Detection Methods for Altered Photograph

1 Introduction

The advent of low-cost and high-resolution digital cameras, and sophisticated photo-editing software, has made it remarkably easy to manipulate and alter digital images. In addition, digital forgeries, often leaving no visual clues of having been tampered with, can be indistinguishable from authentic photographs. And while the technology to manipulate digital media is developing at break-neck speeds, the technology to contend with its ramifications is lagging behind. In this report, we will go to explain some of the methods use to detect tampering images.

2 Methods of detection

a. Re-sampling

Consider the scenario in which a digital forgery is created by splicing together two, or more, individual images. In order to create a convincing match, it is often necessary to re-size, rotate, or stretch the images, or portions of them. These manipulations require re-sampling an image onto a new sampling lattice using some form of interpolation. Although the re-sampling of an image is often imperceptible, specific correlations are introduced in the re-sampled image. When detected, these correlations represent evidence of tampering. We describe the form of these correlations, and propose an algorithm for detecting them in any portion of an image.

The re-sampling signals in 1-D can be modified with 3 steps:

1. Up-sample
2. Interpolate
3. Down-sample

Different types of re-sampling algorithms (e.g., linear, cubic) differ in the form of the interpolation in step 2.Since all three steps in the re-sampling of a signal are linear, this process can be described with a single linear equation. Denoting the original and re-sampled signals in vector form, x and y, respectively, resampling takes the form: $y = Ap/q * x$,where the $n \times m$ matrix Ap/q embodies the entire re-sampling process. Depending on the re-sampling rate, the re-sampling process will introduce correlations of varying degrees between neighboring samples.Depending on the re-sampling rate, the re-sampling process will introduce correlations of varying degree between neighboring samples.

Given a signal that has been re-sampled by a known amount and interpolation method, it is possible to find a set of periodic samples that are correlated in the same way to their neighbors.In practice, of course, neither the re-sampling amount nor the specific form of the correlations are typically known. In order to determine if a signal has been re-sampled, we employ the expectation/maximization algorithm EM to simultaneously estimate a set of periodic samples that are correlated to their neighbors, and the specific form of these correlations. The EM algorithm is a two-step iterative algorithm: (1) in the E-step the probability that each sample belongs to each model is estimated; and (2) in the M-step the specic form of the correlations between samples is estimated.

In cases of 2-D images, the re-sampling of an image introduces periodic correlations. In the re-sampled image, the pixels in odd rows and even columns will be the average of their two closest horizontal neighbors, while the pixels in even rows and odd columns will be the average of their two closest vertical neighbors.

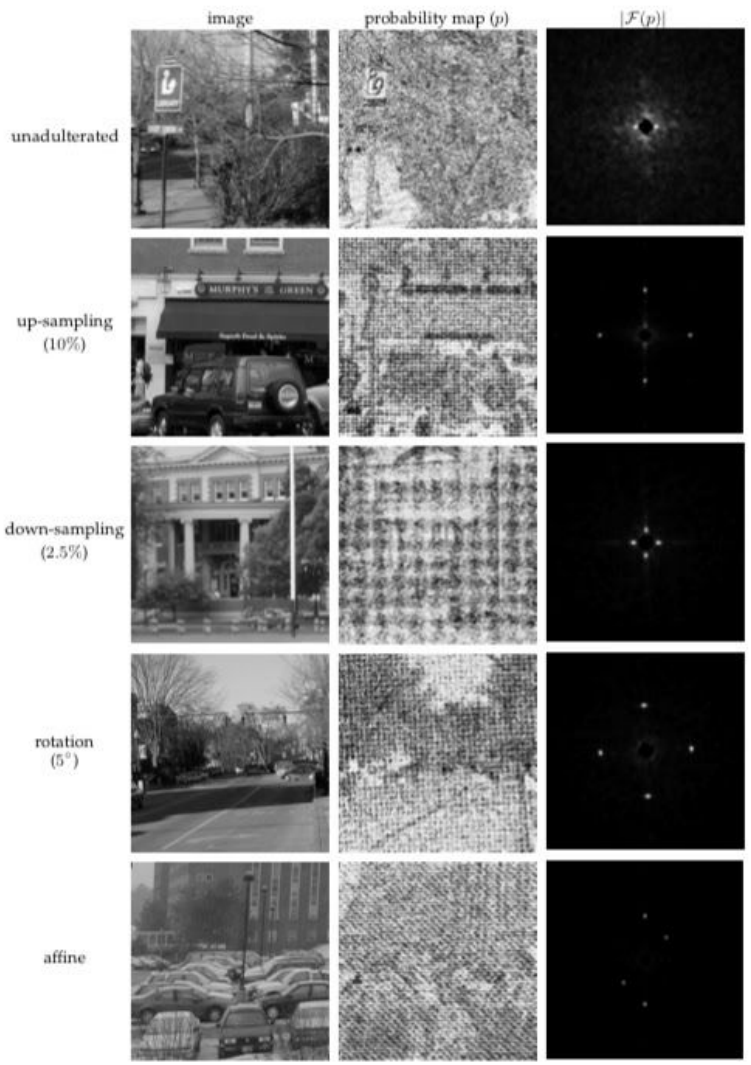


Fig: Shown in the top row is an unadulterated image, and shown below are images re-sampled with different parameters. Shown in the middle column are the estimated probability maps that embody the spatial correlations in the image. The magnitude of the Fourier transforms of these maps are shown in the right-most column. Note that only the re-sampled images yield periodic maps.

b. Double JPEG Compression

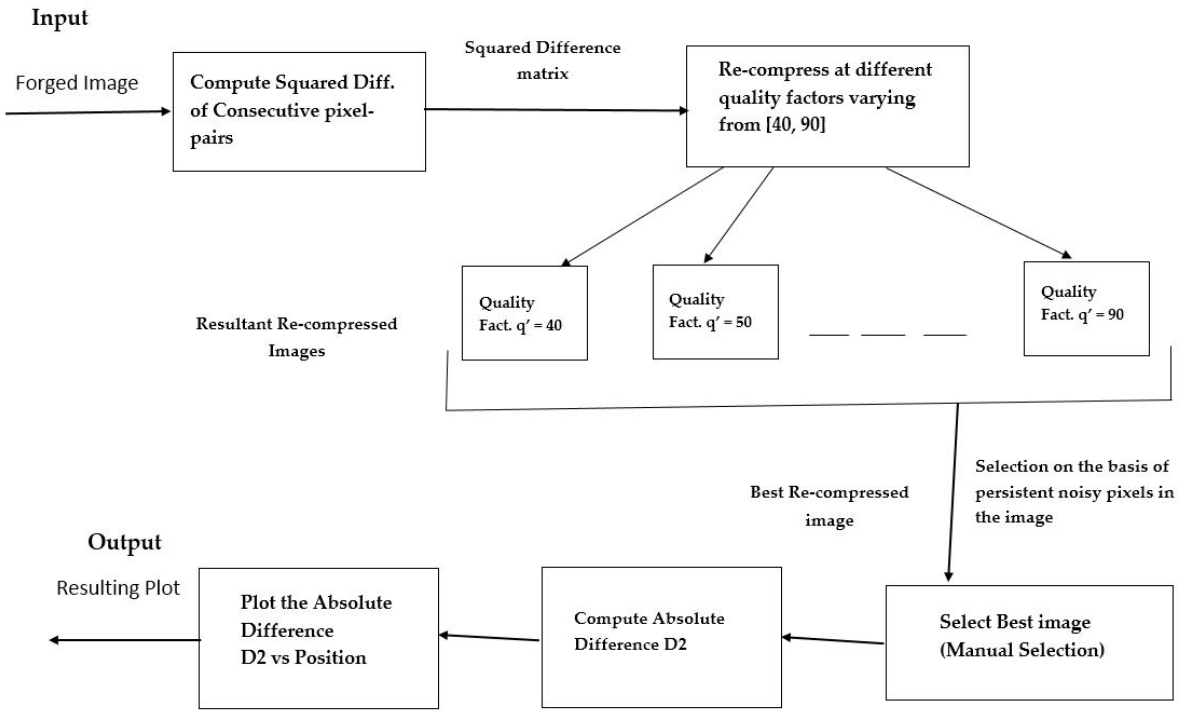
Tampering with a digital image requires the use of a photo-editing software such as Adobe PhotoShop. In the making of digital forgeries an image is loaded into the editing software, some manipulations are performed, and the image is re-saved. Since most images are stored in JPEG format (e.g., a majority of digital cameras store images directly in JPEG format), it is likely that both the original and forged images are stored in this format. Notice that in this scenario the forged image is double JPEG compressed. Double JPEG compression introduces specific artifacts not present in singly compressed images (this observation has also been noted in). Note that evidence of double JPEG compression, however, does not necessarily prove malicious tampering. For example, it is possible for a user to simply re-save a high quality JPEG image with a lower quality. The authenticity of a double JPEG compressed image should, however, be called into question.We start by giving a short description of the JPEG compression algorithm and then quantify the artifacts introduced by double compression.

JPEG is a standardized image compression procedure proposed by a committee with the same name JPEG (Joint Photographic Experts Committee). To be generally applicable, the JPEG standard specified two compression schemes: a lossless predictive scheme and a lossy scheme based on the Discrete Cosine Transform (DCT). The most popular lossy compression technique is known as the baseline method and encompasses a subset of the DCT-based modes of operation. The encoding of an image involves three basic steps:

1. Discrete Cosine Transform
2. Quantization
3. Entropy Encoding

The decoding of a compressed data stream involves the inverse of the previous three steps, taken in reverse order: entropy decoding, de-quantization, and inverse DCT.

Multi-compression based JPEG Forgery Detection



- plot the vector of absolute differences (D2) against pixel positions (P).
- investigate the variation of the elements of D2 over the entire 512×512 image matrix, from the D2 vs. P plot.
- For certain values of q' belonging to [40, 90], the D2 vs. P plot demonstrates a sudden rise, which remains persistent over a range of P, corresponding to the area or region of image tampering.

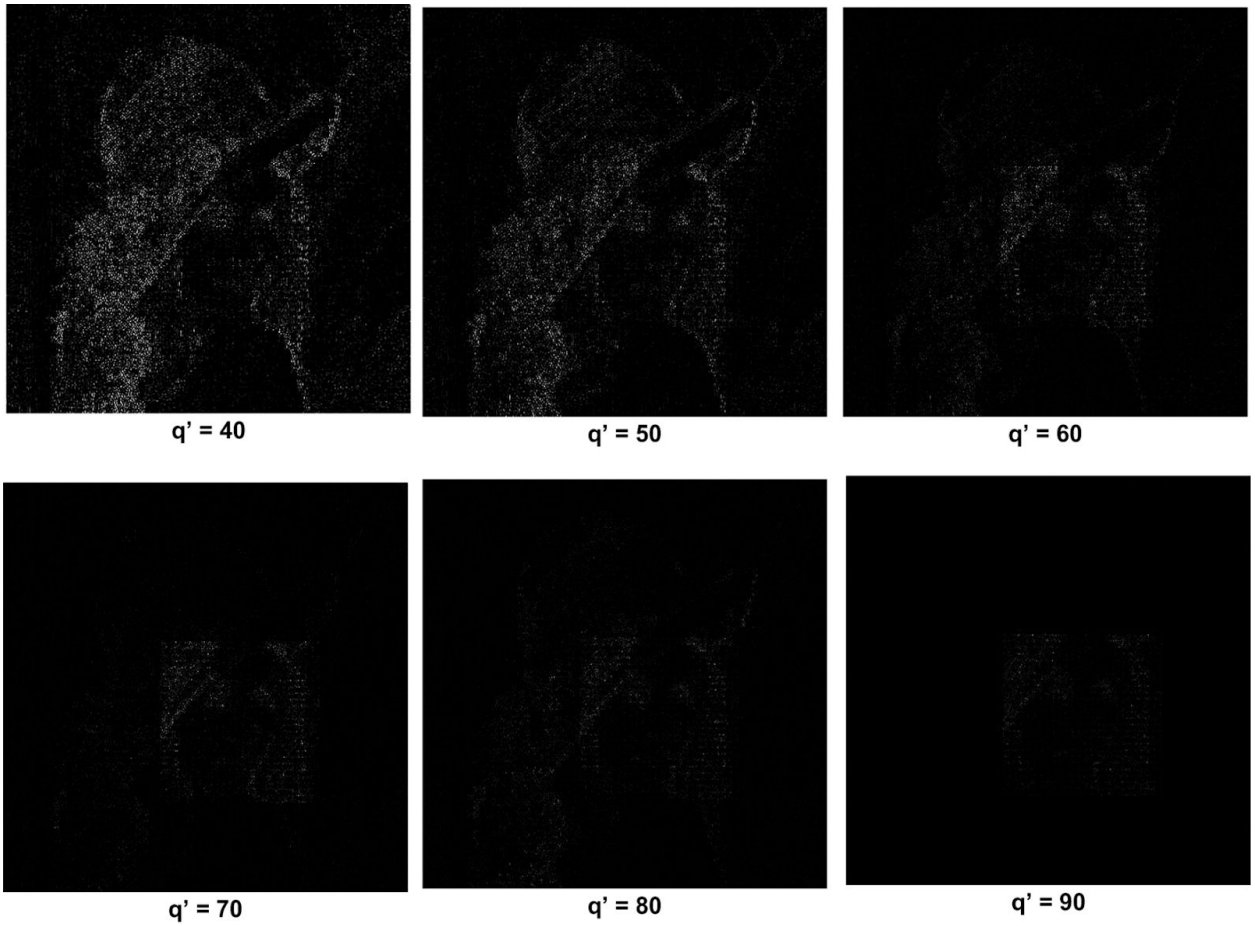
Result :

(a)

(b)

(c)

(a) Original 512×512 image
(b) Central 200×200 portion, re-saved at a different degree of compression
(c) Forged image having its central portion modified



c. Luminance Non-linearities

In order to enhance the perceptual quality of digital images, imaging devices often introduce some form of luminance non-linearity. The parameters of this non-linearity are usually dynamically chosen and depend on the camera and scene dynamics - these parameters are, however, typically held constant within an image. The presence of several distinct non-linearities in an image is a sign of possible tampering.

For simplicity, we assume that pointwise luminance non-linearities can be modeled with a one parameter family of functions of the form: $g(u) = u\gamma$,

where u denotes the intensity of a pixel normalized in the interval [0; 1]. The following technique is used to blindly estimating the value of :

1. sample a range of inverse gamma values 1/γ
2. for each 1/γ in the selected range, apply the inverse function $g{-}1(u) = u1/\gamma$ to the signal, and compute the mean bicoherence
3. select the inverse value 1/γ that minimizes the mean bicoherence.

Shown in the top portion of Fig. 6 is a natural image (1200 1600 pixels in size) and the same image whose upper half has been gamma corrected with = 1:8. The bottom portion shows the estimated gamma values from horizontal scan lines of the unadulterated image (black dots) and the gamma corrected image (white dots). Notice that the values of the gamma estimates from scan lines that span the upper half of the tampered image are generally inconsistent with the lower half.

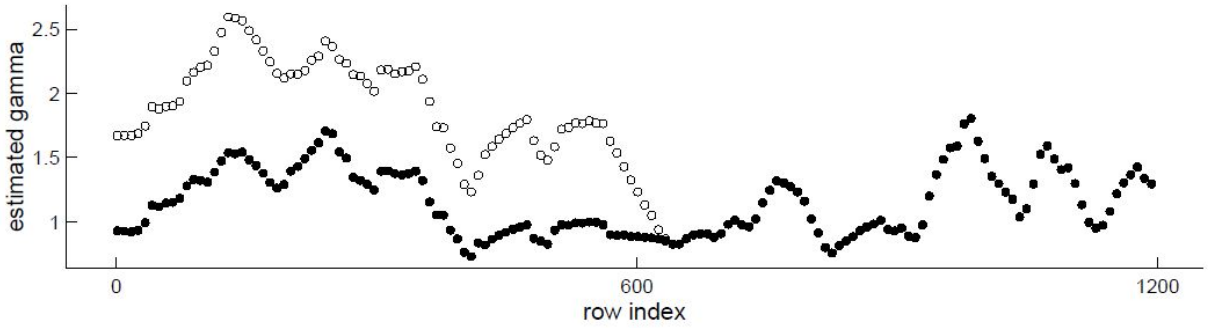


Fig. 6: Top panel: a natural image (left), and the same image whose top portion was gamma corrected with = 1:8 (right). The images are 1200 1600 pixels in size. Bottom panel: Estimated gamma values from horizontal scan lines, where the black dots correspond to estimates from the unadulterated image, and the white dots correspond to estimates from the image whose upper half has been gamma corrected. Each data point corresponds to a running average over 60 scan lines.

d. Signal to Noise Ratio

Digital images have an inherent amount of noise introduced either by the imaging process or digital compression. The amount of noise is typically uniform across the entire image. If two images with different noise levels are spliced together, or if small amounts of noise are locally added to conceal traces of tampering, then variations in the signal to noise ratio (SNR) across the image can be used as evidence of tampering.

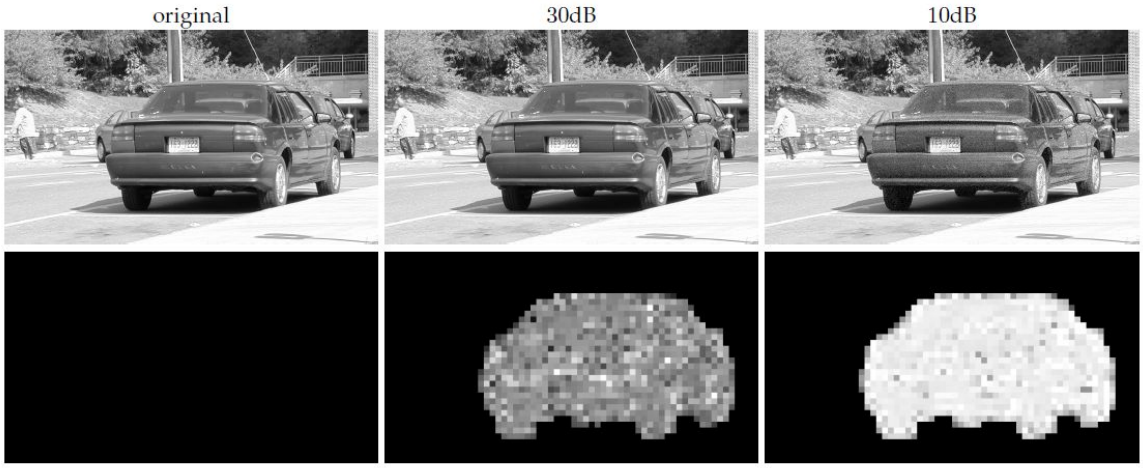


Figure : Shown on the top row is an original image and this image with noise added locally to the car. Shown on the bottom row are the locally estimated noise variances (on the same log scale).