

Image Forgery Identification Using JPEG Intrinsic Fingerprints

A. Garg, A. Hailu, and R. Sridharan

Abstract—In this paper a novel method for image forgery detection is presented. The method exploits the fingerprints left by JPEG compression. The fingerprints are obtained by estimating the quantization matrix and are used to detect different forgeries such as copy-paste, cropping, rotation, and brightness changes. Algorithms were developed for detecting forgeries on a single JPEG compressed image and for the more difficult scenario where the forged image is recompressed. The proposed algorithms' performance improves with increasing quality factor unlike block-artifact based detection schemes. Thus it would provide a good complement to the reliability offered by blocking-artifact based schemes at lower quality factors. A database of around 2000 images was used for testing.

Index Terms—Block-DCT coefficients, Intrinsic fingerprints, JPEG coefficients, quantization tables, tampering detection.

I. INTRODUCTION

INCREASED access to advanced digital image acquisition and manipulation systems has necessitated better image fraud detection. There are a few methods that have been proposed as a check for image integrity. These include active forgery detection methods such as digital watermarking, and passive investigation of fingerprints inherent to the specific image manipulations. The latter approach is more useful, since most images encountered are not usually actively tamper-protected.

Currently, most acquisition and manipulation tools use the JPEG standard for image compression. As a result, one of the standard approaches is to use the blocking fingerprints introduced by JPEG compression, as reliable indicators of possible image tampering. Not only do these inconsistencies help determine possible forgery, but they can also be used to shed light into what method of forgery was used. Many passive schemes have been developed based on these fingerprints to detect re-sampling [8], copy paste [2, 7, 12], scene lighting detection [6].

Manuscript received March 13, 2008.

A. Garg, is a graduate student in the Electrical Engineering Department, Stanford University, Stanford, CA 94305 USA (e-mail: ashu2411@stanford.edu).

A. Hailu, is a graduate student in the Electrical Engineering Department, Stanford University, Stanford, CA 94305 USA (e-mail: ahailu@stanford.edu).

R. Sridharan, is a graduate student in the Electrical Engineering Department, Stanford University, Stanford, CA 94305 USA (e-mail: rangam@stanford.edu).

These schemes are very diverse on what aspect of the image fingerprint they employ. Some methods rely on statistical modeling of the distribution of the quantized JPEG coefficients, of which an example is the use of Benford's law [3]. Other methods depend on modeling of acquisition devices and post processing steps [10]. In addition, there are also methods that use blocking artifact characteristics matrix (BACM) which relies on the disruption of regular symmetrical shapes present in the original compressed images due to varying distributions of pixels located on block borders compared to block centers [4].

In this paper the parameter that is used as a metric for determining forgery is related to average distortion. For each block in the image, this is calculated as a function of the remainders of the DCT coefficients with respect to the quantization matrix (Q matrix) used. The forgery methods investigated using this method include rotation, copy-paste, cropping, and brightness, all of which are easily achievable using both commercially and freely available software. One of the baseline assumptions of this approach is that only one type of forgery is applied per image. In addition, even though the methods discussed here are easily extendible to color images, only grayscale images were investigated.

II. QUANTIZATION MATRIX BASED IMAGE FORENSICS

A. JPEG compression induced fingerprints

JPEG image compression involves three main steps:

- 1) Blockwise DCT transformation of the image,
- 2) Quantization of the DCT transforms coefficients, and
- 3) Variable length encoding of coefficients.

The quantization step introduces distinct fingerprints within each block and across boundaries of adjacent blocks. These artifacts provide built in reliable fingerprints that allow passive integrity checks. In addition, they can also be used in the estimation of the quantization matrix used for compression.

B. Image data

Training and test data sets were obtained from the public domain Uncompressed Color Image Database (UCID), which provides a benchmark dataset for image processing analysis [9]. These images were captured and are available in uncompressed form, with the current database (v2) having over 1300 images. For this project 100 images were taken from this database, converted to grayscale, and used as baseline source images for all further analysis.

C. Forgery detection

General Approach: The initial approach taken was based on the assumption that the Q matrix of the untampered image is known. Such a situation arises when knowledge of the image acquisition process uniquely identifies the Q matrix used for JPEG compression. In this scenario, the forged image is saved as an un-compressed bitmap.

The parameter that is used as a metric for determining forgery is related to average distortion. For each block in the image, this is calculated as a function of the remainders of the DCT coefficients with respect to the original Q matrix as follows:

$$r = \sum_{i=1}^8 \sum_{j=1}^8 r_{ij} \cdot e^{r_{ij}} \quad (1)$$

where

$$r_{ij} = \widehat{\text{mod}}(D_{ij}, Q_{ij})$$

and $\widehat{\text{mod}}(a,b)$ gives the absolute difference between a and the closest multiple of b.

Large values of this measure indicate that the particular block of the image is very different from the one that is expected and, hence is likely to belong to a forged image. Averaged over the entire image, this measure can be used for making a decision about authenticity of the image. The threshold for classification is calculated from a training data set.

The methods used for detecting individual forgeries are as follows:

Copy-paste: One of the most common forgeries is the insertion of a foreign image onto an image. Detecting copy-paste forgery is possible since the foreign image fails to fit perfectly into the original JPEG compressed image. As a result, when the distortion metric is calculated, it exceeds the detection threshold.

It is expected that the foreign image inserted is small relative to the native image, thereby affecting only some blocks of the original image. Therefore, making a decision on individual blocks and then checking on the localization of the affected block fraction helps distinguish copy-paste from other forgeries.

Cropping: Detection of cropping relies on the likely mismatch between the new image's inherited DCT grid with the original 8x8 grid. As a consequence, a search over an 8x8 block at top-left or bottom-right corners would yield a location that minimizes the distortion metric overall and also gives a value below the threshold.

This method fails to identify cropping that preserves the DCT grid alignment. Such an alignment occurs when cropping takes place at multiples of 8 along both the rows and columns of an image. The probability of this event is 1/64 (1/8th along the row multiplied by 1/8th along the column).

Rotation: Images often end up being rotated by 90, 180 or 270 degrees. The rotated image is certain to be an ill fit to the

original 8X8 grid in the DCT domain and therefore the distortion measure when calculated on this image exceeds the threshold.

Isolating a rotation forgery from other forgeries is made simple by the fact that calculating the distortion measure on a rotated version of the given image should lead to a value lesser than the chosen threshold if it was indeed a rotated one to begin with.

It was observed that rotating an image by 180 degrees does not lead to any change in the distortion measure that we are using. This is due to certain symmetries that exist in the DCT transform matrix. A further elaboration of this is presented in as an Appendix.

Brightness: Brightness forgery is detected by calculating the number of blocks with excessive saturated pixels. The Q matrix is calculated after excluding the blocks which contained excessive number of saturated pixels. This Q matrix is then used to calculate the distortion metric which helps make a decision on whether the image is brightness tampered or not based on the threshold set *a-priori*. Whenever the number of "brightness affected" or saturated blocks is small, the image is immediately classified as not having been "brightness forged". It is assumed that no significant information loss takes place due to minor brightness changes in an image. As a result these images are also classified as not having been "brightness forged".

D. Single compression quantization matrix detection

An important step in the general approach towards using the above described methods for forgery detection is the estimation of the quantization table used for compression. Initially, our method revolved around estimating the quantizer step based on the peaks that occur in the histogram of the DCT coefficients. However, this method failed to provide a reliable estimate of the Q matrix because of the rounding operations that take place during the DCT transform cause the peaks in the histogram to spread out thereby making them difficult to detect. However, transforming the histogram to the frequency domain by obtaining the power spectral density makes the peaks more prominent and the quantization step easy to estimate [1, 12].

The top 3x3 block of the Q matrix is estimated in this manner. These 9 values are then compared with various candidate Q matrices which are stored in a look up table based on the JPEG standard Annex-K table and the Q matrix is determined to be the one that is closest to the estimate that has already been obtained. Therefore, this method also obtains an estimate of the quantizer step for the high frequency AC components which typically do not have substantial number of entries in the histogram.

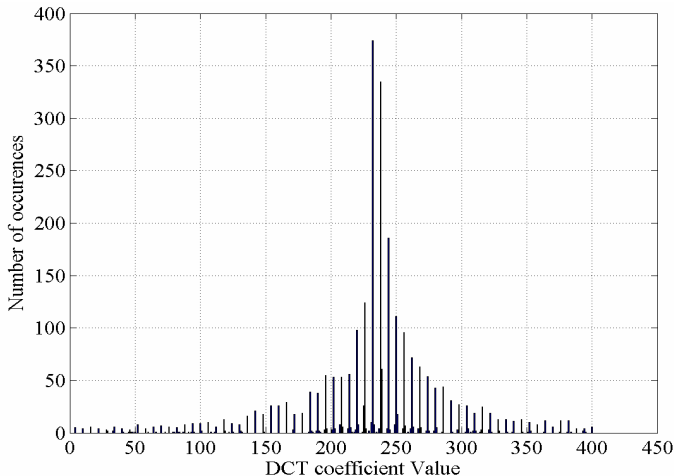


Fig. 1: Histogram for DCT of JPEG Compressed Image

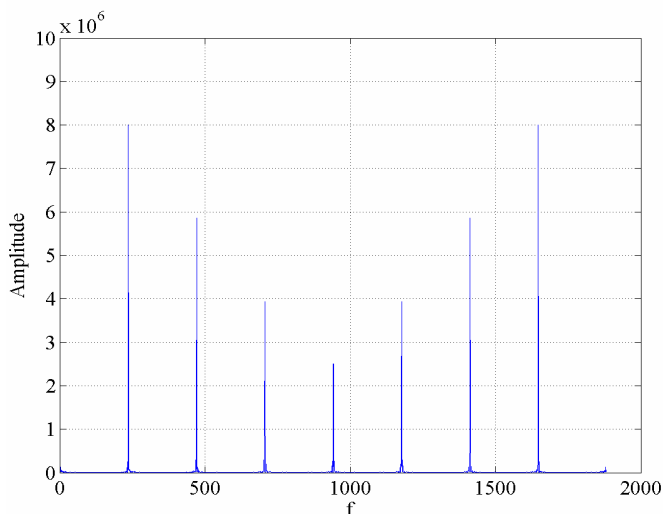


Fig. 2: PSD of DCT coefficient showing peaks at original step size

III. TESTING AND SIMULATION RESULTS

A. Testing Environment

A test image database was created for computing the accuracy of our methods. This involved implementing the algorithms in MATLAB and applying them to the images from the database. The original 100 images were stored at three different JPEG compression ratios of 50%, 75% and 90% quality factors. Fifty images of each compression level were used for training and the remaining fifty for testing.

Copy-paste forgery was done by copying a set of pixels randomly from an arbitrary image and then placing it in the original image. We used a block of size 50x50 for the copied image.

For cropping forgery, some columns and rows were deleted in the original images to provide cropping from the left, top, right, and bottom.

Rotation forgeries were accomplished by 90° and 270° rotation using MATLAB's inbuilt command `rot90`. As mentioned earlier, 180° rotated images fail to be distinguished

by our measure.

For brightness forgery, random values, either above 100 or below -100, were added to every pixel of the image. The number 100 was chosen so as to ensure that sufficient portions of the image went into saturation.

In total, around 2000 images were generated and these were used for both testing and training.

B. Testing Method

Every test image is checked for all possible forgeries. If all tests on the image turn out to be negative, then it is declared to be an untampered image. If the image fails the copy-paste test and any other test, it is still declared as a copy-paste forgery because this test was found to be the most reliable in terms of the false positive rate (percentage of non copy-paste images which are declared as copy-paste). Similarly since the brightness test was found to be the least reliable in terms of the false positive rate, an image is declared to be "brightness forged" only if it is negative for all other forgeries and if it fails the brightness test. If an image fails both cropping and rotation tests, then the one that is more likely to have occurred, based on the computed metric, is declared as having occurred.

C. Simulation Results

The following figures present the false negative rate (number of tampered images shown as untampered) and the false positive rate (FNR and FPR respectively) for different forgeries at different Quality Factors.

The results are as follows:

Table 1: Performance results for different forgeries

| Forgery Type | False Positive Rate | False Negative Rate |
|--------------|---------------------|---------------------|
| Original | 13.61% | - |
| Cropping | 0% | 4.7% |
| Copy-Paste | 0% | 16.3% |
| Rotation | 2.04% | 13.25% |
| Brightness | 2.53% | 6.85% |

A brief interpretation of these results follows:

Cropping: As QF increases, a better estimate of the quantization matrix of the original un-tampered image is obtained, and as a result there are fewer FNR errors. Also, the number of errors, in terms of the FPR, was zero which means that no un-cropped image was detected as a cropped image.

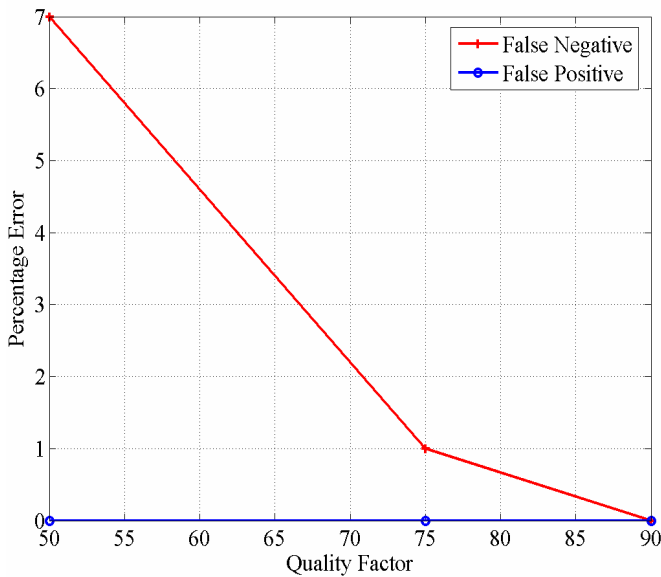


Fig. 3: Plot of FNR and FPR versus QF for cropping

However, it should be noted that if the picture happens to be aligned perfectly to the original grid after cropping, then the cropping forgery would go undetected in this case. As mentioned earlier, the probability of this event happening is $1/64$. However, we eliminated such cases from our sample set so as to enable us to more effectively estimate the performance of our methods.

Copy-paste: As expected, in the case of copy-paste forgery also, the error percentage decreases with increase in Quality factor (QF) for reasons described above. However, in the case of a copy-paste forgery we observe significant performance loss at a QF of 50. This results from the significant deviations of the DCT values at such poor qualities from the quantization step size which leads to large values of the chosen metric on a number of blocks in the image rather than just a few.

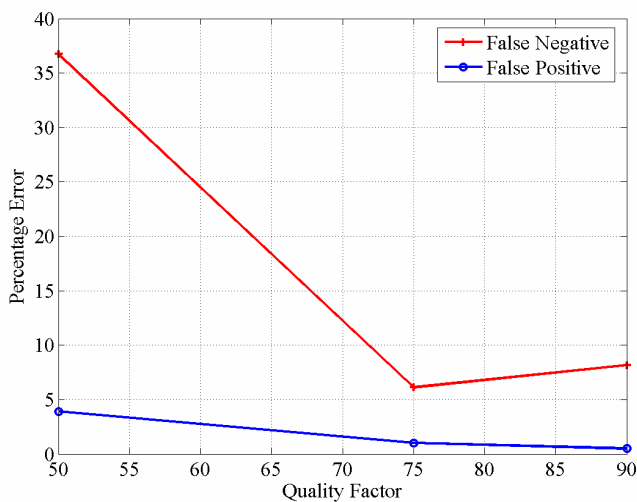


Fig. 4: Plot of FNR and FPR versus QF for copy-paste

Rotation: The test result showed that rotation gives perfect result with respect to the False Positive Error Rate. However,

in case of False Negative Rate, the performance drops considerably for low QF due to greater difficulty in estimating the Q matrix.

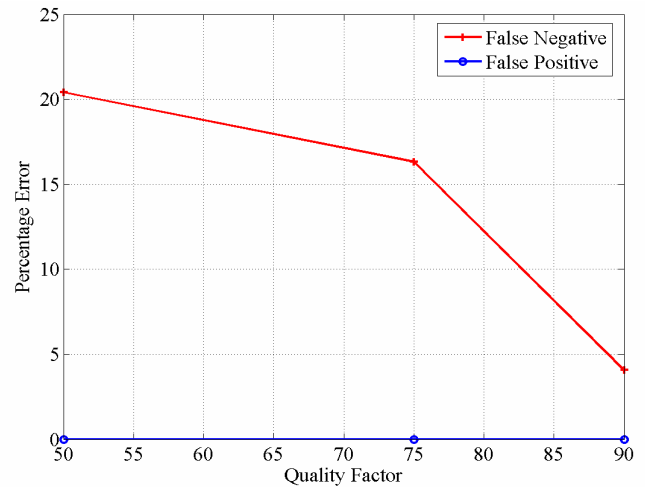


Fig. 5: Plot of FNR and FPR versus QF for rotation

This leads to large values of the chosen metric even after we rotate the given image to make it equivalent to the original one. The results can probably be improved by using some other method to estimate the Q matrix with greater reliability.

Brightness: Brightness forgery detection produced similar results as previous cases with good FPR and FNR which get better with higher quality factor.

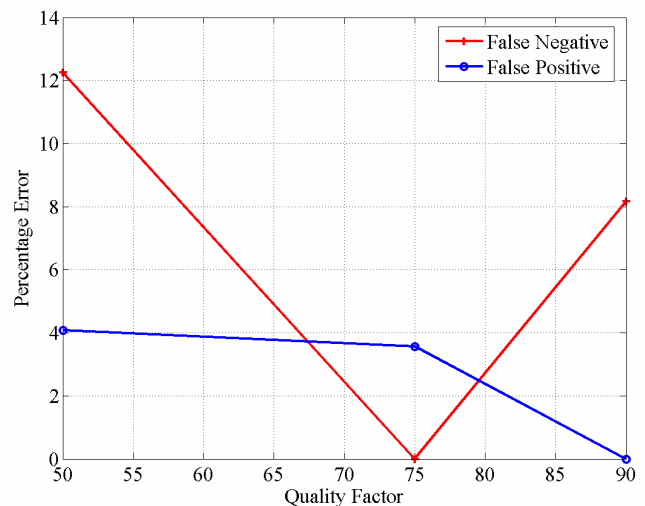


Fig. 6: Plot of FNR and FPR versus QF for brightness

Threshold: The value set for threshold plays an important part in forgery detection. A higher value of the threshold would result in a great number of tampered images being classified as untampered ones while a threshold value that is too low would lead to false alarms due to untampered images being declared as tampered. This fact is confirmed in the plot given in Fig. 7 that shows a trade-off between FPR and FNR. Ideally, we would like to have low FPR and FNR. However,

we would rather have an un-tampered show up as tampered rather than the other way round. As a result, we choose a threshold that is biased towards False Positive Rate.

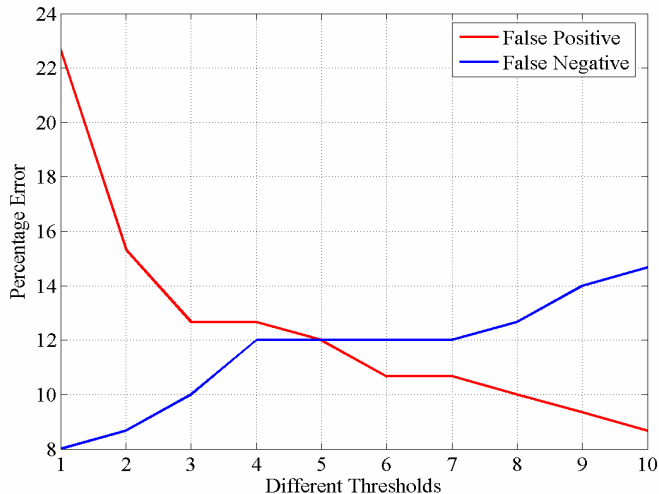


Fig. 7: Plot of FNR and FPR versus threshold values

The threshold was calculated from around 900 of the 2000 images that were created.

IV. DOUBLE JPEG COMPRESSED IMAGES

A. Issues with double JPEG compressed images:

Methods for estimating the primary quantization matrix for a double JPEG compressed image have been proposed in [5]. This paper dealt with the estimation of the primary quantization matrix from a set of possible candidate matrices. The secondary compression present in the given image is disrupted by taking a slightly cropped version of the image and then recompressing it to recreate the original compression process. The images thus obtained are compared with the original image to obtain the most likely match for the primary Q matrix.

These methods were implemented and were found to typically work better when the Quality Factor for the second compression was greater than the first.

Once the primary quantization matrix was estimated, the above described algorithms were then applied for forgery detection.

Limited testing, carried out on the test images, and indicated that the methods described in this paper are easily extended to double JPEG compressed images too.

V. FUTURE MODIFICATIONS

In this project different schemes for image forgery identification were analyzed. However, these schemes mainly revolved around using the Quantization matrix only. Our test showed that that this approach provides decent results but better methods can probably be devised in order to improve the accuracy. One such technique would be to use features generated in the pixel domain as suggested in [4, 12].

Further work can also be directed towards developing techniques to detect other forgeries which are achievable using various image editing tools.

VI. CONCLUSION

The algorithms that we have developed are able to detect forgeries in both single and double JPEG compressed images with reasonable accuracy.

Our test results show that the accuracy of detection improves with increase in Quality Factor. Intuitively one might expect the opposite trend, since blocking artifact increases with increasing compression. However, our method is not based on blocking artifact but rather on the metric that is calculated whose effectiveness decreases with higher compression. Hence, a combination of the new approach with the blockwise distortion measure approach will significantly improve forgery detection by complementing each other's performance.

Among the different kinds of forgeries that we worked on, cropping and rotation were the easiest to detect and copy-paste forgery was probably the toughest.

APPENDIX

Symmetry in DCT transform matrix

Notation:

- rot90 is used to indicate the rotation of a matrix by 90°
- Similarly rot180 indicates rotation by 180°
- X^T refers to the transform of the matrix X.
- A is the matrix used for finding the DCT transform i.e.

$$Y = A * X * A^T$$

is the DCT transform of the matrix X.

It can be shown using matrix algebra that

$$Z * \text{rot}90(X) = (X * \text{rot}90(Z))^T$$

The DCT coefficients of the 180° rotated version of the matrix X is given by

$$\begin{aligned} Y &= A \bullet \text{rot}180(X) \bullet A^T \\ &= (\text{rot}90(X) \bullet \text{rot}90(A))^T \bullet A^T \\ &= \text{rot}90(A)^T \bullet (A \bullet \text{rot}90(X))^T \\ &= \text{rot}90(A)^T \bullet X \bullet \text{rot}90(A)^T \end{aligned}$$

Shown below are the matrices A and the matrix $\text{rot}90(A)^T$

$$\begin{pmatrix} 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 \\ -0.4904 & -0.4157 & -0.2778 & -0.0975 & 0.0975 & 0.2778 & 0.4157 & 0.4904 \\ 0.4619 & 0.1913 & -0.1913 & -0.4619 & -0.4619 & -0.1913 & 0.1913 & 0.4619 \\ -0.4157 & 0.0975 & 0.4904 & 0.2778 & -0.2778 & -0.4904 & -0.0975 & 0.4157 \\ 0.3536 & -0.3536 & -0.3536 & 0.3536 & 0.3536 & -0.3536 & -0.3536 & 0.3536 \\ -0.2778 & 0.4904 & -0.0975 & -0.4157 & 0.4157 & 0.0975 & -0.4904 & 0.2778 \\ 0.1913 & -0.4619 & 0.4619 & -0.1913 & -0.1913 & 0.4619 & -0.4619 & 0.1913 \\ -0.0975 & 0.2778 & -0.4157 & 0.4904 & -0.4904 & 0.4157 & -0.2778 & 0.0975 \end{pmatrix}$$

$$\begin{pmatrix} 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 \\ 0.4904 & 0.4157 & 0.2778 & 0.0975 & -0.0975 & -0.2778 & -0.4157 & -0.4904 \\ 0.4619 & 0.1913 & -0.1913 & -0.4619 & -0.4619 & -0.1913 & 0.1913 & 0.4619 \\ 0.4157 & -0.0975 & -0.4904 & -0.2778 & 0.2778 & 0.4904 & 0.0975 & -0.4157 \\ 0.3536 & -0.3536 & -0.3536 & 0.3536 & 0.3536 & -0.3536 & -0.3536 & 0.3536 \\ 0.2778 & -0.4904 & 0.0975 & 0.4157 & -0.4157 & -0.0975 & 0.4904 & -0.2778 \\ 0.1913 & -0.4619 & 0.4619 & -0.1913 & -0.1913 & 0.4619 & -0.4619 & 0.1913 \\ 0.0975 & -0.2778 & 0.4157 & -0.4904 & 0.4904 & -0.4157 & 0.2778 & -0.0975 \end{pmatrix}$$

As can be seen, the rows of $\text{rot}90(A)^T$ are either the same or the negative of the rows of A . The DCT coefficients of the 180 degree rotated matrix are therefore the same in absolute value to that of the original matrix. As a result the metric calculated for a 180 degree rotated image is the same as that for the original one.

ACKNOWLEDGMENT

We would like to acknowledge Dr. Bernd Girod, Dr. Min Wu, and David Varodayan for their continued support, valuable comments and directions towards achieving goals of this project.

REFERENCES

- [1] J. Fridrich, M. Doljan, nad R. Du, "Steganalysis based on JPEG compatibility ", SPIE Multimedia Systems and Applications, vol. 4518, Denver, CO, pp275-280, Aug. 2001
- [2] F. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", Digital Forensic Research Workshop, Cleveland, USA, Aug. 2003.
- [3] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," Proc. SPIE Int. Soc. Opt. Eng. 6505, 65051L, 2007
- [4] W. Luo, Z. Qu, J. Huang, G. Qiu, "A Novel Method for Detecting Cropped and Recompressed Image Block," Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on , vol.2, no., pp.II-217-II-220, 15-20 April 2007
- [5] J. Lukas and J. Fridrich, "Estimation of Primary Quantization Matrix in Double Compressed JPEG Images," Proc. of the Digital Forensics Research Workshop, Cleveland, OH, Aug. 2003.
- [6] M. K. Johnson and H. Farid , "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting," ACM Multimedia and Security Workshop, New York, NY, 2005.
- [7] T. Ng, S.F. Chang, and Q. Sun, "Blind Detection of Photomontage using Higher Order Statistics", IEEE International Symposium on Circuits and Systems, Canada, May 2004.
- [8] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling," IEEE Trans. on Signal Processing, vol. 53, no.2, pp. 758-767, Feb. 2005.
- [9] G. Schaefer, and M. Stich, "UCID – An Uncompressed Color Image Database," Technical Report, School of Computing and Mathematics, Nottingham Trent University, U.K., 2003
- [10] A Swaminathan, M. Wu, K. Liu J. R., "Digital Image Forensics via Intrinsic Fingerprints," Information Forensics and Security, IEEE Transactions on , vol.3, no.1, pp.101-117, March 2008

- [11] D. S. Taubman, M. W. Marcellin, "JPEG2000 – Image Compression Fundamentals, Standards, and Practice," Kluwer Academic Publishers, 2002.
- [12] S. Ye, Q. Sun, E. and Chang, "Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact," Multimedia and Expo, 2007 IEEE International Conference on , vol., no., pp.12-15, 2-5 July 2007

Work Distribution :

| Task | Garg | Hailu | Sridharan |
|------------------------------|------|-------|-----------|
| Forgery detection techniques | 34% | 33% | 33% |
| Q matrix estimation | 33% | 34% | 33% |
| Training | 33% | 33% | 34% |
| Testing | 34% | 33% | 33% |
| Presentation | 33% | 34% | 33% |
| Report | 33% | 33% | 34% |