Digital Image Forensics

Dr. M. Ishtiaq

FAST – National University of Computer and Emerging Sciences

Introduction

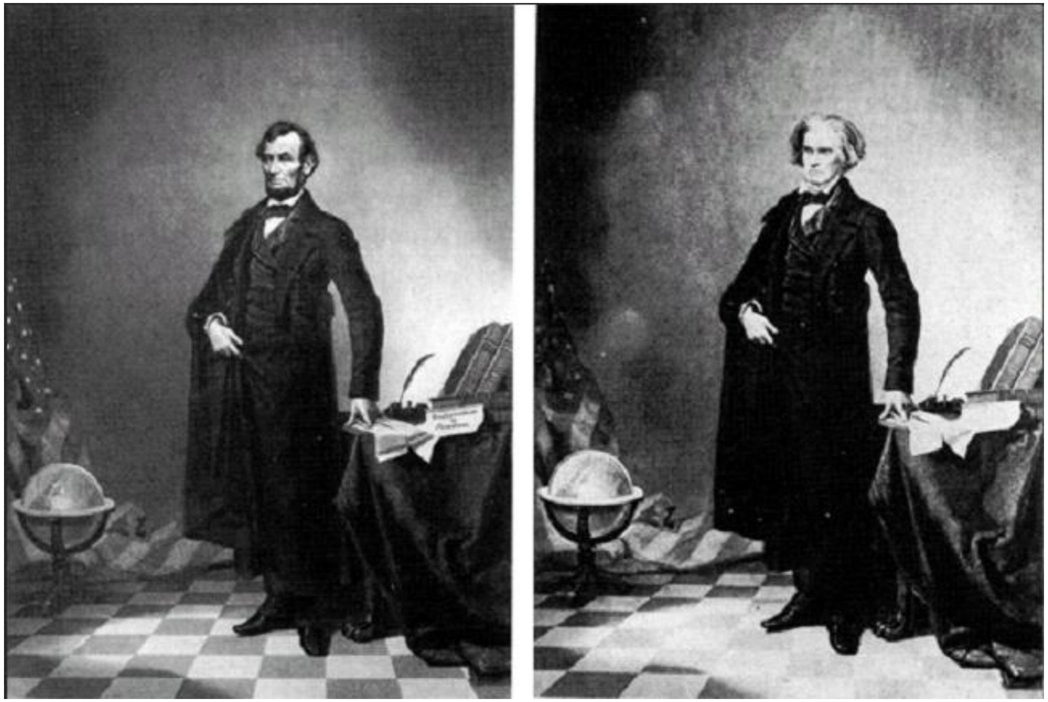
They say,

a picture is worth a thousand words

but what if, those words are lies ?

History of photo manipulation

- Photography lost its innocence long ago.
- 1860 the symbolic portrait of Lincoln is a composite of Lincoln's head and John Calhoun's body

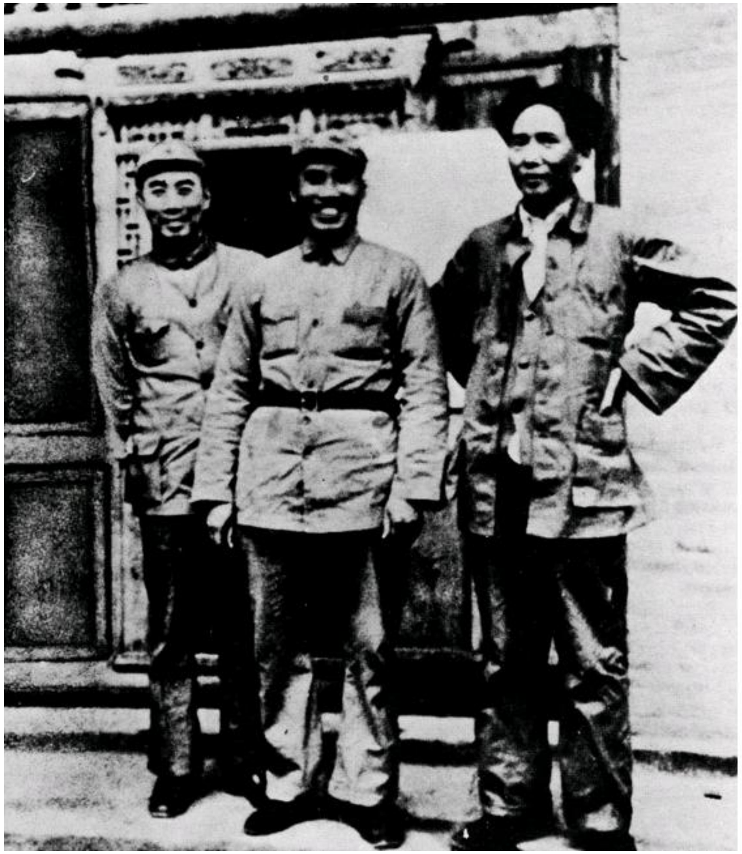


History of photo manipulation

- 1930`s: Stalin had disgraced comrades airbrushed out of his pictures

History of photo manipulation

- 1936: same story with Mao, Po Ku got removed.



History of photo manipulation

- **August 2007**

Photo Manipulation

- With the advancement in:
  - high-resolution digital cameras
  - powerful personal computers
  - sophisticated photo-editing software,
- the manipulation of photos is becoming more common.

Digital Forgeries

- Digital forgeries, often leaving no visual clues of having been tampered with and can be indistinguishable from authentic photographs.
  - **Judicial and news media and many others affected.**
- In a sense images contain natural fingerprints, we can build tools that can detect these fingerprints.
- Although digital forgeries may leave no visual clues of having been tampered with, they may, nevertheless, alter the underlying statistics of an image.
- In order to create a convincing forgery, it is often necessary to re-size, rotate, or stretch portions of the images. This process requires re-sampling the original image onto a new sampling lattice.

Digital Forgeries

- In a re-sampled image new pixel values are determined from the existing pixels of the original image.
- Each new pixel has a specific relationship with its neighboring pixels.
- We need to know whether a pixel in an image satisfies a particular relationship within its context and what is that relationship.
  - If exist, these relationships are periodic.
- To detect a forgery, we must know two things,
  1. Which pixels are related to its neighborhood
  2. What is that relationship.
- Finding periodicity patterns in those relationships will reveal re-sampling patterns.

First attempt at Detecting Forgeries

- A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," in *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758-767, Feb. 2005.

Expectation Maximization (EM)

- By the use of EM algorithm one can simultaneously determine interpolated pixels and their relationships with the neighbors.
- EM is two step iterative algorithm:
  - 1st step (E-Step): Probability that each sample is related to its neighbors.
  - 2nd step (M-step): The specific form of relationship of neighboring pixels.
- EM algorithm is suited for these kind of problems.

EM Algorithm

/* Initialize */

Choose a random $\vec{\alpha}_0$

Choose N and σ_0

set p_0 to the reciprocal of the range of the signal $\vec{y}$

set Y with as the matrix having each row of a pixels with its neighborhood

set h to be a low-pass filter of size $(N_h \times N_h)$

- Here α is initialized randomly and upon convergence it will describe the type of relationship among neighboring pixels
- N is the neighborhood size
- σ is a small number which controls algorithm convergence speed.
- *Y* is each pixel context
- *h* is a 3x3 arithmetic mean filter

EM Algorithm

$n = 0$

repeat

/* Expectation step */

for each sample i

$$R(i) = \left| y(i) - \sum_{k=-N}^{N} \alpha_n(k) y(i+k) \right| \quad \text{/* residual */}$$

end

$R = R * h$ /* spatially average the residual error */

for each sample i

$$P(i) = \frac{1}{\sigma_n \sqrt{2\pi}} e^{-R(i)^2 / 2\sigma^2{}_n} \quad \text{/* conditional probability */}$$

$$w(i) = \frac{P(i)}{P(i) + p_0} \quad \text{/* posterior probability */}$$

end

EM Algorithm

/* Maximization step*/

$W = 0$

for each sample i

$W(i,i) = w(i)$ /*weighting matrix*/

end

$$\sigma_{n+1} = \left(\frac{\sum_i w(i) R^2(i)}{\sum_i w(i)} \right)^{1/2}$$ /*new variance estimate*/

$\vec{\alpha}_{n+1} = (Y^T W Y)^{-1} Y^T W \vec{y}$ /* new alpha estimate */

$n = n + 1$

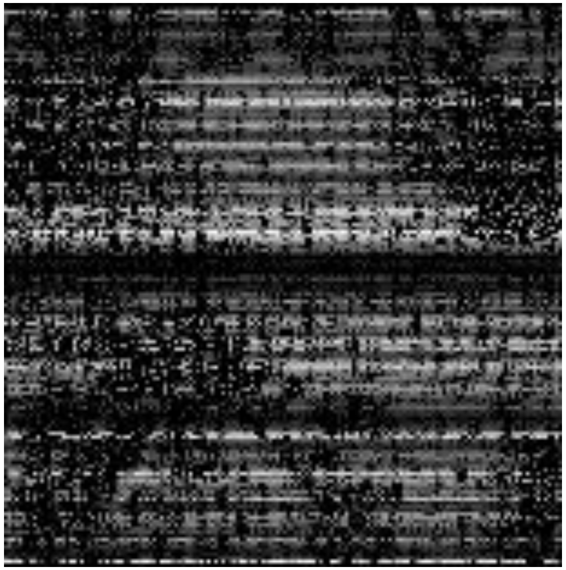
until$(\|\vec{\alpha}_n - \vec{\alpha}_{n+1}\| < \varepsilon)$ /*stopping condition*/

Experimental Setup

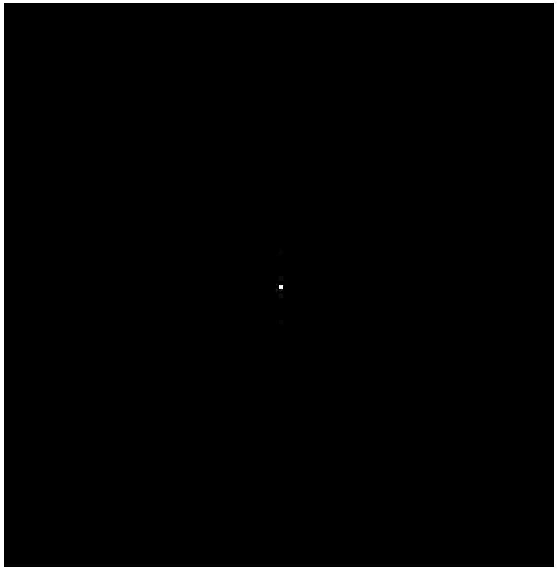
- UCID Dataset
  - A large dataset of 1013 uncompressed images
  - The dataset can download from [16]
  - All the images were cropped to 256x256
  - Three re-sampling methods, i.e. cubic, lancoz2 and lanczos3

Results

Original Image



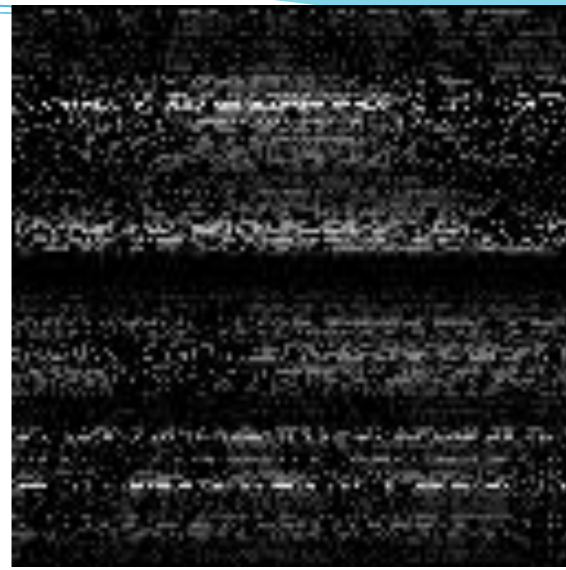
p-Map



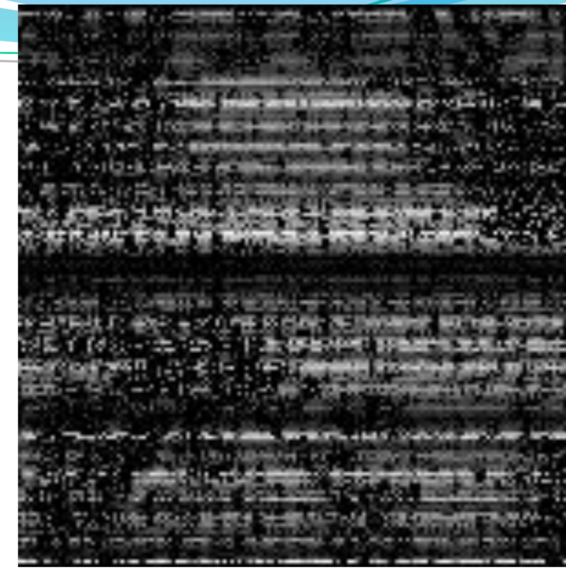
Fourier spectrum of p-Map

Results

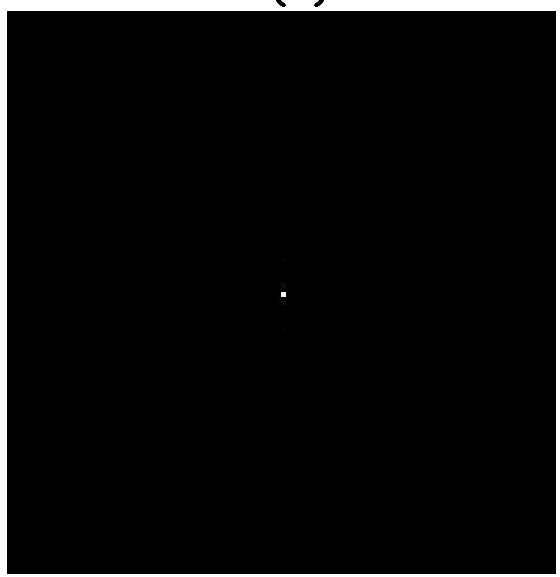
(a) Original image p-Map
(b) Re-sampled image p-Map
(c) - (d) Fourier spectrum of (a) and (b) respectively



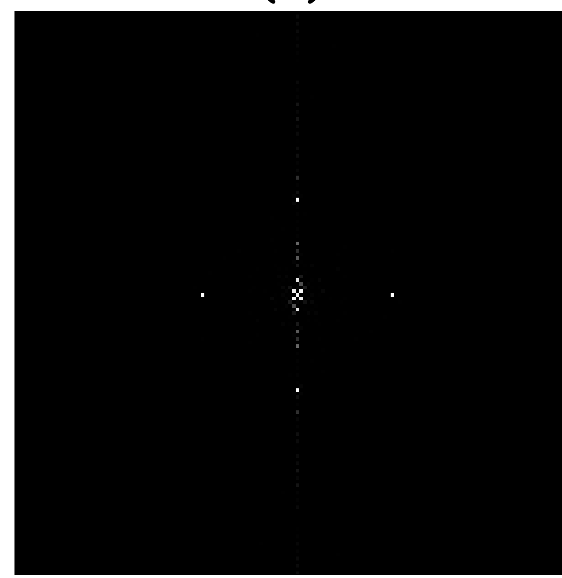
(a)



(b)

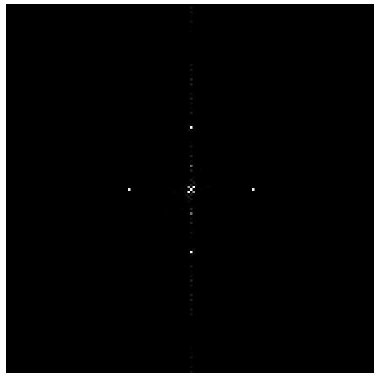
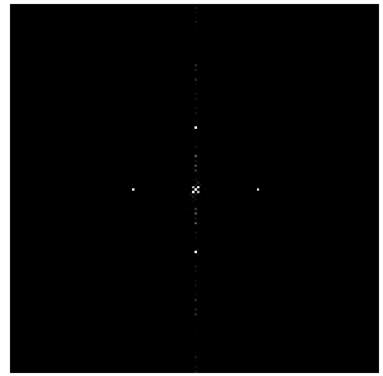
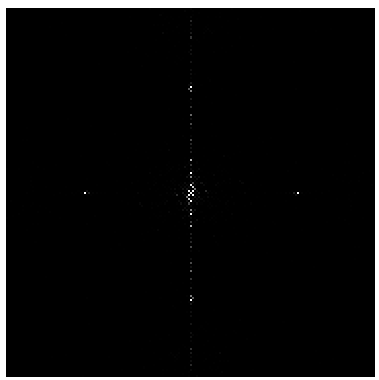
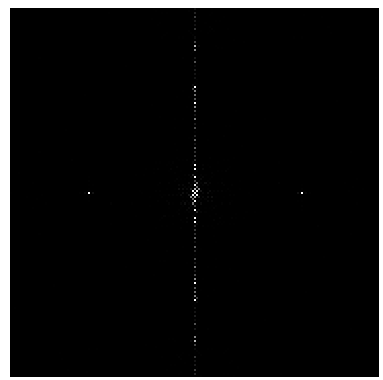
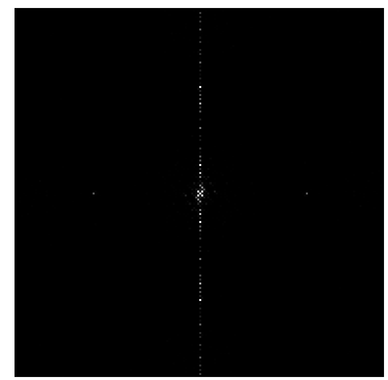
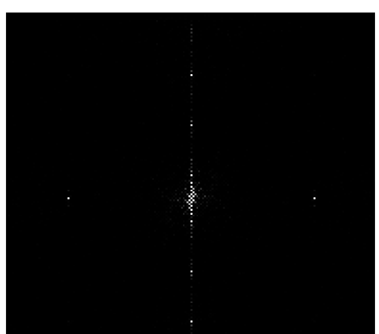
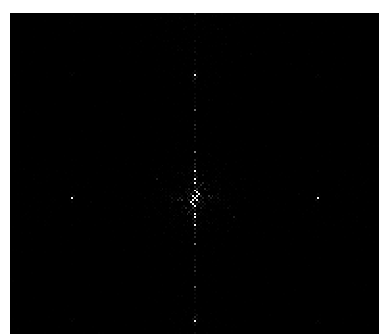
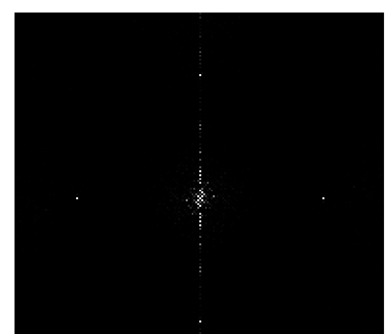


(c)

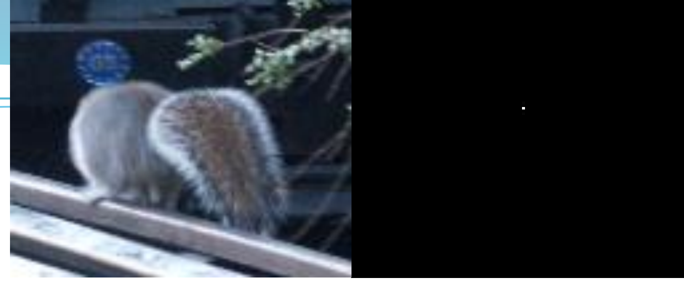


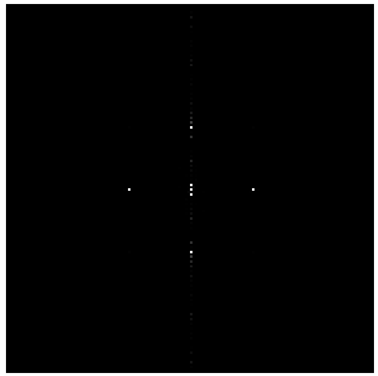
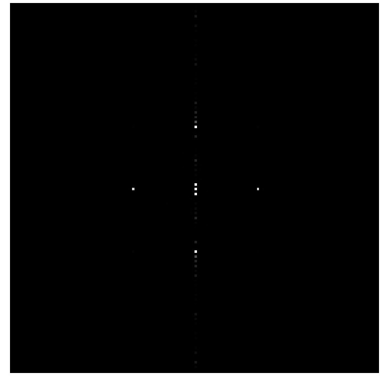
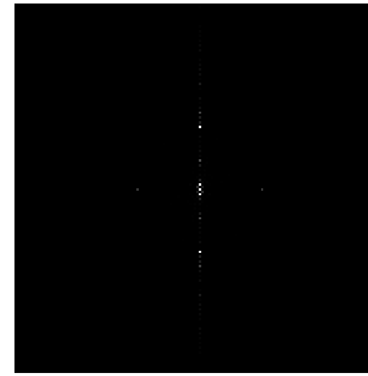
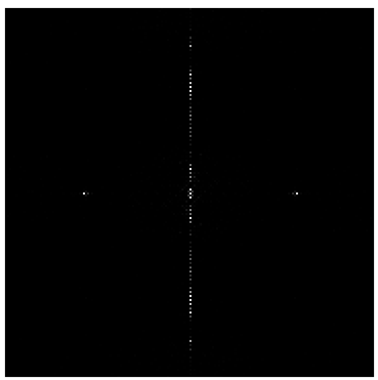
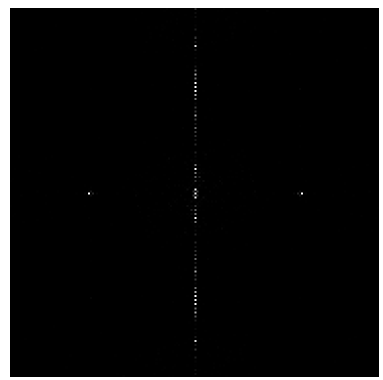
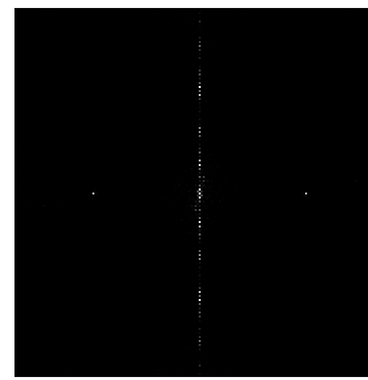
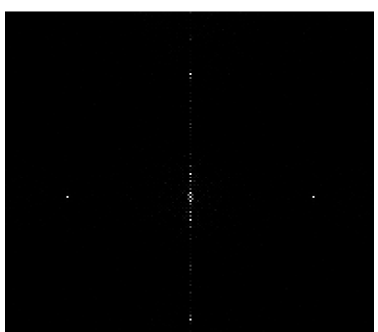
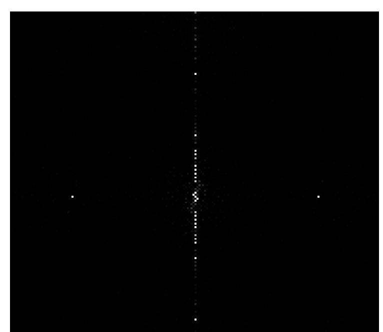
(d)

Results

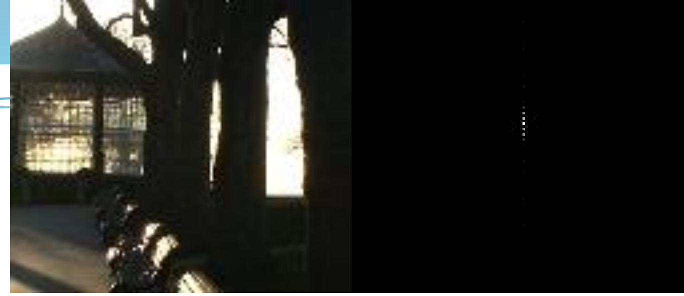
Interpolation factor\Method	Cubic	Lanczos2	Lanczos3
20%			
40%			
50%			

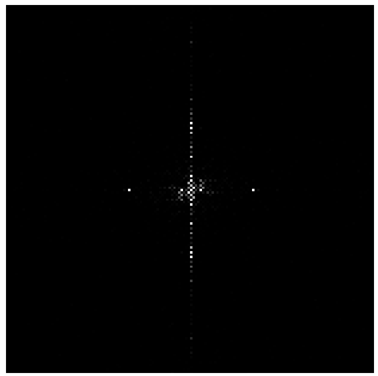
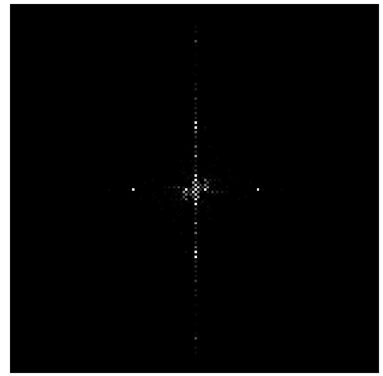
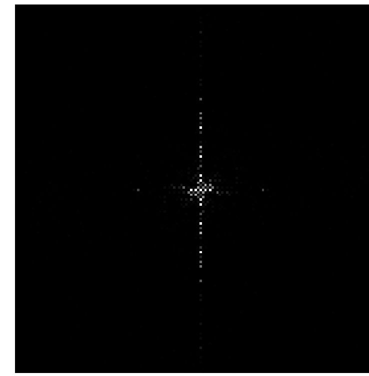
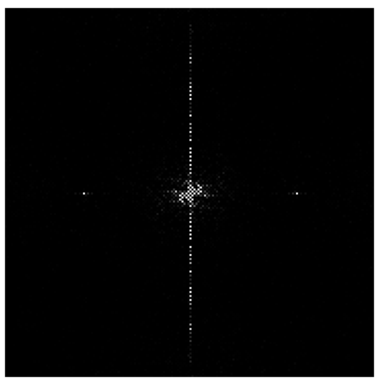
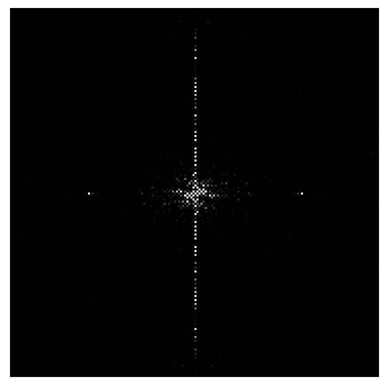
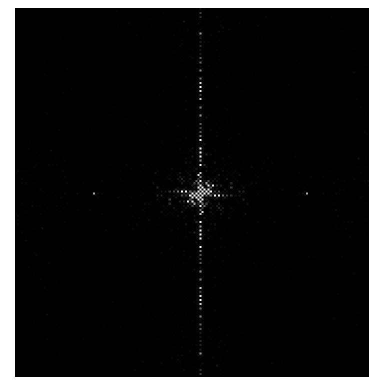
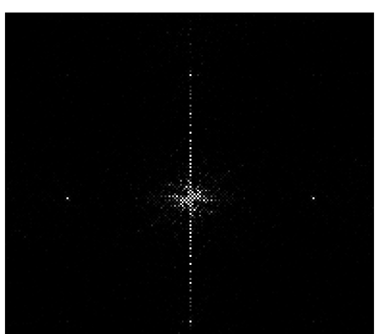
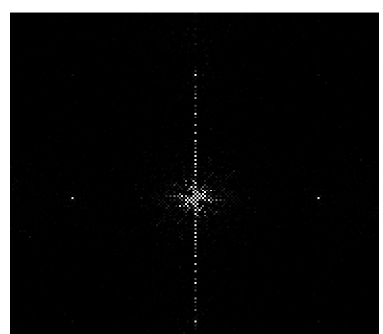
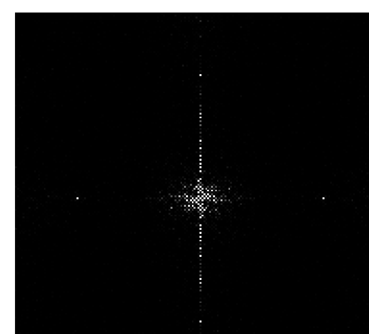
Results



Interpolation factor\Method	Cubic	Lanczos2	Lanczos3
20%			
40%			
50%			

Results



Interpolation factor\Method	Cubic	Lanczos2	Lanczos3
20%			
40%			
50%			

Results

- True Positive = 100%
- False Positive = 0 %
- False Negative = 5 %

Results

- Results on different Attacks

Attack Re-sampling Factor	Filtering		Noise		Histogram Equalization
	Mean	Median	Salt & Pepper	Gaussian	
20%	✗	✗	✓	✗	✓
40%	✓	✓	✓	✗	✓
50%	✓	✓	✓	✗	✓

Conclusion

- Image re-sampling has become an important problem in the field of image forensics.
- The method performs well on varying re-sampling factors and methods.
- The performance was lower for down-sampled images.
- The method is robust against histogram equalization for all factors and mean and median filter for up-sampling above 30%.
- Its fails to detect any re-sampling for Gaussian noise attack but works well in case of salt & pepper noise.
- Future work may include identifying from a given image an interpolation method and resampling factor and also exploit interdependencies in RGB color bands.

References

- G. Friedman, "The trustworthy camera: Restoring credibility to the photographic image," *IEEE Trans. Consumer Electron.*, vol. 39, no. 3, pp. 905–910, Jun. 1993.
- M. Schneider and S.-F. Chang, "A robust content-based digital signature for image authentication," in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, 1996, pp. 227–230.
- D. Storck, "A new approach to integrity of digital images," in *Proc. IFIP Conf. Mobile Communication*, 1996, pp. 309–316.
- B. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, no. 6, pp. 944–957, Jun. 1995.
- S. Bhattacharjee and M. Kutter, "Compression-tolerant image authentication," in *Proc. IEEE Int. Conf. Image Processing*, vol. 1, 1998, pp.
- C. Honsinger, P. Jones, M. Rabbani, and J. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," U.S. patent Application, Docket/E-D, 1999.
- J. Fridrich, M. Goljan, and M. Du, "Invertible authentication," in Proc. SPIE, Security and Watermarking of Multimedia Contents, 2001.
- E. Lin, C. Podilchuk, and E. Delp, "Detection of image alterations using semi-fragile watermarks," in Proc. SPIE, vol. 3971, Security and Watermarking of Multimedia Contents II, 2000, pp. 52–163.
- C. Rey and J.-L. Dugelay, "Blind detection of malicious alterations on still images using robust watermarks," IEE Seminar: Secure Images and Image Authentication, pp. 7/1–7/6, 2000.
- G.-J. Yu, C.-S. Lu, H.-Y. Liao, and J.-P. Sheu, "Mean quantization blind watermarking for image authentication," in Proc. IEEE Int. Conf. Image Processing, vol. 3, 2000, pp. 706–709.
- C.-Y. Lin and S.-F. Chang, "A robust image authentication algorithm surviving jpeg lossy compression," in Proc. SPIE, vol. 3312, Storage and Retrieval of Image/Video Databases, 1998, pp. 296–307.
- J. Fridrich and M. Goljan, "Images with self-correcting capabilities," in *Proc. IEEE Int. Conf. Image Processing*, vol. 3, 1999, pp. 792–796.
- A.C. Gallagher, "Detection of linear and cubic interpolation in jpeg compressed images," in Proc. 2nd Canadian Conf. Computer and Robot Vision., Victoria, British Columbia, Canada, vol. 171, 2005, pp. 65–72.
- B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," IEEE Trans. Inform. Forensics Security, vol. 3, no. 3, pp. 529–538, 2008.
- A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 758–767, 2005.
- http://www.staff.lboro.ac.uk/~cogs/datasets/UCID/ucid.html

Thank You

Questions

?