THE INTERNATIONAL JOURNAL OF
SCIENCE & TECHNOLEDGE

Jpeg Anti-Forensics of Undetectability and Image Quality

S. Mohanapriya
PG Scholar, Sir Issac Newton College of Engineering and Technology,
Nagapattinam, Anna University Chennai, India.
E. Saranya
Asst.Professor, Sir Issac Newton College of Engineering and Technology,
Nagapattinam, Anna University Chennai, India.

Abstract:
This paper proposes aJPEG anti-forensic method, which aims at removing the footprints left by JPEG compression in both the spatial domain and DCT domain, with reasonable loss of image quality, the proposed method can defeat existing forensic detectors that attempt to identify traces of the image JPEG compression history or JPEG anti-forensic processing. In our framework, first because of a total variation-based deblocking operation, the partly recovered DCT information is thereafter used to build an adaptive local dithering signal model, which is able to bring the DCT histogram of the processed image close to that of the original one. Then, a perceptual DCT histogram smoothing is carried out by solving a simplified assignment problem, where the cost function is established as a total perceptual quality loss due to the DCTcoefficient modification. The second-round deblocking and decalibration operations successfully bring the image statistics that are used by the JPEG forensic detectors to the normal status. Experimental results show that the proposed method outperforms the state-of-the-art methods in a better tradeoff between theJPEG forensic undetectability and the visual quality of processed images.

Keywords: *JPEG-antiforensic, Image acquisition, DCT histogram smoothing,Quantization,dithering signal, total variation, assignment problem.*

1. Introduction

Due to the widespread availability of digital cameras and the rise of the Internet as a means of communication, digital images have become an important method of conveying visual information. Increasing development of high-quality camerasand powerful photo-editing tools significantly reduces the difficulty to make visually plausible fake images. Doctored images are appearing with growing frequency, for instance,in advertising and in political and personal attacking. To prevent digital image forgeries from being passed off as unaltered originals, researchers have developed a variety of digital image forensic techniques. Anti-forensics, whose objective is to mislead forensic investigators, can help researchers to study the weaknesses in existing forensictechniques for further development of trustworthy digital forensics [1].

Fan and De Queiroz well studied the artifacts left by JPEG compression in [2], where two forensic detectors were proposed to detect JPEG artifacts in the DCT domain andin the spatial domain, respectively. In order to conceal the JPEG compression history of digital images, Stamm etal. [3] pioneered the work of JPEG anti-forensics, trying tofill the gaps in the comb-like distribution of DCT coefficients in each subband. In their work, a dithering operation is proposed to conduct DCT histogram smoothing based onthe Laplacian model for AC component coefficients. This dithering operation successfully fools the detector in [2] that examines DCT-domain artifacts. Stamm et al. later proposed to carry out a deblocking operation based on median filtering [4] after the DCThistogram smoothing [3].

Later on, researchers pointed out that the JPEG anti-forensic processing in [3] leaves footprints which can be detected by two advanced detectors [4], [5]. Another disadvantage of the method in [3] is to noticeably degrade the image visual quality, which however can be improved, to some extent, by a perceptual anti-forensic dithering method [6]. In order to fool some existing JPEG forensic detectors (not machine learning based) as well as to keep a high visual quality of the processed image, an approach to JPEG anti-forensics is proposed in [7], which attempts to remove the blocking artifacts in the spatial domain of the image through a variational energy minimization.

It is worth noticing that some relative work can also be adopted either for JPEG anti-forensics, e.g., the double JPEG compression anti-forensic method in [8], In our previous JPEG anti-forensic work [7], we mainly focused on removing JPEG blocking artifacts in the spatial domain. In this paper, we extend and improve it, mainly by integrating a further step of explicit smoothing of the DCT histogram. An extended four-step procedure is proposed, which is composed of total variation (TV)-based deblocking, perceptual DCT histogram smoothingbased on an adaptive local dithering signal model, secondround TV-based deblocking and de-calibration. The effectiveness of the proposed anti-forensic method is confirmed by its undetectability against existing JPEG forensic detectors [2], [4], [5], [7], [15], in both the spatial and the DCTdomains.

2. Basics of JPEG Compression

In this section we explain the basics of JPEG Compression and Corresponding footprints. JPEG itself encodes each component in a colour model separately, and it is completely independent of any colour-space model, such as RGB, HSI, or CMY. The best compression ratios result if a luminance/chrominance colour space, such as YUV or YCbCr, is used. The luminance describes the brightness of the pixel while the chrominance carries information about its hue. These three quantities are typically less correlated than the (*R, G, B*) components.

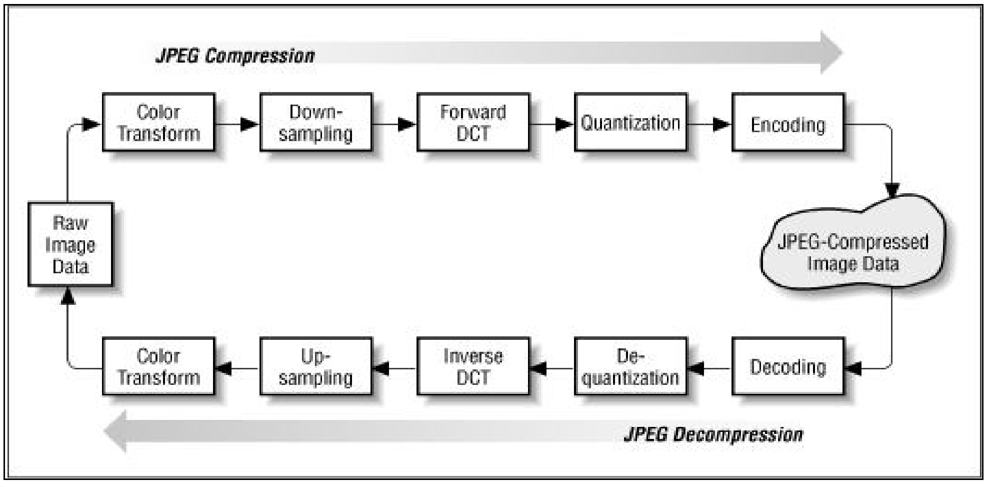


Figure 1: Jpeg compression process

Furthermore, psycho-visual experiments demonstrate that the human eye is more sensitive to luminance than chrominance, which means that we may neglect larger changes in the chrominance without affecting our perception of the image.

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.29900 & 0.58700 & 0.11400 \\ -0.16874 & -0.33126 & 0.50000 \\ 0.50000 & -0.41869 & -0.08131 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}.$$

Figure 2: Rcb to ycrcb conversion

Since this transformation is invertible, we will be able to recover the *(R, G, B)* vector from the *(Y, Cb, Cr)* vector. This is important when we wish to reconstruct the image. (To be precise, we usually add 128 to the chrominance components so that they are represented as numbers between 0 and 255.). When we apply this transformation to each pixel in our block. We obtain three new blocks, one corresponding to each component. These are shown below where brighter pixels correspond to larger values. The image is then divided into 8 by 8 blocks of pixels. each 8×8 block of each component (Y, Cb, Cr) is converted to a frequency-domain representation, using a normalized, two-dimensional type-II discrete cosine transform (DCT).

$$G_{u,v} = \frac{1}{4}\alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} g_{x,y}\cos\left[\frac{(2x+1)u\pi}{16}\right]\cos\left[\frac{(2y+1)v\pi}{16}\right]$$

Figure 3: Discrete cosine transform equation

When a gray scale image undergoes JPEG compression, it inserts segmented into a series of 8×8pixel blocks, then the DCT of each block is computed. Next, each DCT coefficient is quantized by dividing it by its corresponding entry in a quantization matrix Q, such that a DCT coefficient X at the blockposition (i, j) is quantized to the value $\dot{X}$= round(X/Qi,j). Finally, the quantized DCT coefficients are rearranged using the zigzag scan order and losslessly encoded. To decompress the image, the sequence of quantized DCT coefficients is losslessly decoded then rearranged into its original ordering. De quantization is performed by multiplying each quantized coefficient by its corresponding entry in the quantization matrix, resulting in the de-quantized coefficient Y=Qi,j* X.

Finally, the inverse DCT (IDCT) of each block of DCT coefficients is computed and the resulting pixel values are rounded to the nearest integer. Pixel values greater that 255 or less than 0 are truncated to 255 or 0 respectively, yielding the decompressed image. Due to quantization process the de-quantized coefficient can only assume values that are integer multiples of quantization step size. Thus histogram of de-quantized coefficient of the ith sub-band appears to be comb shape with peaks spaces apart by quantization step size. We refer this characteristic comb shape of D.C.T. coefficient histogram as JPEG compression footprints.

This process reveals two details, the first is that quantization process has occurred earlier and second is the original quantization step size can be revealed which was used[9].

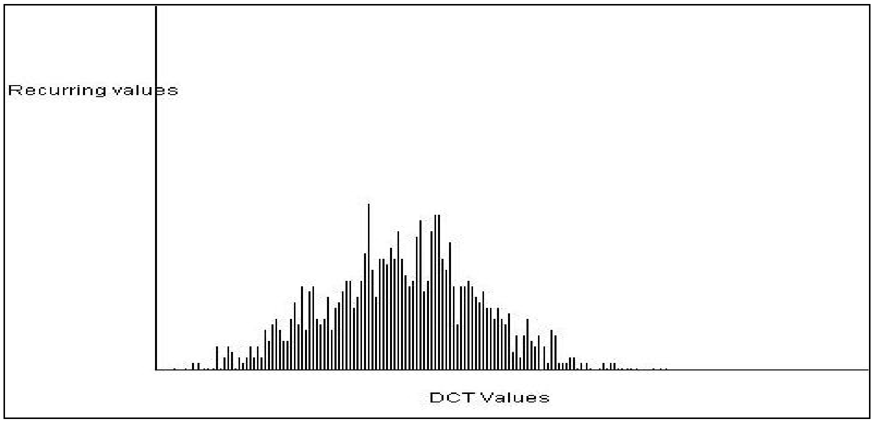


Figure 4: Original image histogram

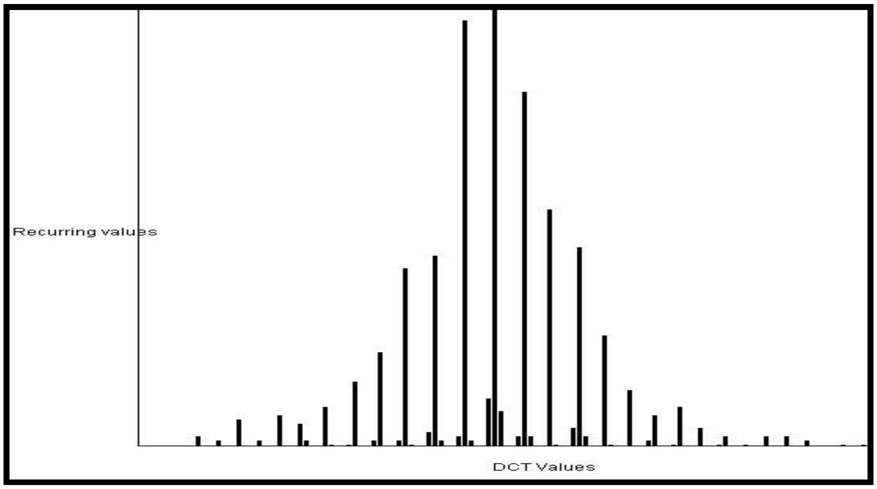


Figure 5: Compressed Image Histogram

3. Background

3.1. Detecting Jpeg Compression

Fan and De Queiroz [2] proposed an algorithm for maximum-likelihood estimation (MLE) of the JPEG quantization table, from a spatial-domain bitmap representation of the image. The method can also serve as a detector to classify an image as not JPEG compressed, if each entry of the estimated quantization table is either 1 or “undetermined” [2], [3]. Focusing on 8×8 block boundaries, Fan and De Queiroz [2] also proposed a JPEG blocking signature measure as:

$$KF = \sum_{k} |HI\ (k) - HI\ I\ (k)|$$

Where*HI* and *HI I* are normalized histograms of pixel value differences across block boundaries and within the block,respectively (see [2] for details).

3.2. Jpeg Anti-Forensics

Valenzise *et al*. proposed a perceptual anti-forensic dithering operation [16], whose resulting JPEG forgery has a higher perceptual quality than the one processed by Stamm *et al.*’s dithering method [2]. A “just-noticeable distortion” [17] criterion is adopted to control the amount of introduced distortion. A minimum-cost bipartite graph matching problem is used as the mathematical model for the adaptive insertion of the dithering signal. A greedy algorithm is implemented to get an approximate solution in order to reduce the computation cost. Moreover, some relative techniques can also be extended for JPEG anti-forensics, *e.g.*, the Shrink-and-Zoom (SAZ) attack proposed by Sutthiwan and Shi [5], though it was initially designed for double JPEG anti-forensics. Given a JPEG image,a shrinkage (image down-scaling) operation is firstly applied; then the processed image is zoomed back to the same size as the original one, to obtain the JPEG anti-forensic image.

3.3. Countering Jpeg Anti-Forensics

Valenzise *et al.* [15], [16] claimed that the dithering signal of [2] degraded the image quality by introducing noises. Inspired by the JPEG ghost’s detector, they designed an efficient detector against JPEG anti-forensic dithering, which examines the noisiness of re-compressed versions of the image under test. The TV of the re-compressed image (the ℓ1 norm of the spatial first-order derivatives) [13] is employed as the image noisiness measure. For a given image, the detector re-compresses it using different quality factors $q = 1,2, \ldots, 100$, as a function of which, TV*(q)* is computed as the total variation of the re-compressed image.

4. Proposed Method

In this section, we propose a novel method for JPEG anti-forensics which can remove from a JPEG image boththe blocking artifacts in the spatial domain and the DCT quantization artifacts in the DCT domain. Our method is able to fool existing JPEG forensic detectors, meanwhile it ensures a high visual quality of the processed image.In practice, we find it extremely difficult to conduct a single step attack to defeat multiple JPEG forensic detectors that work in different domains, while keeping a high image visualquality. Therefore, in this paper, we consider removing JPEG artifacts alternatively in the spatial and in the DCT domains.

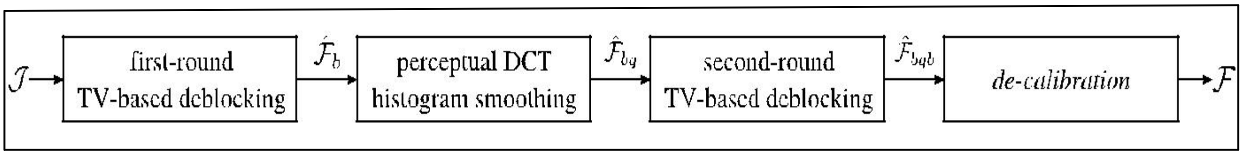

$\mathcal{J}$
first-round TV-based deblocking
$\hat{\mathcal{F}}_b$
perceptual DCT histogram smoothing
$\hat{\mathcal{F}}_{bq}$
second-round TV-based deblocking
$\hat{\mathcal{F}}_{bqb}$
de-calibration
$\mathcal{F}$

Figure 6: The proposed JPEG forgery creation process

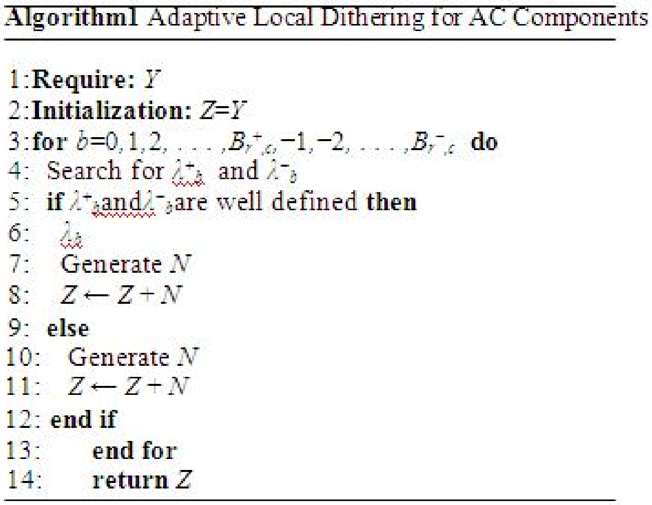
4.1. JPEG constrained using TV based variation

For JPEG deblocking purposes, we hereby propose a variational approach to minimize a TV-based energy consisting of a TV term and a TV-based blocking measurement term. TV-based deblocking in the spatial domain such as besides the removal of JPEG blocking artifacts, another purpose of this step is to partly and plausibly fill gaps in the DCT histogram, so as to facilitate the following step of explicit histogram smoothing. Experimentally, it is necessary and beneficial to conduct this first-round deblocking, especially for a better histogram restoration in the high frequency subbands where all DCT coefficients are quantized to zero in the JPEG image. The final result of this provides us with asatisfying intermediate image ˆ*F b*.

4.2. Histogram Smoothing

After JPEG image *J* has been processed using the TV-based deblocking method, the gaps in the DCT domainhave been partly filled in the obtained image ˆ*F b* (an example DCT histogram is shown in Fig. 7-(c)). In order to achieve a better forensic undetectability, it is necessary to fill the gaps left in the DCT histogram of ˆ*F b*.In this section, we propose a perceptual DCT histogram smoothing method, the partly recoveredinformation in the DCT domain of ˆ*F b* will help us to build an adaptivelocal dithering signal model based on both the Laplacian distribution and the uniform distribution for a better goodness-of-fit.

In the deblocked image ˆ*F b*, the comb-like DCT quantization artifacts are no longer as obvious as those in the JPEG image *J* (an example is shown in Fig. 7-(c)). Under the hypothesis that the partly recovered DCT-domain information is reliable, the next step naturally goes to further filling the remaining gaps in the DCT histogram. This leads us to the construction of an adaptive local model for the DCT coefficient distribution, with which a perceptual histogram mapping method is thereafter proposed to modify the DCT coefficients while minimizing the total SSIM (structural similarity) [14] value loss.


Algorithm1 Adaptive Local Dithering for AC Components

```
Require: $Y$
Initialization: $Z=Y$
for $b=0,1,2,\ldots,B^+_{r,c},-1,-2,\ldots,B^-_{r,c}$ do
  Search for $\lambda^+_b$ and $\lambda^-_b$
  if $\lambda^+_b$and$\lambda^-_b$are well defined then
    $\lambda_b$
    Generate $N$
    $Z \leftarrow Z+N$
  else
    Generate $N$
    $Z \leftarrow Z+N$
  end if
end for
return $Z$
```

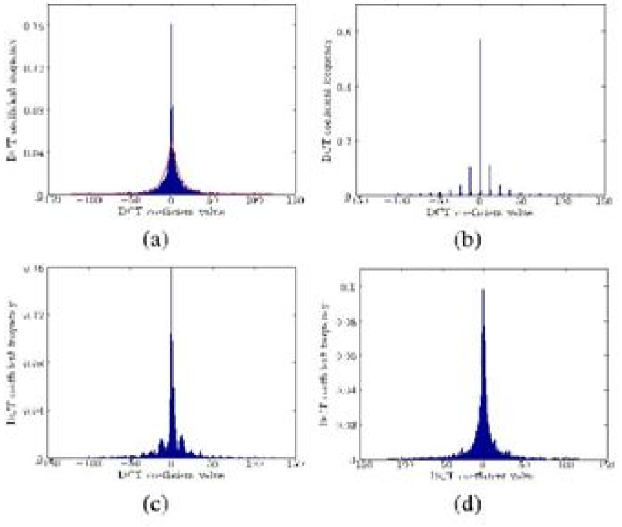


Figure 7: (a) is the DCT histogram of subband (2, 2) from an example genuine, uncompressed UCID-v2 image, and the red curve is the fitting result using the discrete Laplacian distribution model. Then the image is JPEG compressed with quality factor 50, and the proposed JPEG anti-forensic method is applied. (b), (c), and (d) are the corresponding DCT histograms of (a) in the JPEG image, after the first-round TV-based deblocking, and after the adaptive local dithering signal is injected respectively.

Furthermore, *F̂bq* achieves a slightly higher PSNR value, but slightly lower SSIM value, than *F̂q*. Considering theresults of both metrics, the two kinds of images have comparable visual qualities. Another advantage of the TV-based deblocking is the removal of JPEG blocking artifacts. It is therefore necessary to conduct the first-round TV-based deblocking for a better tradeoff between the visual quality and the histogram restoration quality of the processed image.

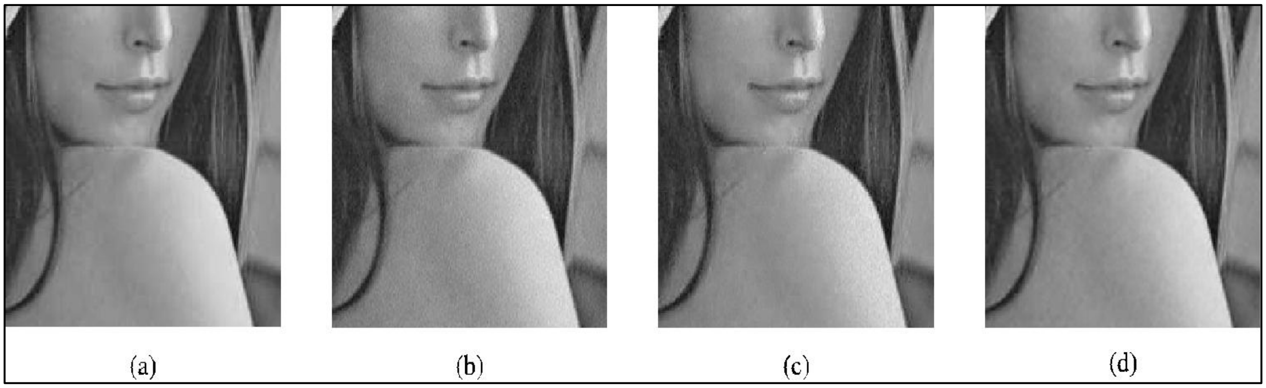


Figure 8: Example results (close-up images) around the shoulder of Lena of ˆF bq compared with J, FS, and FV, where J is compressed with quality factor 50. Their SSIM values (with I as the reference) are: (a) 0.9809, (b) 0.9509, (c)0.9610, and (d) 0.9731. We can see that less noise is introduced in ˆFbq especially in the relatively smooth area of the imag

4.3. Deblocking

Second round TV-based deblocking and regularization in this section again move to spatial domain, here the removal of the DCT quantization artifacts is at the cost of introducing a small amount of unnatural noise and blocking artifacts in the spatial domain to the output image *ˆFbq*, despite that we have tried to minimize the image quality loss. The procedure is basically the same as that in 4.A, yet with some modifications to the parameter setting. The created image after this step is denoted as *ˆFbqb*. The resulting image *ˆFbqb* is at last processed by the *decalibration* operation to generate the JPEG forgery *F*.

4.4. Decalibration

For *ˆF bqb*, all the existing detectors seems to be well fooled except the calibrated feature based detector [5]. In this section decalibration is simply carried out by means of using optimize an energy function otherwise in order to fool the detector, a random threshold for each image is drawn from the distribution of the calibrated feature values for genuine, uncompressed images, or directly minimize the calibrated feature value. The minimization problem is formulated as:

$$X* = \arg\min_{X} \sum_{k=1}^{28} \left| \mathrm{var}\,(\mathrm{D}k\,X) - \mathrm{var}\,(\mathrm{D}k\,Xcal) \right|$$

After decalibration, the JPEG forgery *F* is obtained.

5. Experimental Results

The following fig shows the experimental results by using the proposed system for the test bed data of uncompressed image from UCID-v2.

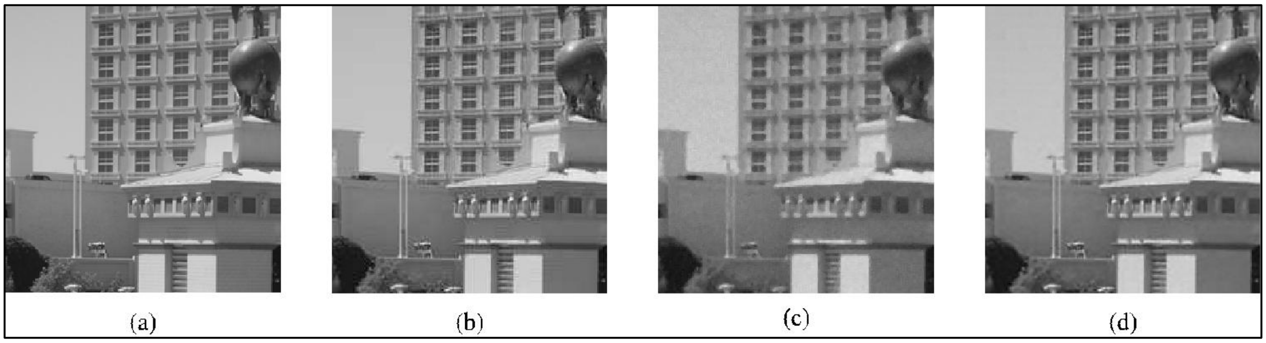


Figure. 9. Example results (close-up images) of F compared with I (an uncompressed image from UCID-v2), J, and F_{SqSb}, where J is compressed with quality factor 50. Our JPEG forgery F has a better image quality compared with F_{SqSb} [3], [16]. (a) I. (b) J. (c) F_{SqSb}. (d) F.

6.Conclusion

JPEG anti-forensic images be passed off as never compressed by testing under existing JPEG forensic detectors. However we are aware that there might still exist some artifacts which can be detected by more reliable detectors to be designed in the future. Further research shall be devoted to advanced optimization methods for solving the minimization problems, and to smoothing the DCT coefficient histogram to better approximate the original distribution.

7.Reference

1. R. Bohme and M. Kirchner, “Counter-forensics: Attacking image forensics,” in Digital Image Forensics, H. T. Sencar and N. Memon, Eds. New York, NY, USA: Springer-Verlag, 2013, pp. 327–366.
2. Z. Fan and R. L. De Queiroz, “Identification of bitmap compression history: JPEG detection and quantizer estimation,” IEEE Trans. ImageProcess., vol. 12, no. 2, pp. 230–235, Feb. 2003.
3. M. Stamm, S. Tjoa, W. S. Lin, and K. J. R. Liu, “Anti-forensics of JPEG compression,” in Proc. IEEE Int. Conf. Acoust., Speech, SignalProcess., Mar. 2010, pp. 1694–1697.
4. G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, “Countering JPEG anti-forensics,” in Proc. 18th IEEE Int. Conf. Image Process., Sep. 2011, pp. 1949–1952.
5. S. Lai and R. Bohme, “Countering counter-forensics: The case of JPEG compression,” in Proc. Int. Conf. Inf. Hiding, 2011, pp. 285–298.
6. G. Valenzise, M. Tagliasacchi, and S. Tubaro, “The cost of JPEG compression anti-forensics,” in Proc. IEEE Int. Conf. Acoust., Speech,Signal Process., May 2011, pp. 1884–1887.
7. W. Fan, K. Wang, F. Cayre, and Z. Xiong, “A variational approach to JPEG anti-forensics,” in Proc. IEEE Int. Conf. Acoust., Speech, SignalProcess., May 2013, pp. 3058–3062.
8. P. Sutthiwan and Y. Q. Shi, “Anti-forensics of double JPEG compression detection,” in Proc. Int. Workshop Digital Forensics Watermarking, 2011, pp. 411–424.
9. `zRevealing the Traces of JPEG Compression Anti-Forensics” in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 2, FEBRUARY 2013.
10. Z. Wei and K. N. Ngan, “Spatio-temporal just noticeable distortion profile for grey scale image/video in DCT domain,” IEEE Trans. CircuitsSyst. Video Technol., vol. 19, no. 3, pp. 337–346, Mar. 2009.
11. G. Valenzise, M. Tagliasacchi, and S. Tubaro, “Revealing the traces of JPEG compression anti-forensics,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 2, pp. 335–349, Feb. 2013.
12. H. Farid, “Exposing digital forgeries from JPEG ghosts,” IEEE Trans.Inf. Forensics Security, vol. 1, no. 4, pp. 154–160, Mar. 2009.
13. L. I. Rudin, S. Osher, and E. Fatemi, “Nonlinear total variation based noise removal algorithms,” Phys. D, Nonlinear Phenomena, vol. 60, nos. 1–4, pp. 259–268, 1992.
14. Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEETrans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.
15. W. Luo, J. Huang, and G. Qiu, “JPEG error analysis and its applications to digital image forensics,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 480–491, Sep. 2010.
16. M. Stamm, S. Tjoa, W. S. Lin, and K. J. R. Liu, “Undetectable image tampering through JPEG compression anti-forensics,” in Proc. 17thIEEE Int. Conf. Image Process., Sep. 2010, pp. 2109–2112.
17. H. Li, W. Luo, and J. Huang, “Countering anti-JPEG compression forensics,” in Proc. IEEE Int. Conf. Image Process., Oct. 2012,pp. 241–244.