Image Authentication System using LDPC and Watermarking Technique

Ankit Bhatnagar
M.Tech Scholar
Computer Science & Engineering
RKDFIST, Bhopal

Jasvinder Pal Singh
Assistant Professor
Computer Science & Engineering
RKDFIST, Bhopal

Gaurav Shrivastava
HOD
Computer Science & Engineering
RKDFIST, Bhopal

ABSTRACT
Now a days, the rate of using digital image is increasing exponentially because of its low cost and easy manipulation property. It is obvious that digital images captured from CCD cameras or other digital image devices have to be analyzed and determined before processing it, to keep the integrity and ensure the accuracy and reliability of the digital image. We need some sort of robust methods and standard procedures that guarantee and strengthen the authenticity of digital image.

Image authentication is a technique that analyzes a digital image and determines whether it is altered or not. Image authentication technique is very useful for various organizations such as health care, law enforcement agencies and insurance sector etc. Image authentication is also important in content delivery via untrusted intermediaries, such as peer-to-peer (P2P) file sharing. Untrusted intermediaries might tamper the contents of image. Distinguishing the legitimate diversity of encodings from malicious manipulation is the challenge addressed in this paper. We developed a LDPC and watermark based new approach for image authentication. With the help of this approach we can authenticate images effectively. In our technique, we provide LDPC quantized image projection and the Encrypted image as authentication data. As well as watermark image that was embedded into original image to identify legitimate or illegitimate state of image authentication system. These data can be correctly decoded only with the help of an authentic image as side information. This technique provides the desired robustness against legitimate encoding alteration, while detecting illegitimate variations.

Keywords:
Image Authentication, Low Density Parity Check (LDPC), Digital Watermarking.

1. INTRODUCTION
Proliferation of digital media is accompanied by increasing functionality and usability of software for manipulating digital media. For example, advancement in digital imaging technologies have led to the development of low-cost and high-resolution digital still and video cameras and scanners. Digital Videos and images generated by various sources are widely used in a number of applications from medical imaging and law enforcement to banking and daily consumer use. Relying on digital media such as law enforcement and security makes robust techniques for media authentication a must [2]. These techniques are also vital in content delivery via untrusted intermediaries, such as peer-to peer (P2P) file sharing or P2P multicast streaming [1].

In the P2P file sharing applications, intermediaries might tamper the contents of file for a variety of reasons, such as hindering with the distribution of a specific file, piggybacking unauthentic content, or generally discrediting a particular distribution system. Distinguishing the legitimate diversity of encodings from malicious manipulation is the major technical challenge for image authentication systems.

Forensics, Watermarks and media hashes have been used in past for image authentication. In digital forensics, the user verifies the authenticity of an image solely by checking the received content [3,5]. Unfortunately, without any information from the original, one cannot entirely confirm the integrity of the received content because content unrelated to the original may pass forensic checking. Another alternative for image authentication is watermarking. A "fragile" watermark can be embedded into the host signal waveform without perceptual distortion [6,7]. Users can confirm the authenticity by extracting the watermark from the received matter. The system design should ensure that the watermark survives lossy compression, but that it "breaks" as a result of a malicious manipulation. Unfortunately, Watermark authentication is not backward compatible with previously encoded, unmarked contents which cannot be authenticated later. Embedded watermarks may also increase the bit-rate required when compressing a media file. Media hashing [8,9] achieves verification of previously encoded media by using an authentication server to supply authenticated data to the user. Media hashes are inspired by cryptographic digital signatures[10], but unlike cryptographic hash functions, media hash functions are supposed to offer the 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 equivalent hash values. A common approach of media hashing is to extract features which have perceptual importance and should outlast compression. The authentication data are generated by compressing these features or generating their hash values. The user analyze the authenticity of the received content by comparing the features or their hash values to the authentication data.

We propose a combination of Encryption based on Low Density Parity Check (LDPC) code and watermarking technique for image authentication. In [1], a method for backward-compatible image authentication based on distributed source coding is presented. This method provides a Slepian-Wolf encoded [11] quantized image projection as the authentication data which can be successfully decoded only by using an authentic image as side information. The fixed decoder used in [1,12] can do successful image authentication for JPEG compressed images but image authentication is not possible using fixed decoder if the channel applies contrast

and brightness adjustment in addition to JPEG compression. Our proposed work makes Image Authentication robust to affine transformations.

In our proposed work, the user checks the integrity of the received content using a small amount of data derived from the original content. The authentication server provides a user with a LDPC encoded image projection and the Encrypted Image as authentication data and the user attempts to decode this bitstream using the image-to-be-authenticated as side information. The LDPC result indicates that lower the distortion between side information and the original, the fewer authentication bits are required for correct decoding. This allows us to distinguish between legitimate encoding variations of the image and illegitimate modifications. In Section 2, We first describe a two-state channel that models the target image then in section 3 and 4 we present the proposed image authentication work and its rationale in detail. Simulation results will be presented in Section 5.

2. TWO-STATE CHANNEL

We model the target image y by way of a two-state lossy channel, shown in Fig 1. In the legitimate state, the channel performs lossy compression and reconstruction, such as JPEG or JPEG2000, with peak signal-to-noise ratio (PSNR) of 30 dB or better. In the tampered state, it includes a malicious attack.

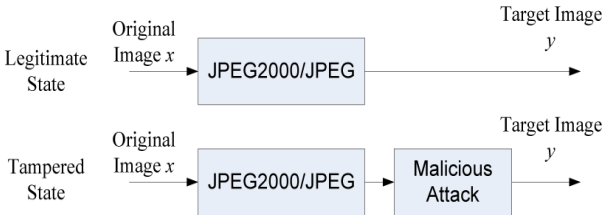


Fig 1. The target image y is modeled as an output of a two-state lossy channel. In the legitimate state, the channel consists of lossy compression and reconstruction, such as JPEG and JPEG2000; in the tampered state, the channel further applies a malicious attack.

Fig 2 demonstrates a sample input and two outputs of this channel. The source image is a Kodak test image at 512 × 512 resolution. In the legitimate state, the channel is JPEG2000 compression and reconstruction at (the worst permissible) 30 dB PSNR. In the tampered state, a further malicious attack is applied, a 19×163 pixel text banner is overlaid on the reconstructed image and some objects are removed.

Fig 2. Examples of the two-state lossy channel output. (a) x original, (b) y at the output of the legitimate channel, and (c) y at the output of the tampered channel.

The joint statistics of x and y vary depending on the state of the channel. In the legitimate state, the difference resembles white noise due to the compression. In the tampered state, the channel additionally introduces tampering which results in image-like differences in some regions. This suggests that low frequency components can greatly distinguish legitimate and tampered regions. Let X and Y be low-frequency block projections of images x and y, respectively. The image authentication problem at the projection level in the hypothesis testing setting is described as follows:

$$X|Y \sim \begin{cases} P(X|Y) = \mathcal{N}(Y, \sigma_e^2) \\ Q(X|Y) = (1-\gamma)\,\mathcal{N}(Y, \sigma_e^2) + \gamma P_{tamp}(X|Y) \end{cases}$$

Where the distribution is P(X|Y) if y is legitimate and Q(X|Y) if it is tampered. Also, $\gamma \in [0,1]$ is the fraction of tampered image blocks, and Ptamp(X|Y) is their probability model. We assume that Ptamp(X|Y)=U(X) is a uniform distribution over the dynamic range of X. Having both projections X and Y, the optimal decision is based on the likelihood ratio test: $P(X,Y)/Q(X,Y) \lessgtr T$. The next section describes our image authentication scheme which uses these statistical assumptions to generate authentication data using LDPC and watermarking technique[1].

3. PROPOSED IMAGE AUTHENTICATION SYSTEM BASED ON LDPC AND WATERMARKING

Here, we propose a framework for image authentication using LDPC technique (Low Density Parity Check Codes) and Digital Watermarking technique. The way that we can prove the semantic aspect of an image authentication based on the encryption and decryption. The image authentication based on LDPC coding and watermarking is shown in Fig 3. We denote the source image as x. The user receives the image to be-authenticated y as the output of a two-state lossy channel that models legitimate and illegitimate modifications. The left-hand side of Fig 3 shows that the authentication data consist of a Watermarked Image ,LDPC encoded quantized image projection of x and the Encrypted Image. The verification decoder, in the right-hand side of Fig 3, knows the statistics of the worst permissible legitimate channel and can correctly decode the authentication data only with the help of an authentic image Y as side information. The detail explanation of Fig 3 is described in next section.

4. PROPOSED AUTHENTICATION DATA GENERATION & VERIFICATION ALGORITHM

Authentication Data Generation is done at the Sender side and Verification is done at the Receiver side as shown in Fig 3.

4.1 At Sender Side

1: Input an Image x that has to be sent.

2: Apply Watermark embedding process that embeds Watermark Image W_m into the original Image x that gives us Watermarked image X_m.

3: Apply Transformation on Watermarked Image X_m that yield a gray scale image X_T of size 336 × 336.

4: Divide the Image x_T into 16×16 Block and then a Mean Projection is applied on each block which gives us a projected data X which is quantized to yield Xq.

5: On the Projected Data Xq perform LDPC Encoding that produces LDPC bit-stream $S(X_q)$.
6: On the X_q, i.e. the output of Step 4, conversion is performed that converts Xq into an Image X_p .
7: Perform Private key Cryptography Algorithm that produces an Encrypted Image X_E.

The Watermarked Image X_m is then sent to the receiver along with LDPC encoded data $S(X_q)$ and Encrypted Image X_E as Authentication Data.

4.2 At Receiver Side

1: At the receiver, the user seeks to Authenticate the Image y with the help of Authentication Data $S(X_q)$ and X_E.
2: Apply Watermark extraction Technique on Image y to extract Watermark Image W_m. The output of this step is the Watermark Image W_m and the Watermarked extracted Image Y_x.
3: Apply Transformation on Image y_x that yield a gray scale image y_T of size 336 × 336 .
4: Divide the Image y_T into 16×16 Block and then a Mean Projection is applied on each block which gives Projected Data Y which is quantized to yield Y_q.
5: Perform LDPC Decoding on the LDPC bit-stream $S(X_q)$ using Y_q as the side information that constructs $S(X_q)$.
6: On the $S(X_q)$ conversion is performed that converts X_q into an Image Y_p.
7: Perform same Private Key cryptography Algorithm on the Encrypted Image X_E that produces a Decrypted Image Y_D.
8: Compare the results obtained from Step 6 and Step 7 as well as Watermark Image W_m received from step 2 with the original Watermark Image W_m . If the two Images or the Watermark Image do not match, the receiver recognizes that image is tampered. Otherwise the receiver makes a decision based on the likelihood ratio test.

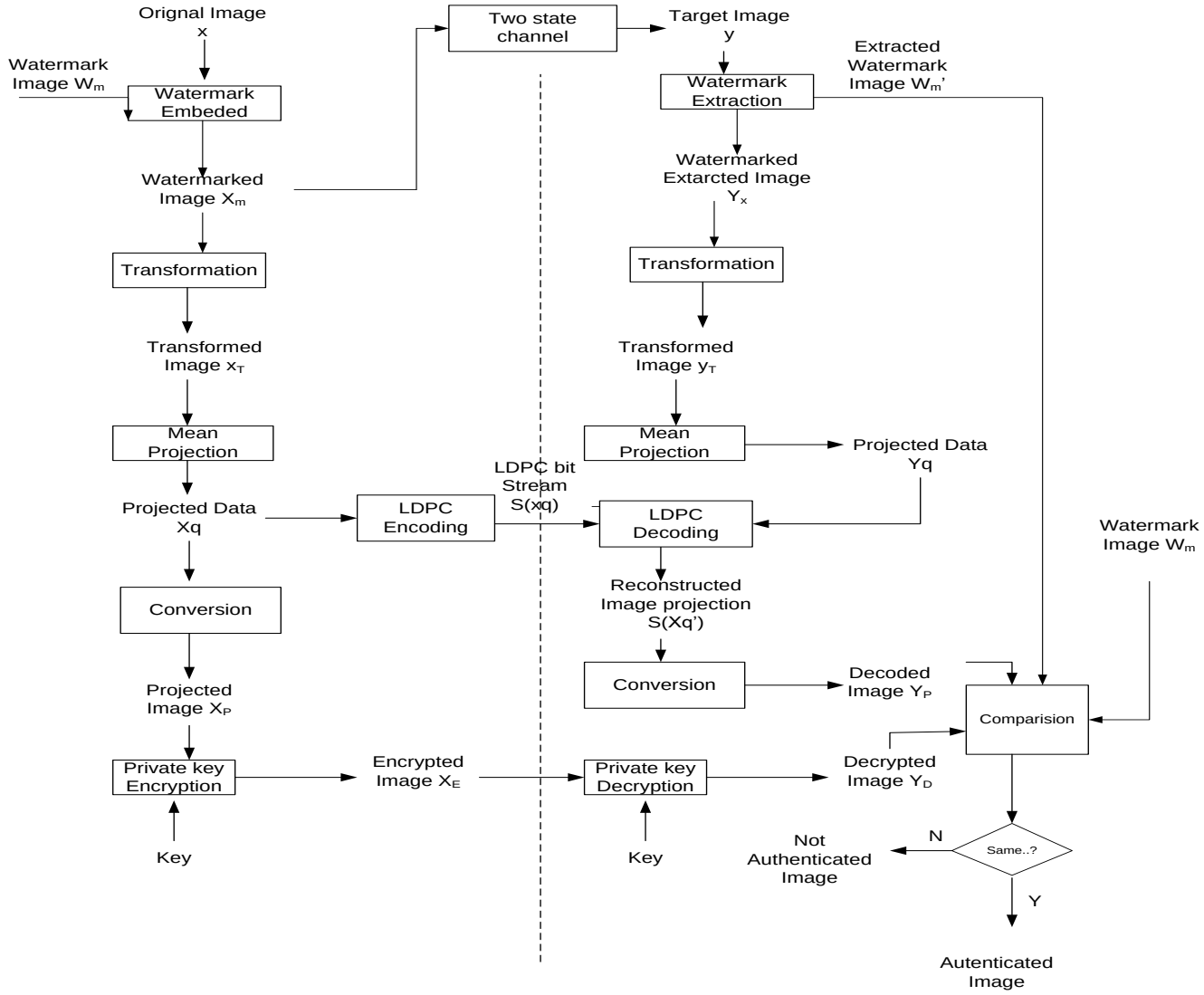


Fig 3: Proposed Image Authentication System Using LDPC

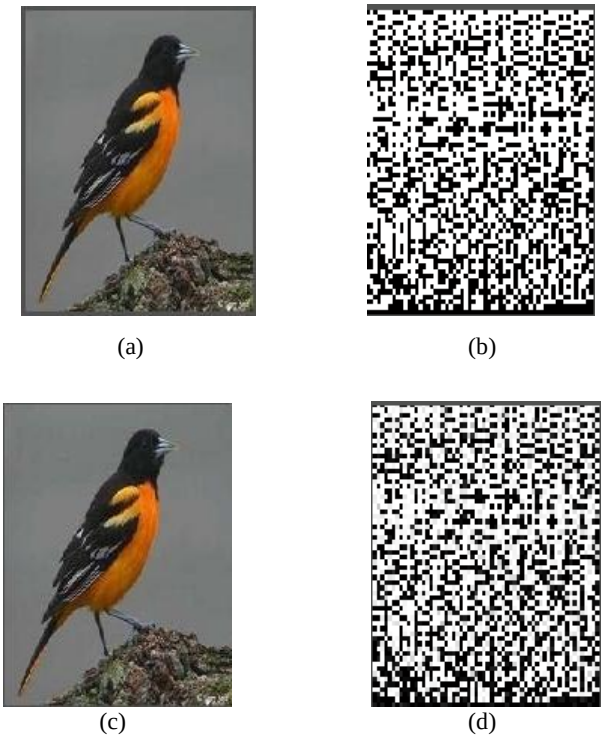
5. EXPERIMENTAL RESULTS AND ANALYSIS

This section describes the details of experiments conducted to examine the efficiency of the Proposed Algorithm for Image Authentication under varying channel conditions. Experiments are conducted on a Bird Image of 512 × 512 resolution at 24-bit color or 8-bit gray resolution and the original Image on the server is stored in JPEG format with quality factor Q = 100.

Five different sets of experiments are conducted for different legitimate states of the channel. In the illegitimate state the channel additionally overlays a text banner (of sizes varying from 80×25 to 160×50, black or white color text depending upon the background gray level) at a random location. In present implementation 8-bit planes of the Mean Projection is used. The LDPC bit stream S(X) is the output of a LDPC encoder [15].

5.1 Authentication of Compressed Images

We evaluate the performance of Proposed System when channel state varies JPEG quality factor Q over the interval [45, 90]. Fig. 4 shows demonstration of proposed system. Here original Image of data size 768 KB is Compressed to 128 KB from (b) and (d) it is clear that both the Image Digests are not same. It means that our system easily checks the authenticity of Compressed images.



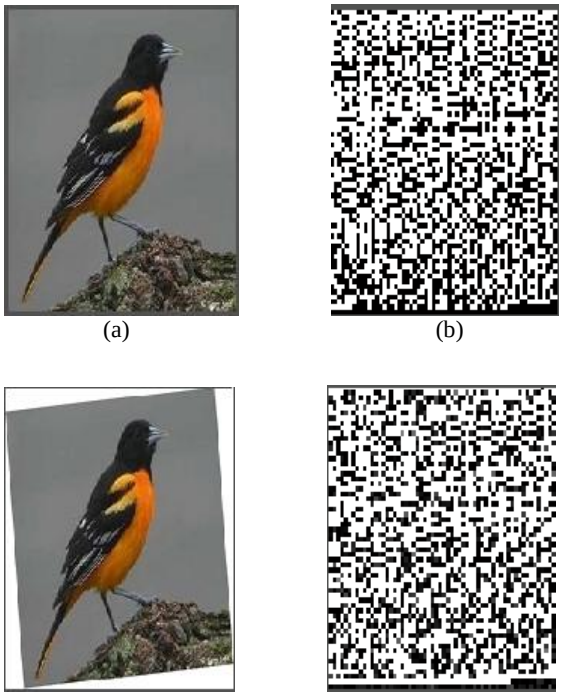
(a) (b)

(c) (d)

Fig 4. Demostration of Authentication System for compressed Images (a) original image of bird (b) image digest of original image (c) image with JPEG compression (d) image digest of compressed image.

5.2 Authentication of Rotated Images

We evaluate the performance of our System with rotation over the interval [-10° ,10°]. Fig. 4 shows the experimental result. From (b) and (d) it is clear that both the Image Digests are not same. It means that our system easily checks the authenticity of rotated images.

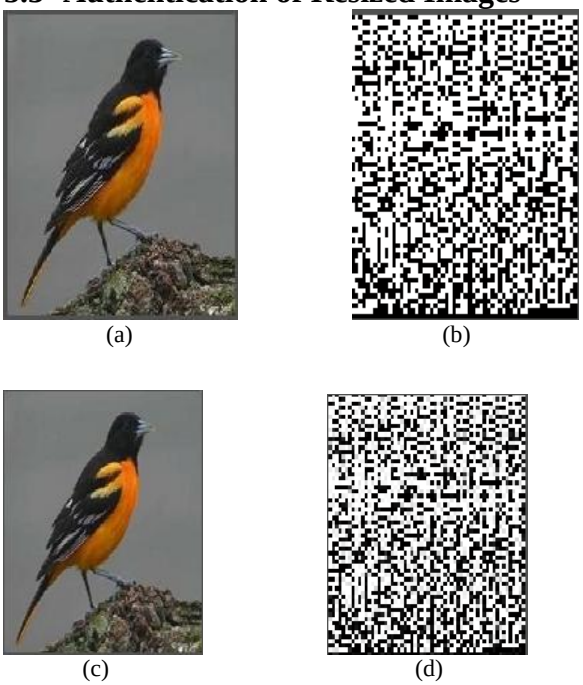


(a) (b)

(c) (d)

Fig 5. Demostration of Authentication System for rotated Images (a) original image of bird (b) image digest of original image (c) image with (-10°,10°) rotation (d) image digest of rotated image

5.3 Authentication of Resized Images



(a) (b)

(c) (d)

Fig 6. Demostration of Authentication System for Resized Images here (a) original bird image of 200× 200 (b) Image digest of original image (c) resized image by 150×150 pixel (d) image digest of rotated image

We check the performance of the our system for the test images which resized along x and y direction independently over ratios [0.4, 2]. Fig. 5. shows the experimental result. From (b) and (d) it is clear that Both Image Digests are not same. It means that our system easily check the authenticity of resized images.

5.4 Authentication of adjusted Brightness and Contrast parameters

We evaluate the performance of the our System with brightness and contrast adjustment parameters (a,b) on {(10,−20), (20,−10), (10, 20), (20,10), (-10, 20), (-20, 10)}. Fig. 6. shows the experimental result. From (b) and (d) it is clear that both the Image Digests are not same. It means that our system easily check the authenticity of adjusted brightness and contrast parameters images.

(a)

(b)

(c)

(d)

Fig 7. Demostration of Authentication System for adjusted brightness and contrast parameters here (a) original image of bird (b) Image digest of original image (c) Image with contrast and brightness adjustment (d) Image digest of contrast and brightness adjusted image

5.5 Tampering Localization

We test the tampering localization system only with maliciously tampered images. The malicious tampering consists of the overlaying of a text banner of size 35×15 pixel. The text color is white. The text banner is placed for malicious tampering, because greater tampering makes tampering more easily detected, but makes localization more difficult. Our system easily identifies authenticity of Tampering localization of image. Fig. 7. shows the experimental result from (b) and (d) it is clear that both the Image Digests are not same. It means that our System easily checks the authenticity of tampered image.

(a)

(b)

(c)

(d)

Fig 8. Demonstration of Authentication System for tampering localization Images, here (a) original Image of bird (b)image digest of original image (c) tamperd image with 35×15 pixel text banner (d) image digest of tampered image.

Fig 9. shows the graph of Authentication ratio for bird Images here Y axis represent Ratio of legitimate/illegitimate Images and X axis represents channel conditions on which Authentication of image is checked.

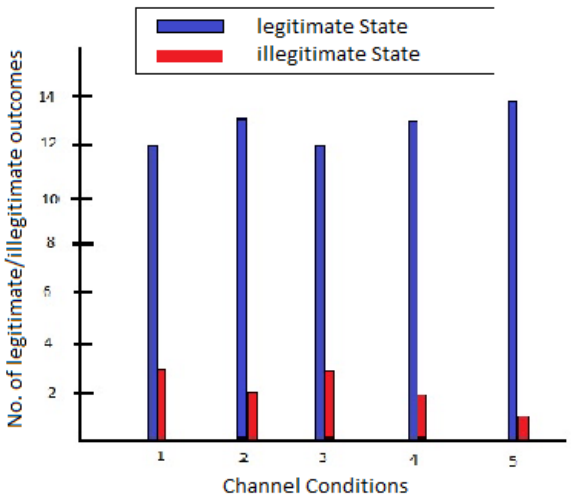


Fig 9. Graph of Authentication Ratio

Table 1. shows experimental results which is derived from the Bird Image. This image is altered by adjusting their parameters. The result shows that our proposed System authenticate the Image with high authentication ratio.

Table 1. Authentication ratio for bird image

S.No.	Channel Conditions	Adjustment Parameters	Total Number of Adjusted "Bird" Image	legitimate Result	illegitimate Result	Efficiency
1.	Compression	[45,90] Quality Factor	15	12	3	80%
2.	Rotation	$[-10^{\circ},10^{\circ}]$ Degree	15	13	2	86.67%
3.	Resize	[0.4,2] Ratio	15	12	3	80%
4.	Contrast & Brightness	[-10,20] & [-20,10] Ratio	15	13	2	86.67%
5.	Tampering	[5×5,40×40] Pixels	15	14	1	93.33%

6. CONCLUSION

The Image Authentication System, based on Low Density Parity Check (LDPC) codes distinguishes between legitimate encoding variations of an image and illegitimately modified versions. This paper investigated the robustness of the scheme for image authentication described in [1] and proposed several improvements. We obtained a robust algorithm for image authentication using LDPC. It is clear from the results (from Fig. 3 to Fig. 6) that the proposed scheme gives almost the same performance as an oracle decoder or a decoder using the EM algorithm [14] for parameter estimation, using methods that have much less computational complexity.

7. REFERENCES

[1] Yao-Chung Lin, David Varodayan, Bernd Girod, "Image Authentication Using Distributed Source Coding", IEEE Transactions on Image Processing, vol. 21, no. 1, Jan. 2012.

[2] Nitin Khanna, Antoni Roca, George T. C. Chiu, Jan P. Allebach, Edward J. Delp "Improvements on Image Authentication and Recovery Using Distributed Source Coding". National Science Foundation, under Award Number 0524540,2009.

[3] H. Farid, "Image forgery detection", IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.

[4] J. Lukas and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images", presented at the Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003.

[5] A. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images", *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3948–3959, Oct. 2005.

[6] 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.

[7] R. B. Wolfgang and E. J. Delp, "A watermark for digital images", in *IEEE International Conference on Image Processing*, Lausanne, Switzerland, Sep. 1996.

[8] C.Y. Lin and S.F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation", *IEEE Transcations on Circuits and Systems for Video Technology*, vol. 11, no. 2, pp. 153–168, Feb. 2001.

[9] C.S. Liu and H.Y.M. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme", *IEEE Transcations on Multimedia*, vol. 5, no. 2, pp. 161–173, June 2003.

[10] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transcations on Information Theory*, vol. IT-22, no. 6, pp. 644–654, Jan. 1976.

[11] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources", Information Theory, IEEE Transactions on, vol. 19, no. 4, pp. 471–480, Jul 1973.

[12] 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.

[13] 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.

[14] 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.

[15] Angelos D. Liveris, Zixiang Xiong, Costas N. Georghiades, "Compression of Binary Sources With Side Information at the Decoder Using LDPC Codes", IEEE Communications Letters, vol. 6, no. 10, oct 2002.