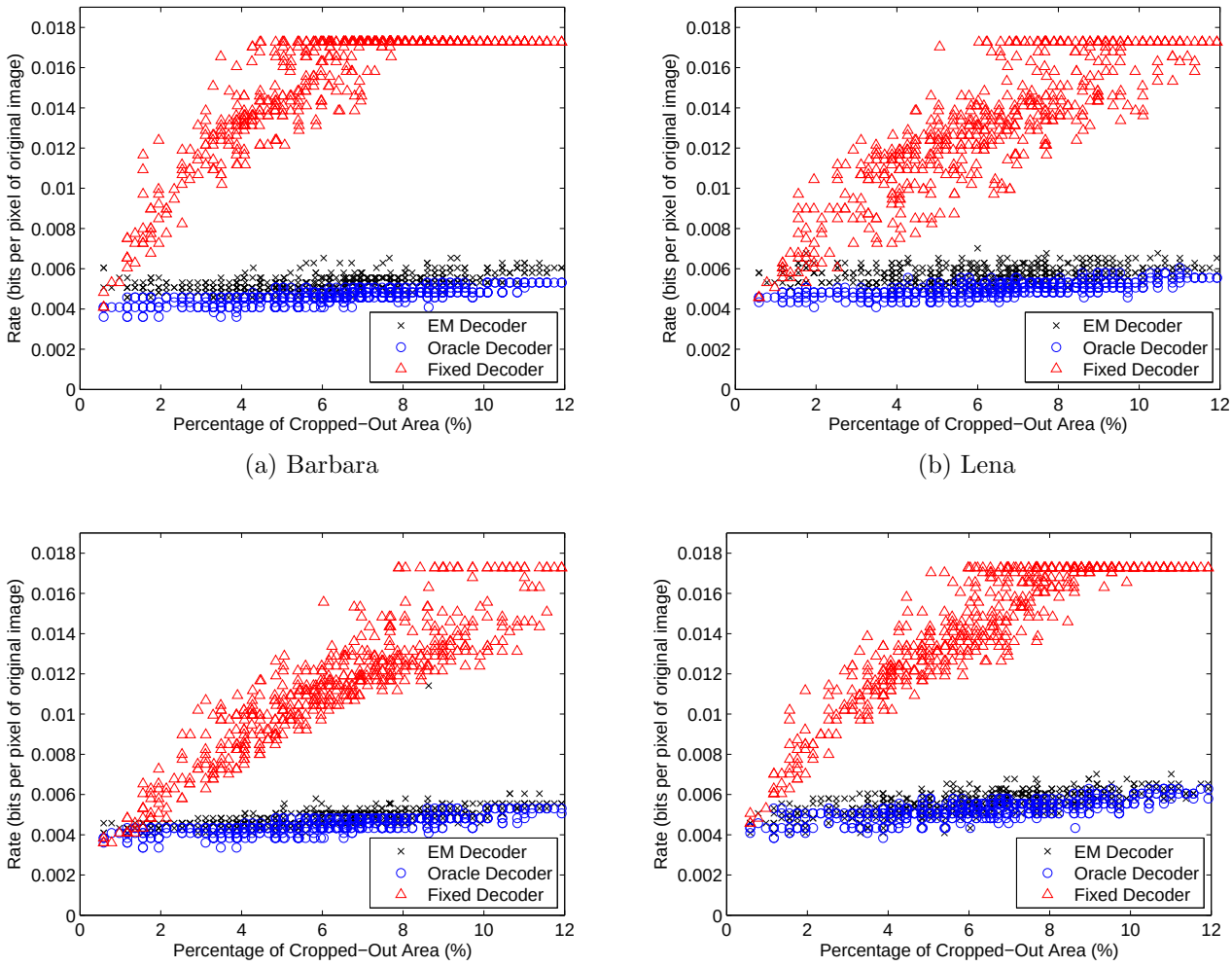
We have extended our image authentication system to handle cropped and resized images. Our authentication decoder learns the stretching and shifting parameters via an unsupervised EM algorithm. We demonstrate that an authentication Slepian-Wolf bitstream of 220 bytes is sufficient to distinguish between legitimate encodings of slightly cropped and resized images and illegitimately modified versions. The work can be extended to other manipulations using an appropriate M-Step.

## ACKNOWLEDGMENTS

This work has been supported, in part, by a gift from NXP Semiconductors to the Stanford Center for Integrated Systems and, in part, by the Max Planck Center for Visual Computing and Communication.

## REFERENCES

1. Y.-C. Lin, D. Varodayan, and B. Girod, "Image authentication based on distributed source coding," in *IEEE International Conference on Image Processing*, (San Antonio, TX), Sep. 2007.
2. Y.-C. Lin, D. Varodayan, and B. Girod, "Image authentication and tampering localization using distributed source coding," in *IEEE Multimedia Signal Processing Workshop*, (Crete, Greece), Oct. 2007.




(a) Barbara (b) Lena

(c) Mandrill (d) Peppers

Figure 7. Minimum rate for decoding legitimate test images using different decoders.


3. Y.-C. Lin, D. Varodayan, and B. Girod, "Spatial models for localization of image tampering using distributed source codes," in *Picture Coding Symposium*, (Lisbon, Portugal), Nov. 2007.
4. L. E. Baum, T. Petrie, G. Soules, and N. Weiss, "A maximization technique occurring in the statistical analysis of probabilistic functions of markov chains," *Annals of Mathematical Statistics* **41**, pp. 164–171, Oct. 1970.
5. J. J. Eggers and B. Girod, "Blind watermarking applied to image authentication," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, (Salt Lake City, UT), May 2001.
6. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in *IEEE Internation Conference on Image Processing*, (Lausanne, Switzerland), Sep. 1996.
7. C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Transactions on Circuits and Systems for Video Technology* **11**, pp. 153–168, Feb. 2001.
8. C.-S. Lu and H.-Y. M. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," *IEEE Transactions on Multimedia* **5**, pp. 161–173, June 2003.
9. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory* **IT-22**, pp. 644–654, Jan. 1976.

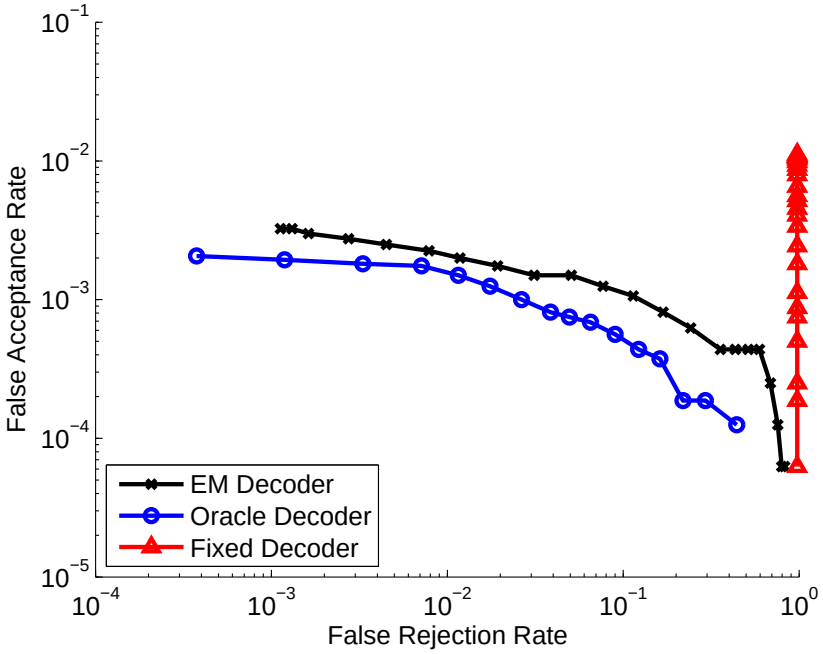



Figure 8. Receiver operating characteristic curves for different decoders.


10. E. Martinian, S. Yekhanin, and J. S. Yedidia, "Secure biometrics via syndromes," in *Allerton Conference on Communications, Control and Computing*, (Monticello, IL), Sep. 2005.
11. S. C. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometric," in *IEEE International Conference on Acoustics, Speech, and Singal Processing*, (Honolulu, HI), April, 2007.
12. Q. Sun, S.-F. Chang, M. Kurato, and M. Suto, "A new semi-fragile image authentication framework combining ECC and PKI infrastructure," in *IEEE International Symposium on Circuits and Systems*, (Phoenix, AZ), May 2002.
13. D. Varodayan, A. Aaron, and B. Girod, "Rate-adaptive codes for distributed source coding," *EURASIP Signal Processing Journal, Special Section on Distributed Source Coding* **86**, pp. 3123–3130, Nov. 2006.
14. D. Varodayan, A. Mavlankar, M. Flierl, and B. Girod, "Distributed grayscale stereo image coding with unsupervised learning of disparity," in *IEEE Data Compression Conference*, (Snowbird, UT), 2007.
15. D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Transactions on Information Theory* **IT-19**, pp. 471–480, July 1973.
16. F. Lefebvre, J. Czyz, and B. Macq, "A robust soft hash algorithm for digital image signature," in *International Conference on Multimedia and Expo*, (Baltimore, Maryland), 2003.
17. C. D. Roover, C. D. Vleeschouwer, F. Lefebvre, and B. Macq, "Robust image hashing based on radial variance of pixels," in *IEEE International Conference on Image Processing*, (Genova, Italy), 2005.
18. D. Varodayan, D. Chen, M. Flierl, and B. Girod, "Wyner-Ziv coding of video with unsupervised motion vector learning," *EURASIP Signal Processing: Image Communication Journal* **23**, pp. 369–378, June 2008.