International Journal on Emerging Technologies **3**(2): 137-141 (2012)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Image Authentication Using Distributed Source Coding

Sagar Chouksey*, Anmol Gupta**, Rashi Agrawal and Mayur Ghadle*******

**Department of Electronics and Telecommunication Engg., Lakshmi Narain College of Technology, Bhopal, (MP)*
***Department of Computer Science Engineering, Oriental Institute of Science and Technology, Bhopal, (M.P)*
****Department of Information Technology, Sagar Institute of Research & Technology, Bhopal, (M.P)*
*****Department of Mechanical Engineering, Technocrats Institute of Technology, Bhopal, (M.P.)*

(Received 05 May, 2012, Accepted 05 October, 2012)

ABSTRACT: This paper investigates the performance and proposes modifications to earlier methods for image authentication using distributed source coding. Image authentication is important in content delivery via untrusted intermediaries, such as peer-to-peer (P2P) file sharing. Many differently encoded versions of the original image might exist. On the other hand, intermediaries might tamper with the contents. Distinguishing the legitimate diversity of encodings from malicious manipulation is the challenge addressed in this paper. We develop a novel approach based on distributed source coding for the problem of backward-compatible image authentication. The key idea is to provide a Slepian-Wolf encoded quantized image projection as authentication data. This version can be correctly decoded only with the help of an authentic image as side information. Distributed source coding provides the desired robustness against legitimate encoding variations, while detecting illegitimate modification.

I. INTRODUCTION

The objective of image authentication is to distinguish legitimate variations in content from maliciously edited ones. Past approaches for image authentication fall into three groups: forensics, watermarking, and robust hashing. In digital forensics, the user verifies the authenticity by solely checking the received content [1]. Unfortunately, these forensic methods cannot work well in images of low quality, since compression noise or re-encoding would weaken those forensic traces. The next option for image authentication is watermarking. In this option, a semi-fragile watermark is embedded into the host signal waveform without perceptual distortion [2-4]. Users can confirm the authenticity by extracting the watermark from the received content. The system design should ensure that the watermark survives lossy compression, but that it “breaks” as a result of malicious manipulations.

Unfortunately, watermarking authentication is not backward compatible with previously encoded contents. Embedded watermarks might also increase the bit rate required when compressing a media file.Robust hashing can check the integrity of the received content using a small amount of data derived from the original content. Cryptographic hashing [5-7] is a special case in which the authentication data are generated using a scrambling hash function that is nearly impossible to invert; any modification of the content is not allowed as modifications yield a very different hash value. However, cryptographic hashing is not applicable to the image authentication problem as processed images are not exactly identical to the original but carry the same meaning. Researchers have been investigating robust hashing schemes that distinguish allowable distortion from malicious editing.

Section 1.1 reviews robust hashing schemes to offer an overview of previous approaches to the image authentication problem. Section 1.2 describes the key element of this work, distributed source coding, by reviewing Slepian-Wolf results, and some practical implementations of the Slepian-Wolf codec.

A. Robust Hashing for Image Authentication

Robust hashing achieves verification of previously encoded media by using an authentication server to supply authentication data to the user. Digital signatures [5,8] have solved the problem when only unaltered content is allowed. The idea is to generate a hash value of the original content using a cryptographic hash function, which is then signed by the private key of an authority using an asymmetric encryption system. The user can check if the content is altered by comparing the hash value of the received content to that in the digital signature. However, this solution is not applicable when some legitimate editing is allowed, since changing any single bit leads to a completely different hash.

If two media signals are perceptually indistinguishable, they should have identical hash values. The authentication data are generated by compressing these features or their hash values. The user checks the authenticity of the received content by comparing the features or their hash values to the authentication data. Typical robust hashing schemes for image authentication consist of three parts: feature extraction, coding of feature vector, and verification. In feature extraction, the original image is analyzed to obtain a set of feature vectors that would be robust against some type of processing, such as lossy compression. The (possibly quantized) feature vectors are coded into a bit stream as a part of the authentication data. The authenticity of the received image is verified at the receiver along with the authentication data which can be delivered through secure channels or embedded in the image.

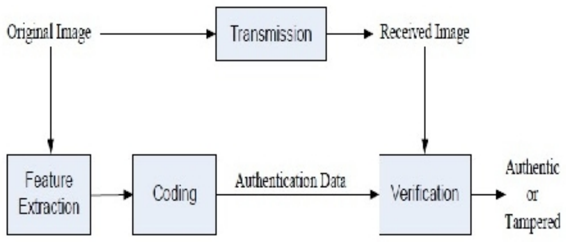

Fig. 1. Flow of Robust Hashing for Image Authentication.

B. Practical Slepian-Wolf Coding

Distributed source coding addresses separate compression of statistically dependent random sequences. Each encoder separately observes a random sequence and sends a bitstream to a single decoder. The decoder reconstructs the random sequences from the incoming bitstreams

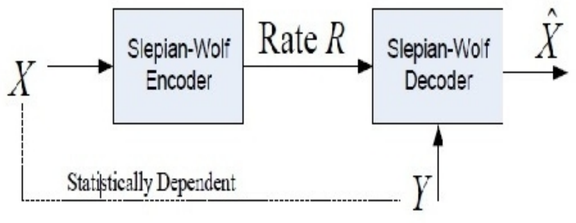

Fig. 2. Slepian-Wolf theorem.

A special case of the Slepian-Wolf theorem. The discrete memory less random variables X and Y are statistically dependent, but Y is only available at the decoder. The key idea is to send the syndrome of the source X to the decoder. The decoder *corrects* the error by decoding the concatenation of the syndrome and the side information Y.

II. REVIEW OF IMAGE AUTHENTICATION USING DISTRIBUTED SOURCE CODING

The methods presented in this paper work well in differentiating legitimate JPEG/JPEG2000 compressed images from illegitimate versions with a small banner inserted in the image using very small amount of authentication data. But these methods are not robust to non-malicious operations such as global contrast and brightness enhancement, and rotation. In [9, 10] these methods are modified to include the use of the EM algorithm in the Slepian-Wolf decoder for learning parameters of the global affine contrast and brightness operation. A brief review of the original authentication system is presented here. The source image, denoted by x, is transmitted through a two-state lossy channel. The image-to-be-authenticated, as received by the user, is denoted by y. In legitimate state, the channel performs lossy JPEG or JPEG2000 compression and reconstruction, while illegitimate state additionally includes malicious tampering by adding a text banner. The left hand side of the figure shows different operations at the sender/authentication server to generate the authentication data which is transmitted through a separate secure communication channel. The first step is to generate the projection coefficients X, by using a pseudo random projection (based on a randomly drawn seed Ks) on the original image x. This random projection is quantized to Xq, before sending it to Slepian-wolf encoder and a cryptographic hash function. . In [12, 9–11] Slepian-Wolf encoder based on rate-adaptive low density parity-check (LDPC) codes is used while in present study Turbo codes [9, 10] are used. The authentication data consists of random seed Ks, a cryptographic hash value of Xq, both signed with a private key and a small part of the Slepian-Wolf bit stream S(Xq). For generating the authentication data upon request, every time a different random seed Ks is used. This prevents the possibility of breaking the system by confining the tampering to thenull space of the projection. The authentication decoder, on the right-hand side of Figure 1 projects received image y to Y in the same way as done on server side. The Slepian-Wolf decoder uses this projection Y as side information to estimate Xq from Slepian-Wolf bit stream S(Xq). Finally, the image digest of X q is compared with image digest received from the server by decrypting the digital signature D(Xq,Ks). If these two image digests are not identical, the received image y is declared to be inauthentic. To make the system robust to affine contrast and brightness operations, the Slepian-Wolf decoder block in Fig. 1 is modified from a joint-biplane LDPC decoder to the contrast and brightness learning Slepian-Wolf decoder [7]. Using the EM algorithm, this decoder learns the global contrast and brightness parameters directly from the Slepian-Wolf bit stream S(Xq) and the side information Y.

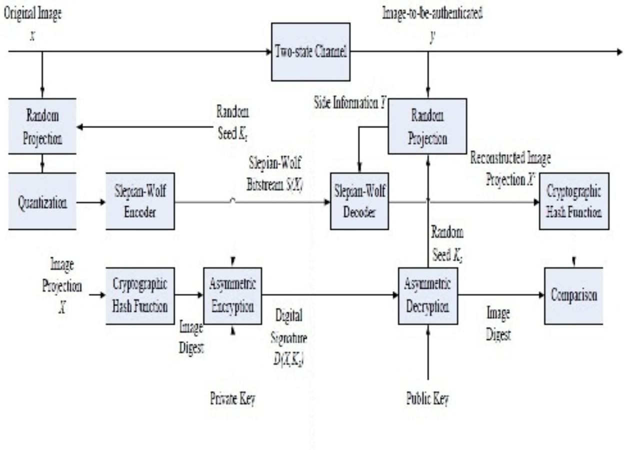

Fig. 3. Slepian-Wolf bit stream S(Xq) and the side information Y.

III. TWO-STATE CHANNEL

We model the image-to-be-authenticated *y* by way of a two state lossy channel. In the legitimate state, the channel performs lossy compression and reconstruction, such as JPEG and JPEG2000, with peak signal-to-noise ratio (PSNR) of 30 dB or better. In the illegitimate, it additionally includes a malicious attack.

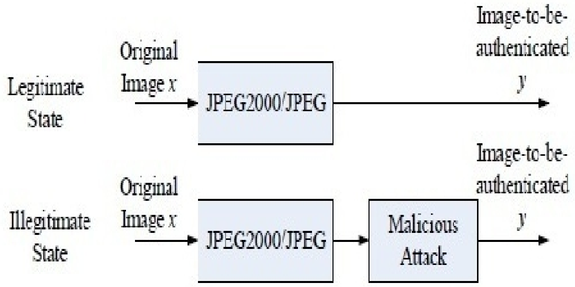

Fig. 4. Atwo state lossy channel.

Fig compares a sample input and two outputs of this channel. The source image *x* is "lena" at 512 x 512 resolution. In the legitimate state, the channel is JPEG2000 compression and reconstruction at 30dB PSNR. In the illegitimate state, a further malicious attack is applied: a 32x100 pixel text banner is overlaid on the reconstructed image. The joint statistics of *x* and *y* vary depending on the state of the channel. We illustrate this by plotting in Fig.3.6 the distribution of the residual $D = Y - X$, where X and Y are image projections of *x* and *y* in Fig. 3, respectively. The projection is a blockwise pseudo randomly weighted mean and will be described in detail in the next section. Since the legitimate channel consists of JPEG2000 or JPEG compression and reconstruction, the samples of the projection residual D are weighted sums of quantization errors. Therefore, the distribution of D resembles a Gaussian, by the central limit theorem. In the illegitimate channel state, the image samples in the tampered region are unrelated to those of the original image, giving the distribution of D non-negligible tails. It is the modification of the joint statistics of X and Y that is exploited for authentication.

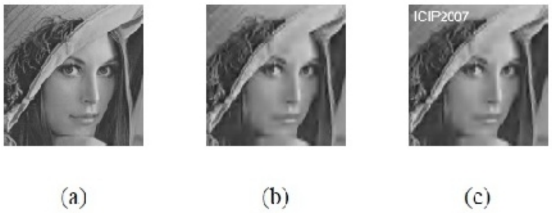

Fig. 5. Portion of Lena image.

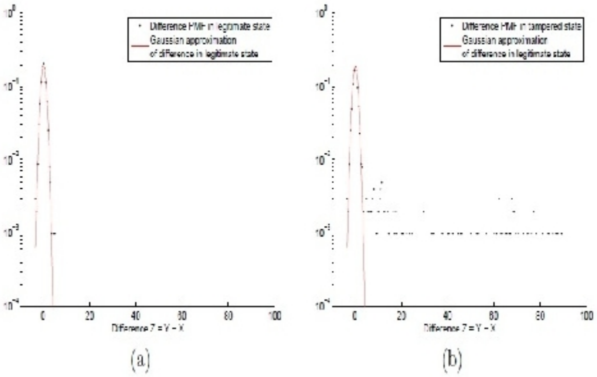

Fig. 6. Difference distribution between two state lossy channel.

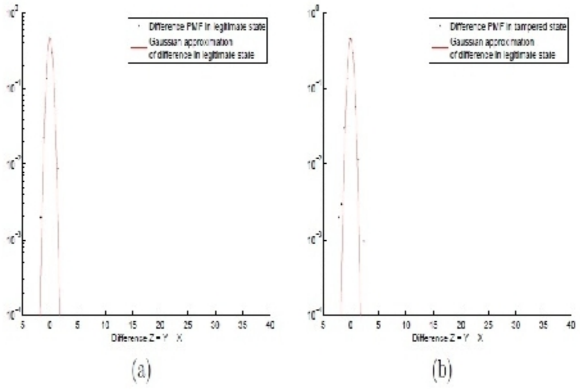

Fig. 7. Difference distribution between two state lossy channel input and output.

IV. SIMULATION RESULTS

We use the test images, at 512 × 512 resolution in 8-bit grayscale resolution. The two-state channel in Figure 3 has JPEG2000 or JPEG compression and reconstruction applied at several qualities. The malicious attack consists of the overlaying of a 19 × 163 text banner at a random location in the image or removing a randomly selected Maximally Stable Extremal Region (MSER) by interpolating the region from its boundaries. The text color is white or black, whichever is more visible, to The quantization of the authentication encoder is varied so that the Slepian-Wolf encoder processes between 1 to 8 bitplanes, starting with the most significant. The Slepian-Wolf codec is implemented using rate-adaptive LDPC codes with block size of 1024 bits. During authentication data generation, the bitplanes of X are encoded successively as LDPCA syndromes. The bitplanes are conditionally decoded, with each decoded bitplane acting as additional side information for subsequent bitplanes, as in [7].

A. Authentication Data Size

Figures compares the minimum rate that would be required to decode the Slepian- Wolf bitstream S(Xq) for side information Y due to legitimate and tampered channel states for *Lena* with the projection X quantized to 4 bits. The following observations also hold for other images and levels of quantization. The rate required to decode S(Xq) with legitimately created side information is significantly lower than the rate (averaged over 100 trials) when the side information is tampered, for JPEG2000 or JPEG reconstruction PSNR above 30 dB. Moreover, as the PSNR increases, the rate for legitimate side information decreases, while the rate for tampered side information stays high and close to the conventional fixed length coding. The rate gap justifies our choice for the Slepian-Wolf bit stream size: the size just sufficient to authenticate both legitimate 30 dB JPEG2000 and JPEG reconstructed versions of the original image.

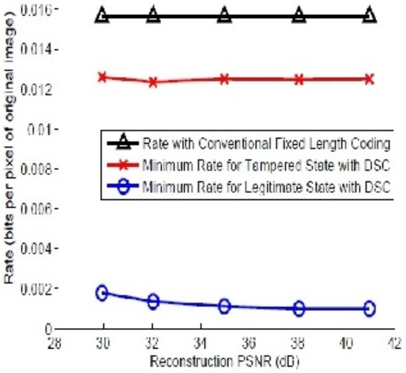

Fig. 8. Maximum selected Slepian-Wolf bit stream size in bytes.

Figure shows the maximum selected Slepian-Wolf bitstream size in bytes among all the test images from 1 to 8 bits in quantization of X. For 4-bit quantization, the Slepian-Wolf bit stream size is less than 80 bytes or 2.3% of the encoded file sizes at 30 dB reconstruction. Compared to conventional fixed length coding, distributed source coding offers a great rate saving. For authentication data size of 120 bytes, conventional fixed length coding can only deliver 1-bit quantized projections, while distributed source coding can offer 5-bit precision. The overall effect is lower decision error.

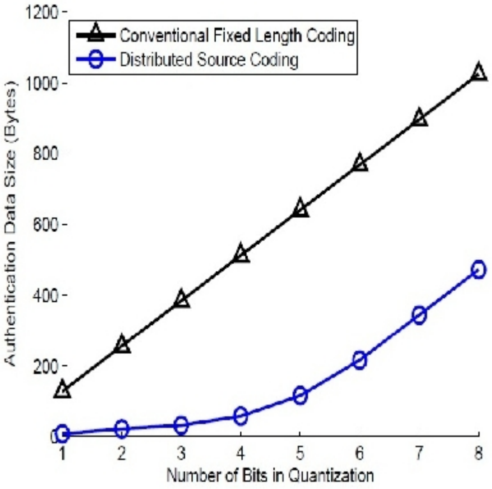

Fig. 9. Data size v/s no of bits.

V. CONCLUSIONS

In this work, we developed a novel backward-compatible image authentication scheme, based on distributed source coding, that distinguishes between legitimate encoding variations of an image and illegitimately modified versions. We demonstrated false acceptance rates close to zero for authentication data size less than 66 bytes or 2.3% of the compressed image size. We intend to extend this scheme to authentication of video sequences in P2P settings.

REFERENCES

[1]. H. Farid. Image forgery detection. *IEEE Signal Processing Magazine*, 26(2):16–25, March 2009.

[2]. 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, September 1996.

[3]. 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

[4]. R.B. Wolfgang and E. J. Delp. A watermark for digital images. In *IEEE International Conference on Image Processing*, Lausanne, Switzerland, September 1996.

[5]. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, January 1976.

[6]. D. Eastlake. US secure hash algorithm 1 (SHA1), RFC 3174, September 2001.

[7]. R Rivest. The MD5 message-digest algorithm, RFC 1321, April 1992.

[8]. R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures
and public-key cryptosystems. *Communications of the ACM*, **21**(2):120–126, 1978.

[9]. Y.C. Lin, D. Varodayan, T. Fink, E. Bellers, and B. Girod, "Authenticating contrast and brightness adjusted images using distributed source coding and expectation maximization," Proc. IEEE International Conference on Multimedia and Expo, ICME 2008, Hannover, Germany, June 2008.

[10]. "Localization of tampering in contrast and brightness adjusted images using distributed source coding and expectation maximization," Image Processing, 2008. ICIP 2008. *15th IEEE International Conference* on, pp. 2204–2207, Oct. 2008.

[11]. Y.C. Lin, D. Varodayan, and B. Girod, "Image authentication and tampering localization using distributed source coding," Multimedia Signal Processing, 2007. MMSP 2007. *IEEE 9th Workshop on*, pp. 393–396, Oct. 2007.

[12]. Y.C. Lin, D. Varodayan, and B. Girod, "Image authentication based on distributed source coding," Image Processing, 2007. ICIP 2007. *IEEE International Conference on*, vol. **3**, pp. III –5–III –8, 16 2007-Oct. 19 2007.

.