JPEG Compression History Estimation for Color Images

SAMPATH KORRA,
Associate Professor,
Department of Computer Science and Engineering,

PILLALAMARRI SREESRINIVAS,
Assistant Professor,
Department of Electronics and Communications Engineering,

Siddhartha Institute of Technology and Sciences,
Narapally, Hyderabad, Telangana – 500 088.

Abstract

The secret information would be transmitted between the sender and recipient to raise the security requirement of multimedia items. Watermarking is the most often used method for adding security to photographs. In many cases, using a watermarking strategy to provide security is not viable. Because the security message is visible, hackers may add a watermark on the original image, just like the sender did, and then send the changed image to the recipient. The copyright information is available to everybody. The unique intrinsic fingerprint of the image source coders is used as proof for security to overcome difficulties in the watermarking technique. A forensic detector is built based on the inherent fingerprint of image source encoders. This detector determines which source encoder is being used, as well as the coding parameters and confidence measures for the output.

1. Introduction

Data exchange in audio-visual processing and network technologies has enabled the dissemination and sharing of multimedia material through networks, while also increasing the security concerns of multimedia contents. Hacking router data, altering the original data sent by the source, and retransmitting the changed data to the destination has become more common in network technology.

As a result, my article is being utilised to create algorithms for detecting and classifying original images from network transmissions. The approach is motivated by picture validation and image transmission security. Using the tool, the algorithm can determine if the image received is genuine or a counterfeit. The rapid confluence of multimedia signal processing, communications, and networking technologies has expedited the interchange of digital multimedia data and permitted widespread digital media distribution during the last few decades.

News reporting, insurance claim investigation, criminal investigation, and a variety of other applications have all made extensive use of digital photographs. Individuals may, however, access, replicate, or change information because of its digital nature. Traditional forensic techniques safeguard multimedia material by concealing new data in the original signal via proactive and additive methods.

A digital watermark was inserted into the image at the time of acquisition, for example, to make the trustworthiness of digital photos responsible. Changes in the digital watermark can be used to identify any later alteration of the image. Similarly, user identity information is encoded in each spread copy in traitor-tracing digital fingerprinting to identify the matching user and locate the source of the unlawful copies.

However, it requires that all camera manufacturers agree on a single standard, and implementing such extrinsic safety methods may be too expensive and unfeasible for some real-world applications. Extrinsic measures are frequently ineffective in enforcing content protection. Each copy of multimedia data, on the other hand, has its own capture, processing, and transmission procedure.

2. Literature survey

JPEG lossy compression operations are tolerated by an image authentication system. In the highlighted picture, an encrypted feature vector generated from the image DCT coefficients is implanted redundantly and invisibly. The feature vector from the received picture is calculated again on the receiver side and compared to the extracted watermark to validate the image authenticity. This approach is resistant to JPEG compression up to an 80 percent maximum compression, but vulnerable to malicious assaults such as cutting and copying.

Each disseminated copy is individually labelled with the user's ID, allowing for proactive tracking of multimedia distribution. Multi-user collusion is a potent anti-digital fingerprinting method in which a number of attackers work together to delete the embedded identity information. It examines side information based multimedia fingerprinting to combat such multi-user collusion and to enable multimedia forensics.

It explains how to use image authentication to take advantage of the generation and storage of an embedded image thumbnail. A sequence of filtering procedures, contrast adjustment, and compression are used to represent the development of a thumbnail. It calculates the model parameters automatically and illustrates how they differ dramatically across camera manufacturers and photo-editing software. Also, explain how this signature may be paired with encoding information from the underlying full-resolution picture to improve the signature's uniqueness.

Computer visuals are becoming increasingly lifelike as technology develops. As a result, methods for differentiating between genuine photos taken with digital cameras and computer-generated images must be developed. It explains an innovative solution to this problem. It detects that photographs from digital cameras contain signs of re sampling as a consequence of utilising a colour filter array with demosicing techniques, rather than focusing on statistical differences between the images textures.

Each picture site has a filter above it that is sensitive to the red, green, or blue component of the incident light. Other colour filter array designs and filters are occasionally employed, but the Bayer is by far the most popular. At each pixel point, the raw picture from the image sensor comprises just a single signal value. Furthermore, this pixel value corresponds to a single colour component (red, green, or blue in the case of the Bayer filter array).

3. Methodology

One of the increasing issues in the field of digital picture forensics is the identification of copy-move forgeries. To overcome this issue, a variety of approaches have been offered. One of the most difficult challenges these systems faced was detecting duplicated picture portions without being influenced by standard image processing procedures such as compression, noise addition, and rotation.

- **JPEG Compression History Estimation for Color Images**

You'll frequently come across digital colour photographs that have been compressed with JPEG. Its goal was to retrieve the different parameters used during prior JPEG operations, which were referred to as JPEG compression history (CH). This data is frequently lost on the way to the image's current representation.

Due to quantization, the discrete cosine transform coefficient histograms of previously JPEG-compressed pictures show near-periodic behaviour. It uses simulations to illustrate the accuracy of estimates before providing a statistical technique to utilise this structure to estimate the image's CH.

JPEG is the most widely used compression format for digital colour photographs. It compresses images by quantizing the DCT coefficients of the image's three colour planes; for a quick review of JPEG. The different parameters utilised during JPEG compression and decompression, on the other hand, are not standardised.

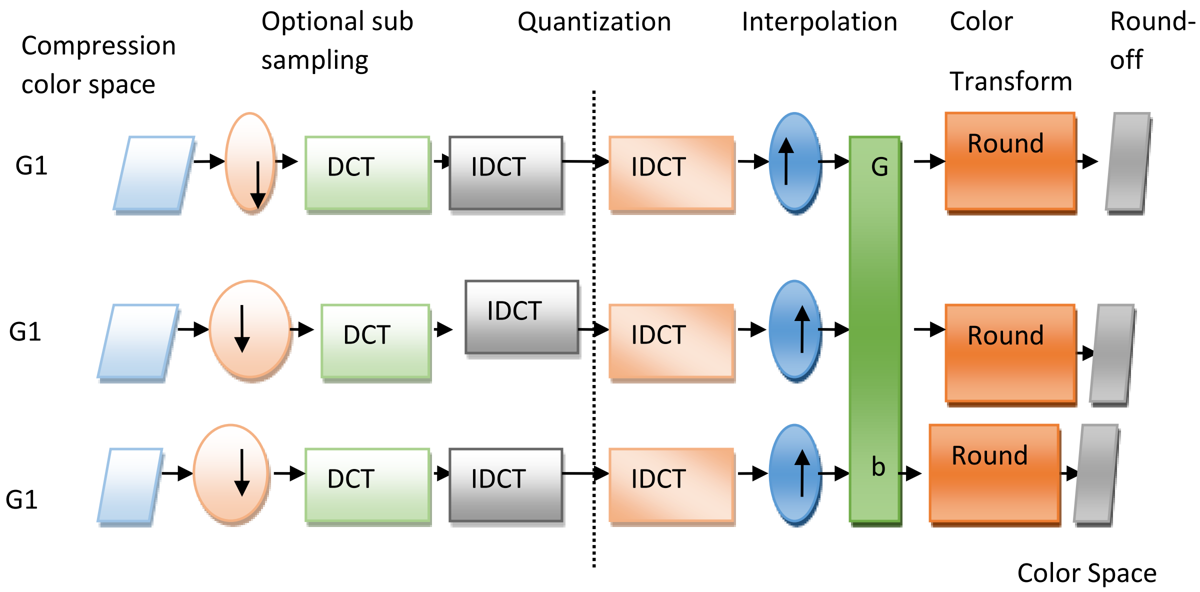

Fig.1 Overview of JPEG Compression and Decompression

- **Estimation of Primary Quantization Matrix for Steganalysis of Double-Compressed JPEG Images**

If a JPEG picture has been compressed twice, each time using a different quantization matrix but the same 8 by 8 grid, it is called double-compressed. Some well-known steganographic algorithms (Jsteg, F5, and OutGuess) output double-compressed stego pictures by default. If double alters the statistics of DCT coefficients, it has a detrimental impact on the accuracy of various steganalysis methods based on the assumption that the stego picture is only single-compressed.

- **Double-compression detector**

The double-compression detector's classifiers were trained on 10,000 single-compressed and 10,000 double-compressed picture samples. In the case of double-compressed photos, images in the training set were chosen at random with a uniform distribution of steganographic techniques, message lengths, and major quality factors. It doesn't employ photos from L that don't have double-compression artefacts in their histograms (the cases when SQS were divisors of the PQS). These were SQF 75 and PQF 74, 75, 96, 98 photographs, as well as SQF 80 and PQF 80, 96, 98 images.

- **Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact**

With today's commonly accessible image editing tools, it's simple to fabricate digital photographs. It proposes a passive method for detecting digital forgeries by examining blocking artefact discrepancies. It discovers that the blocking artefacts created during JPEG compression may be utilized as a "natural authentication code" when given a digital image. The estimated quantization table is then used to suggest a blocking artefact measure based on the power spectrum of the DCT coefficient histogram.

4. Result and discussion

A passive method for detecting digital picture counterfeiting that uses JPEG blocking artefacts to measure quality discrepancy. This method can identify spliced picture forgeries that use a different quantization table, as well as forgeries that cause blocking artefact inconsistencies in the whole image, such as block mismatching and object retouching. Furthermore, the quantization table estimation procedure is substantially quicker than approaches based on greatest likelihood.

Table.1 Quantization table for Nikon Coolpix5400

1	1	1	1	1	2	2	2
1	1	1	1	1	2	2	2
1	1	1	1	2	2	3	2
1	1	1	1	2	3	3	2
1	1	1	2	3	4	4	3
1	1	2	3	3	4	5	4
2	3	3	3	4	5	5	4
3	4	4	4	4	4	4	4

Table.2 Quantization table for Sony P10

1	1	1	1	1	2	3	3
1	1	1	1	1	3	3	3
1	1	1	1	2	3	3	3
1	1	1	1	3	4	4	3
1	1	2	3	3	5	5	4
1	2	3	3	4	5	6	5
2	3	4	4	5	6	6	5
4	5	5	5	6	5	5	5

The detection of digital counterfeiting without the use of a signature or a watermark is a new study area. A passive method for detecting digital forgeries based on image quality anomalies induced by JPEG compression blocking artefacts.

5. Conclusion

Because the unique intrinsic fingerprint of the image source encoder is incorporated in the received picture, the forensic detector does not require any information other than the decoded image at the receiver. This technique is not suited for providing security to digital photos due to several issues with the watermarking approach. As a result, the Intrinsic Fingerprint Forensic Detector is created. This method offers higher security than the extrinsic method. The digital picture is more secure than watermarking because it uses the intrinsic fingerprint of each source coder.

References

1. Adams, J., and Hamilton, J. (1997) ’Design of practical filter array interpolation algorithms for digital cameras’. Proc. SPIE.
2. Bayram, S., Avcibas, I., Sankur and Memon, B. N. (2006) ‘Image manipulation detection,” Journal of ElectronicImaging, Volume 15, Issue4, 041102 (17 pages), vol. 15(4).
3. Bayram, S., Sencar, H. T. and Memon, N.(2005) ‘Source Camera Identification Based on CFA
4. Buccigrossi, R.W. and Simoncelli, E.P. (1999) ‘Image compression via joint statistical characterization in the wavelet domain’, IEEE Transactions on Image Processing, 8(12):1688.1701.
5. Chang, Y.C. and Reid, J.F. (1996) ‘RGB calibration for analysis in machine vision’. IEEE Transactions on Pattern Analysis and Machine Intelligence, 5(10):1414–1422.
6. Chupeau, B., Massoudi, A. and Lefèbvre, F. (2007) “Automatic estimation and compensation of geometric distortions in video copies”, Proc. SPIE 6508
7. Devernay, F. and Faugeras, O. (1995) ‘Automatic calibration and removal of distortion from scenes of structured environments,’ In SPIE Conference on Investigative and Trial Image Processing, San Diego, CA, 1995.
8. Fridrich, J. And Luk´a˘s, J. (2003) ‘Estimation of primary quantization matrix in double compressed JPEG images’. In Digital Forensic Research Workshop.
9. Friedman, G. L. (1993) ‘The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image’, IEEE Trans. Consumer Electron. Vol. 39, pp. 905-910.
10. Fridrich, F., Soukal, D. and Lukas, J. (2003) ‘Detection of Copy-Move Forgery in Digital Images’, Digital Forensic Research Workshop, Cleveland, USA, Aug.