Image Authentication Using Distributed Source Coding

[1,]Dr. Krishna Mohanta, [2,]Dr.V.Khanaa
[1,]Sri Sai Ram Engineering College, Chennai 600 044.
[2,]Dean – Pg Studies Bharath University., Chennai-600 073

Abstract:
We Present A Novel Approach Using Distributed Source Coding For Image Authentication. The Key Idea Is To Provide A Slepian-Wolf Encoded Quantized Image Projection As Authentication Data. This Version Can Be Correctly Decoded With The Help Of An Authentic Image As Side Information. Distributed Source Coding Provides The Desired Robustness Against Legitimate Variations While Detecting Illegitimate Modification. The Decoder Incorporating Expectation Maximization Algorithms Can Authenticate Images Which Have Undergone Contrast, Brightness, And Affine Warping Adjustments. Our Authentication System Also Offers Tampering Localization By Using The Sum-Product Algorithm.

Index Terms- Distributed Source Coding, EM Algorithm, Image Authentication, Sum-Product Algorithm.

1. Introduction

Media content can be efficiently delivered through intermediaries such as peer-to-peer sharing. In these system each user not only receives the requested content but also act as a rely forwarding the received portion to the other user .since the same content can be re- encoded several times, media content in those p2p file sharing system is available in various digital format such as JPEG and JPEG2000.On the other hand, the untrusted intermediaries might tamper with the media for a variety of reason such as interfering with the distribution of particular files as piggy backing unauthentication content orgenerally discrediting a particular distribution system .In 2005 survey indicates that more than fifty percentage of popular songs in KaZaA are corrupted and replaced with noise of different songs. The problem is more challenging if some legitimate adjustment such as crop [ping and resizing an image .We applied distributed source coding and statistical methods to solve image authentication problem.

2. Background

Previous Work in Image Authentication Past approaches for image authentication fall into three groups: forensics, watermarking, and robust hashing. Fixed projection has the weakness that an attacker who knows the null space of the projection can alter the image without affecting the authentication data. Using pseudo-random projections or tilings, such as in [28], keeps the null space a secret. Secure Biometrics Our approach has similarities to slepian-wolf coding for secure storage of biometric data The secure biometric problem and the image authentication problem have important differences, For secure biometric data from two different peoples are assumed to be independent. In image authentication the tampered target images are usually correlated to the original but with static different to those of the authentic target image.

3. Image Authentication System

The authentication data provides information about the original image to the user. The user makes the authentication decision based on the target image and the authentication data. (a).x original image (b).y at the output of the legitimate channel (c).y at the output of the tampered channel It demonstrates a sample input and two outputs of this channel. The source image x is a Kodak test image at 512 x 512 resolution. In the legitimate state, the channel is JPEG2000 compression and reconstruction at (the worst permissible) 30dB PSNR. In the tampered state, a further malicious attack is applied: a 19x163 pixel text banner is overlaid on the reconstructed image and some objects are removed. Proposed Image Authentication System In our authentication system shown in Fig.4, a pseudorandom projection (based on a randomly drawn seed Ks) is applied to the original image x and the projection coefficients X are quantized to yield Xq. The authentication data are comprised of two parts, both derived from Xq. The Slepian-Wolf bitstream S(Xq) is the output of a Slepian-Wolf encoder based on LDPC codes [45] and the much smaller digital signature D (Xq, Ks) consists of the seed Ks and a cryptographic hash value of Xq signed with a private key. The authentication data are generated by a server upon request. Each response uses a different random seed Ks, which is provided to the decoder as part of the authentication data. This prevents an attack which simply confines the tampering to the null space of the projection. Based on the random seed, for each 16 x 16 non overlapping block Bi, we generate a 16 x 16 pseudorandom matrix Pi by

drawing its elements independently from a Gaussian distribution N(1,) and normalizing so that =1. We choose=0.2 empirically. In this way, we maintain the properties of the mean projection while gaining sensitivity to high-frequency attacks. The inner product is uniformly quantized into an element of Xq. The rate of the Slepian-Wolf bitstream S(Xq) determines how statistically similar the target image must be to the original to be declared authentic. If the conditional entropy H(Xq/Y) exceeds the bitrate R in bits per pixel, Xq cannot be decoded correctly [2]. Therefore, the rate of S(Xq) should be chosen to be just sufficient to authenticate the legitimate image at its worst permissible quality. In our system, we select a Slepian-Wolf bitrate just sufficient to authenticate both legitimate 30 dB JPEG2000 and JPEG reconstructed versions of the original image. Practically, the Slepian- Wolf bitrate is determined by finding the minimum decodable rate for the training images with the worst permissible quality. This worst permissible quality is external parameter that depends on the particular

application. Generally, if a smaller quality degradation is permissible, fewer bits are required for authentication. If a worse quality is permissible, more bits are needed.At the receiver, the user seeks to authenticate the image y with authentication data S(Xq) and D(Xq,Ks). It first projects y to Y in the same way as during thentication data generation using the same random seed Ks. A Slepian- Wolf decoder reconstructs Xq‘ from the Slepian-Wolf bitstream S(Xq) using Y as side information. Decoding is via LDPC belief propagation [45] initialized according to the statistics of the legitimate channel state at the worst permissible quality for the given original Finally, the image digest of Xq‘ is computed and compared to the image digest, decrypted from the digital signature D(Xq,Ks) using a public key. If these two image digests do not match, the receiver recognizes that image y is tampered. Otherwise the receiver makes a decision based on the likelihood ratio test:P(Xq‘,Y)/Q(Xq‘,Y)> T, Where P and Q are probability models derived from (1) for legitimate and tampered states, respectively, and T is a fixed decision threshold.The authentication system presented in this section can address various types of lossy compression. The next section discusses an adaptive distributed source coding decoder to broaden the robustness of the system for some common adjustments, such as contrast and brightness adjustment, and affine warping.

(a).The original imag
(b).Legitimate image
(c).Realigned target image color overlaid

It shows a target image which has simultaneously undergone contrast brightness and affine wrapping adjustment .The blue area associated with the 16x16 blocks indicate the cropped -out regions the other block from the cropped-in region.

4. Tampering Localization

Decoder Factor Group There are two classes of nodes :the variable nodes represent the random variables of interest the factor nodes represent the probabilistic relationship among the adjacent image. variable nodes based on the factor graph representation the sum product algorithm is used.

5. Conclusions

This paper presents and investigates a novel image authentication scheme that distinguishes legitimate ncoding variations of an image from tampered versions based on distributed source coding and statistical methods. A two-state lossy channel model represents the statistical dependency between the original and the target images. Tampering degradations are captured by using a statistical image model, and legitimate compression noise is assumed to be additive white Gaussian noise. Slepian-Wolf coding that exploits the correlation between the riginal and the target image projections achieves significant rate savings.

References

[1]. R.B.Wolfgang and E.J.Delp,‖A Watermark for Digital Images,‖.
[2]. J.Fridrich,‖Robust Bit Extraction From images‖.
[3]. S.Roy and Q.Son,‖Robust Hash For Detecting And Locallizing Image Tampering,‖.
[4]. A. Liveris Z.Xiong, and C.Georghiades,‖compression of Binary Sources with side information at the decoder
[5]. using LPDC Codes,‖.Y.C.Lin,‖Image Authentication Using Distributed Source Codind,‖.