I.J. Image, Graphics and Signal Processing, **2015, 12, 10-17**
Published Online November 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2015.12.02

Anti-Forensics of JPEG Images using Interpolation

Saurabh Agarwal[1], Satish Chand[2]
[1,2]Dept. of Computer Engineering, Netaji Subhash Institute of Technology, Sector-3, Dwarka, New Delhi, 110078, India
Email: saurabhnsit2510@gmail.com, schand20@gmail.com

Abstract—The quantization artifacts and blocking artifacts are the two significant properties for identifying the forgery in a JPEG compressed image. There are some techniques for JPEG compressed images that can remove these artifacts resulting no traces for forgery. These methods are referred as anti-forensic methods. A forger may perform some post-operations to disturb the underlying statistics of JPEG images to fool current forensic techniques. These methods create noise and reduce the image quality. In this paper we apply three different interpolation techniques namely nearest neighbor, bilinear and bicubic techniques to remove JPEG artifacts. The experimental results show that the bicubic interpolated images are found to be of better quality as compare to the nearest neighbor and bilinear interpolated images with no JPEG artifacts. For quality analysis of these interpolation methods on the images three popular quality metric are used. The proposed method is very simple to perform. This interpolation based method is applicable to both single and double JPEG compression.

Index Terms—Anti-forensics, JPEG compression, Interpolation, compression artifacts, Image quality.

I. Introduction

Due to advancement of computation and communication technologies, there are easily available good quality photo capturing devices and photo editing softwares. These indirectly or directly help to make visually good quality doctored images that may create intentionally or unintentionally problems in personal, political and public life. The existing methods for digital image forensics are passive and blind because they are not based on any watermark or signature. Quite good amount of research work has been done in the field of image forensics [1-5]. Farid [2] reports that splicing two images of different JPEG compression quality is helpful in detection of forgery. It is mentioned in [3] that there is re-quantization in digital multimedia content when there is tampering in it. Therefore detection of re-quantization is an important element for assessing the authenticity of a digital image.

Some researchers have developed their counter forensic, also called antiforensics technique, so that forgery cannot be detected easily [6-10]. Basically these papers do antiforensics by adding noise or blurring the image so that forgery is not detectable. Antiforensic does help in finding the limitations of the forensic techniques that in turn forces to develop more robust forensic techniques. The forensic and antiforensics techniques may be considered analogous to virus and antivirus.

The digital images are stored in various formats such as .tiff, .pcx, .png, .bmp, .jpeg. The JPEG standard is one of the most popular standards because it can provide zero (lossless) compression to any good amount of compression depending upon the requirement and at the same time it maintains good quality of image. There have been several techniques to detect forgery in JPEG images [11-17]. Forgery detection in a JPEG image is indirectly helped due to its own compression artifacts. In a JPEG image, two types of artifact appear: quantization artifacts in frequency domain and blocking artifacts in spatial domain. If image tempering is done, then the image needs to be saved two times that creates double quantization artifact in histogram of DCT coefficients and the block synchronization gets disturbed. With the help of these artifacts forgery detection can be done easily. An attacker tries to hide or reduce these artifacts so that his forgery cannot be detected. While hiding or reducing the artifacts the image quality gets compromised by these methods. In this paper we discuss interpolation techniques that hide or reduce the artifacts and at the same time maintain image quality. We compare the quality of the interpolated images with some available state of the art quality assessment measures that include mean square error (MSE), peak signal to noise ratio (PSNR), structural similarity index (SSIM) [18] and blind image spatial quality evaluator (BRISQUE) [19].

Rest of the paper is organized as follows. Section 2 reviews the related work and section 3 discusses the interpolation methods. The experimental results are given in section 4 and the paper is concluded in section 5.

II. Related Work

Latest developments help provide multimedia data in digital form, which can easily be spliced and cloned. It may sometime encourage digital piracy that may lead to financial losses to the owner. Sometimes a person having bad intention may misuse this capability of digital media to forge an image. This has been done in past in several cases. For example, in order to taking political benefit, Kenyan politician Mike Sonko posted an image (Figure 1) on Facebook of himself being embraced by the Mandela.

However someone ultimately found the original photo, in which Mandela was actually embracing boxer Muhammad Ali against a completely different background.

1 (a) 1 (b)

Fig.1. (a) Fake image in which Mandela embracing Mike Sonko (b) Original image in which Mandela embracing Muhammad Ali

In Denmark in the year 2013 the social media showed an of powerful storm image (Figure 2) to create sensational news that was ultimately found to be spliced. It was discovered that the storm cloud featured in the image closely matched with the storm of Montana in 2010.

Fig.2. Doctored Image of Storm in Denmark

Depending on the operation the image forgery may be categorized into two broad groups: image splicing and copy-move forgery. In splicing forgery, two or more different images are used to create fake image and in copy-move forgery the replication of a portion of the same image is used to create fake image. To counteract the problem of forgery, several methods have been developed for forgery detection in digital images. The paper [20] discusses that the image forgery (copy-move) can be identified in DCT domain. In this method DCT coefficients are calculated of image overlapping blocks and signs of these DCT coefficients is used as a feature. Farid [21] reports that image forgeries can be identified by calculating the lighting angle of different objects and their synchronization. Lukas et al [22] discuss that the falsified regions in an image can be detected by knowing the photo response non uniformity (PRNU) noise of the camera. If in an image various values of PRNU noise exist then image may be forged. The paper [23] discusses that only one light sensor can be used in camera instead of the three sensors due to the cost factor. Since we need three different colors (RGB), the color filter array (CFA) is used to create these colors from the data obtained by using single sensor. The different cameras have different CFA patterns and different interpolation methods. So by finding the CFA pattern and the interpolation methods, the authenticity of an image can be decided.

One of the important formats for storing digital images is JPEG standard because it perhaps provides good quality using less storage. Accordingly there have been several methods for detecting forgery in JPEG images [11-17]. JPEG image forgery detection can be based on the quantization artifacts or/and blocking artifacts. The Forensic techniques based on the quantization artifacts [11-13] identify image forgery by detecting localized inconsistencies in DCT domain. The localized inconsistency occurs only when if one of the two images used to create forgery was previously JPEG compressed image. There occur periodic/regular patterns in DCT coefficients of the corresponding regions in the image that was previously compressed. The forensic methods [14-17] find the irregularities in spatial domain based on the blocking artifacts. If the grid boundaries of the pasted regions do not synchronize with that of the background image, then the pasted regions will have different grid boundaries with respect to that background image.

Generally the tampered images have to be restored two times that creates double quantization artifacts in the histogram of the DCT coefficients and the blocking pattern, which is generally of 8x8 pixels, in the spatial domain also gets distorted. An attacker with the help of this information can make changes in the image so that traces of the forgery become non-detectable. Removing the traces of both types of artifacts is generally referred as antiforensics. Antiforensic techniques prevent proper forensic investigation process or make it much harder. These techniques reduce quantity and quality of the evidences present in a digital image thus making the analysis and examination of the evidences difficult or impossible.

For concealing the JPEG compression traces in digital images many antiforensic techniques are available. One of the most popular techniques proposed by Stamm et al. [6] is based on dithering. Dithering removes the quantization artifacts in DCT coefficients by filling the gaps. The blocking artifacts are removed by adding some signals in the image. However, the paper [7] reports that the operations performed in [6] introduce noise in the image and decrease the visual quality of the image. The singly compressed JPEG images follow the Benford's law that states, "the probability distribution of first digits of the DCT block coefficients is logarithmic." However the doubly compressed images do not follow this distribution [24]. Some antiforensic techniques have been discussed based on the Benford's law. In order to make a doubly compressed image non-detectable, Milani et al. [8] modify the statistics of the first digits of the DCT block coefficients by redistributing of data in which the difference of the actual DCT coefficients and the estimated coefficients using the Benford's law is minimized. The paper [9] discusses an anti-forensic method that conceals the traces of singly JPEG compressed image by recovering the distribution of first

significant digits of the original DCT coefficients by operating on the distribution of their logarithmic remainders. However the above mentioned methods [8-9] are complex and also create distortion in the image. In [10], it is reported that the DCT coefficients do not follow Laplacian distribution for all type of images as discussed in [6]. In that paper a non-parametric method based on DCT histogram smoothing without using any statistical model is discussed. However, Fan et al [25] report that the method [10] is not suitable for the images which have large smooth regions. In that method, the DCT coefficients are calculated using the total variation-based deblocking operation. These DCT coefficients create an adaptive local dithering signal model that brings the DCT histogram of the processed image close to that of the original one. The paper [26] tries to remove the traces of JPEG compression by adding the tailored noise that converts the DCT coefficients of the compressed image such that their distribution is similar to that of the uncompressed image. However, this noise sacrifices the image visual quality. In this paper, we discuss application of interpolation techniques as image anti-forensics that can conceal the footprints of JPEG compression and also maintain good visual quality of the images.

III. Interpolation Methods

In this section we discuss a process to remove JPEG artifacts in images. In JPEG artifacts, the histogram of some of the DCT values does not occur continuously unlike in the uncompressed DCT values. It means that some of the DCT values in JPEG artifacts are zero that needs to be found out. For finding these missing values some interpolation methods can be applied. The interpolation methods are of two types: adaptive and non-adaptive.

Adaptive interpolation is applied based on the characteristics of image (sharp edges vs. smooth texture) to compute missing values. Non-adaptive interpolation uses the predetermined pattern of computation to recover the missing values irrespective of the image characteristics. The adaptive interpolation methods are difficult to implement and require more computation time; thus they are less preferred. On the other hand, the non-adaptive interpolation methods are simple to implement and require less computation. The most commonly used non-adaptive interpolation methods are nearest neighbor [27], bilinear [27] and bicubic interpolation methods [28], depending on the number of neighboring pixels used to calculate the missing pixel value.

A. Nearest Neighbor Interpolation

This is the simplest interpolation method and requires least processing time. It considers only one pixel to estimate the missing pixel value. Each interpolated output pixel is assigned the value of the nearest sample point in the input image.

B. Bilinear Interpolation

In bilinear interpolation, the adjoining 2×2 neighborhood of known pixel values surrounding the unknown pixel are considered. The value of the unknown pixel is obtained by taking the weighted average of these four pixels. Let $I(x,y)$ denote the intensity of the unknown pixel at position (x,y) and $I(x_1,y_1)$, $I(x_2,y_1)$, $I(x_1,y_2)$ and $I(x_2,y_2)$ be the intensities of its 2×2 four neighbors positioned at (x_1,y_1), (x_2,y_1), (x_1,y_2) and (x_2,y_2). The value of I at the interpolated point in the image can be estimated as

$$I(x,y) = w_1 I(x_1,y_1) + w_2 I(x_2,y_1) + w_3 I(x_1,y_2) + w_4 I(x_2,y_2) \quad (1)$$

Where w_i, i = 1 to 4 are the weights that are decided according to the distance, close pixels assigned higher weights as compared to the far pixels [27]. Since it considers the average value of four neighbor pixels, it provides much smoother looking images as compared to the nearest neighbor interpolation in which the missing pixel value is replaced by a single pixel.

C. Bicubic Interpolation

The bicubic interpolation considers a neighbor of 4×4 pixels for estimating the missing pixel value. The general form for a Bicubic interpolation is as follows:

$$I(x,y) = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{ij} x^i y^j = a_{00} + a_{10}x + a_{01}y + a_{11}xy + a_{02}y^2 + a_{21}x^2y + a_{12}xy^2 + a_{22}x^2y^2 + a_{30}x^3 + a_{03}y^3 + a_{31}x^3y + a_{13}xy^3 + a_{32}x^3y^2 + a_{23}x^2y^3 + a_{33}x^3y^3 \quad (2)$$

The coefficients a_{ij}, i,j=0,1,2,3 are obtained by calculating the gradients in both x and y directions and the cross derivative at each of the four corners of square. The bicubic interpolation produces sharper images than the nearest neighbor and bilinear interpolation methods both and it is perhaps the ideal combination of processing time and output quality. For this reason it is a standard in most of the image editing softwares and image capturing devices.

We will apply the above mentioned interpolation techniques to JPEG images in order to remove their artifacts. Basically these artifacts are due to some missing values in the DCT histogram, which are filled using interpolation. Once these missing values are obtained, the image forgery detection methods based on JPEG artifacts cannot identify the JPEG compression history of the image.

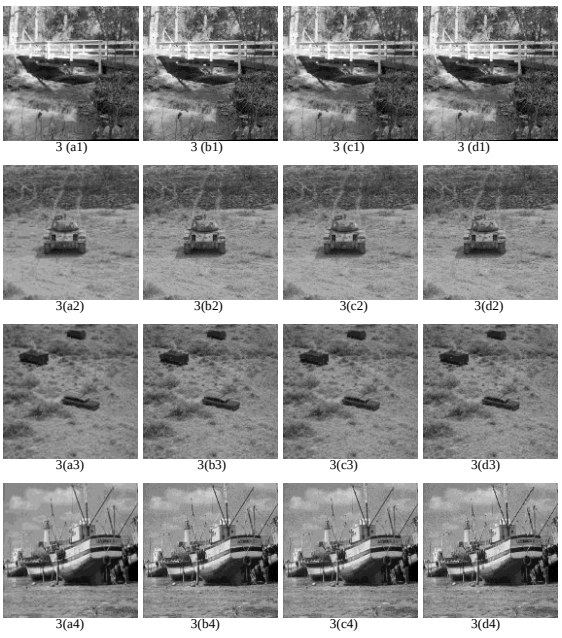
We first reduce the image by some factor of the original image through interpolation & then apply the same interpolation technique to enlarge this reduced image into original size. We apply above three

interpolation technique i.e. nearest neighbor, bilinear and bicubic interpolation on the images two times once to reduce & second to get the original size of the reduced image.

IV. Experimental Results

In our experiments we take 15 different images from USC SIPI image database [29], which are in .tiff format. First we convert these images into JPEG format with quality factor eighty as we need JPEG compressed images and we want to remove the JPEG artifacts. We apply above mentioned interpolation techniques to each of these JPEG images. For applying the interpolation technique we first reduce the image size by a factor of 0.9 of the original image & then apply the same technique to enlarge this reduced image into the original size. Similar type of approach is used in paper [30] for removing double JPEG compression detection using bilinear interpolation called shrink and zoom method. We applied this method with three interpolation methods and also compare their quality with different quality metrics.

We apply three different interpolation technique i.e. nearest neighbor, bilinear and bicubic interpolation on each image two times once to reduce image size & then to get the original size of the reduced image. We in fact performed experiments by reducing the images for different factors 0.8, 0.85. 0.90, 0.95 and we found that 0.9 is the optimal factor for removing the artifacts and getting the better image quality. We have also shown the results in terms of interpolated images using bicubic, bilinear and nearest neighbor techniques along with the original images in Figure 3, the images in the first column are the original images (5 images out of 15 images), the second column contains the bicubic interpolated images, the third column contains the bilinear interpolated images and the last column contains the nearest neighbor interpolated images.



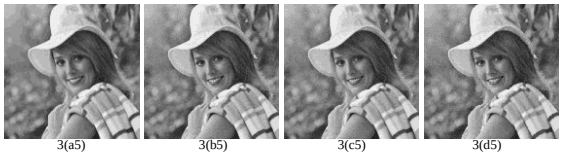


Fig.3. The First Column Contains 5 Original Images: (a1) Stream & Bridge, (a2) tank1, (a3) Car & APCs1, (a4) Fishing Boat, (a5) Girl (Elaine), Second, Third And Fourth Columns Contain Corresponding Bicubic, Bilinear And Nearest Neighbor Interpolated Images Respectively.

We have used various quality parameters namely mean square error (MSE), peak signal to noise ratio (PSNR), structural similarity index (SSIM)[18] and blind image spatial quality evaluator (BRISQUE)[19].

A. Mean Square Error (MSE)

It is defined as the average squared difference between the reference image (P) and the distorted image (Q), each of size m×n. It is calculated pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total number of pixels. It is computed by the following formula-

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[p(i,j)-Q(i,j)\right]^2 \tag{3}$$

B. Peak Signal to Noise Ratio (PSNR)

It is defined as follows-

$$PSNR = 10.\log_{10}\left[L^2/MSE\right] \tag{4}$$

Where L is the dynamic range of the pixel values.

Higher PSNR value indicates higher quality of the image.

C. Structural Similarity Index (SSIM) [18]

MSE and PSNR are computationally simple but they don't consider viewing conditions and the characteristics of the human visual perception. The SSIM is based on the local luminance, contrast and structural information. It is computed as follows-

$$SSIM = \frac{(2\mu_x\mu_y + C)(2\sigma_{xy} + D)}{(\mu_x^2 + \mu_y^2 + C)(\sigma_x^2 + \sigma_y^2 + D)} \tag{5}$$

Where μ_x, μ_y are the mean intensity, σ_x, σ_y are the standard deviation, σ_{xy} is the covariance and C, D are the constants.

D. Blind Image Spatial Quality Evaluator (BRISQUE) [19]

This image quality assessment model is based on natural scene statistics. This model is highly correlates with human subjective scores. It computes Mean subtracted contrast normalized coefficients (MSCN) over

the whole image. For an image I, the MSCN coefficient image, Î, is computed by

$$\hat{I} = \frac{I(i,j) - \mu(i,j)}{\sigma(i,j) + C} \tag{6}$$

where $\mu(i,j) = \sum_{k=-K}^{K} \sum_{l=-L}^{L} w_{k,l} I_{k,l}(i,j)$ and

$$\sigma(i,j) = \sqrt{\sum_{k=-K}^{K} \sum_{l=-L}^{L} w_{k,l} (I_{k,l}(i,j) - \mu(i,j))^2}$$

Here $w = \{w_{k,l} \mid k = -K,.....,K, l = -L,.....,L\}$ is a 2D circularly-symmetric weighting function and C is a constant.

With the help of MSCN, image quality is evaluated in SSIM.

The MSE, PSNR and SSIM are full-reference quality assessment measures; they require the original undistorted image to compare with the distorted image. The BRISQUE is no-reference quality assessment measure; it does not require any reference image for quality assessment.

We have compute the above mentioned performance parameters MSE, PSNR, SSIM and BRISQUE and their values are given in Tables 1, 2, 3 and 4 respectively. The smaller value of MSE and BRISQUE parameters indicate the good quality of the image, where as higher values of PSNR and SSIM indicate the good quality of the image.

We observe from Table 1 that the MSE value is best for bicubic interpolated images taken in our experiments for all images, followed by bilinear interpolated images and finally nearest neighbor interpolated images.

Table 1. MSE for Different Images using Different Interpolation Methods

Test Images	Mean Square Error for the test images taken from USC SIPI database [29]		
	Bicubic	Bilinear	Nearest
Stream & bridge	93.709	116.056	242.102
Tank 1	17.182	21.699	47.924
Car & APCs 1	11.576	14.721	32.663
Fishing Boat	35.763	45.761	97.247
Girl (Elaine)	34.472	43.541	96.244
Couple	27.446	34.624	75.856
Aerial	9.813	13.301	28.503
Truck	24.179	32.556	68.692
Airplane	9.697	12.831	30.076
Tank 2	44.909	54.234	124.974
Car & APCs 2	17.976	21.369	49.988
Truck & APCs 1	61.344	76.645	134.861
Truck & APCs 2	87.525	106.643	243.119
Tank 3	15.824	20.179	45.234
APC	12.001	14.202	32.729

In case of PSNR also the bicubic interpolated images have the best performance as evident from Table 2. The performance of bicubic interpolated image is followed by bilinear interpolated images and finally nearest neighbor interpolated images.

Table 2. PSNR of Images using Different Interpolation Methods

Test Images	Peak signal to noise ratio for the test images taken from USC SIPI database [29]		
	Bicubic	Bilinear	Nearest
Stream & bridge	28.413	27.484	24.291
Tank 1	35.781	34.766	31.325
Car & APCs 1	37.494	36.451	32.991
Fishing Boat	32.596	31.525	28.252
Girl (Elaine)	32.756	31.741	28.297
Couple	33.746	32.736	29.331
Aerial	38.212	36.891	33.581
Truck	34.296	33.004	29.761
Airplane	38.264	37.048	33.348
Tank 2	31.607	30.788	27.162
Car & APCs 2	35.583	34.832	31.142
Truck & APCs 1	30.253	29.285	26.831
Truck & APCs 2	28.709	27.851	24.272
Tank 3	36.137	35.081	31.576
APC	37.338	36.607	32.98147

Same is the case for SSIM parameter as shown in Table 3.

Table 3. SSIM of Images using Different Interpolation Methods

Test Images	Structural Similarity Index ratio for the test images taken from USC SIPI database [27]		
	Bicubic	Bilinear	Nearest
Stream & bridge	0.8927	0.8517	0.7706
Tank 1	0.9333	0.9075	0.8462
Car & APCs 1	0.9547	0.9375	0.8828
Fishing Boat	0.9158	0.8823	0.8097
Girl (Elaine)	0.9157	0.8832	0.8055
Couple	0.9176	0.8855	0.8099
Aerial	0.9516	0.9321	0.8869
Truck	0.9239	0.8916	0.8224
Airplane	0.9567	0.9389	0.8849
Tank 2	0.9321	0.9118	0.8513
Car & APCs 2	0.9279	0.9062	0.8492
Truck & APCs 1	0.9415	0.9223	0.8659
Truck & APCs 2	0.9321	0.9046	0.8315
Tank 3	0.9442	0.9249	0.8656
APC	0.9757	0.9689	0.9469

As per the BRISQUE parameter is concern the bicubic interpolated images either have better or comparative performance in case of most of the images as shown in Table 4.

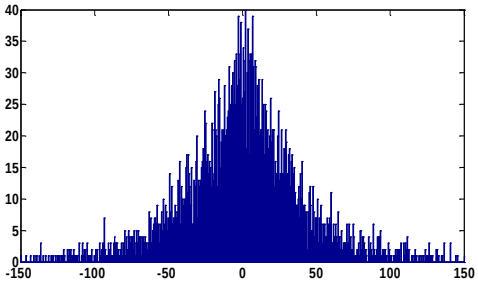
Table 4. BRISQUE of Images using Different Interpolation Methods

Test Images	Blind image spatial quality evaluator for the test images taken from USC SIPI database			
	Original	Bicubic	Bilinear	Nearest
1	13.482	15.442	23.547	23.806
2	17.223	22.888	31.297	25.701
3	29.285	33.087	40.371	35.179
4	13.295	20.768	29.557	22.544
5	16.415	23.147	31.668	24.861
6	13.408	21.258	29.375	23.271
7	22.859	25.259	30.765	27.264
8	18.037	26.456	34.894	26.662
9	26.893	31.641	39.799	31.558
10	18.609	23.414	29.181	24.098
11	15.639	5.0905	13.270	20.228
12	24.781	29.096	33.522	29.012
13	17.823	24.212	28.796	27.102
14	26.888	31.348	37.826	31.337
15	33.459	31.054	35.711	35.2661

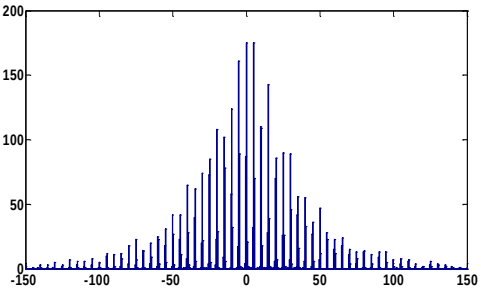
The histogram of AC components in DCT domain for natural or uncompressed images follow the Laplacian distribution as can be seen in Figure 4(b) for the image Stream & Bridge given in Figure 4(a). But in JPEG compressed images this distribution gets disturbed and it becomes comb like pattern as shown in Figure 4(c). This comb like pattern helps in identifying that the image is previously JPEG compressed. We apply above discussed all three interpolation techniques namely bicubic, bilinear and nearest neighbor methods on the image Stream & Bridge (refer Figure 4(a)) and the histogram of (1,1) DCT coefficients ((0,0) is DC coefficient) of the image are shown in Figs. 4(d)-4(f), respectively.

As evident from Figs. 4(d)-4(f) the histograms follow the Laplacian distribution similar to that of the uncompressed image.

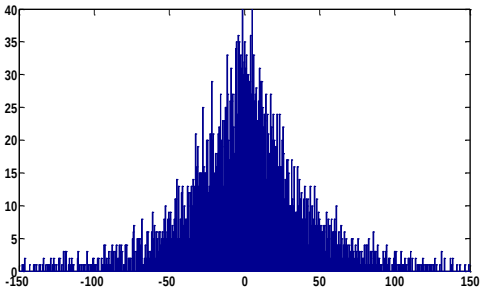
4 (a)



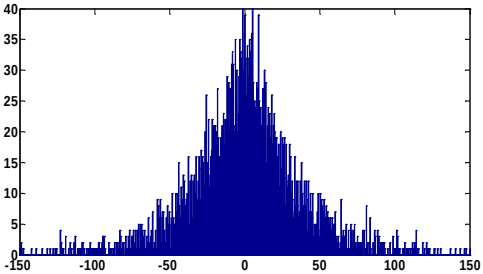
4 (b)



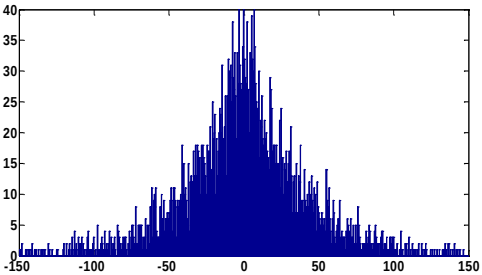
4 (c)



4 (d)



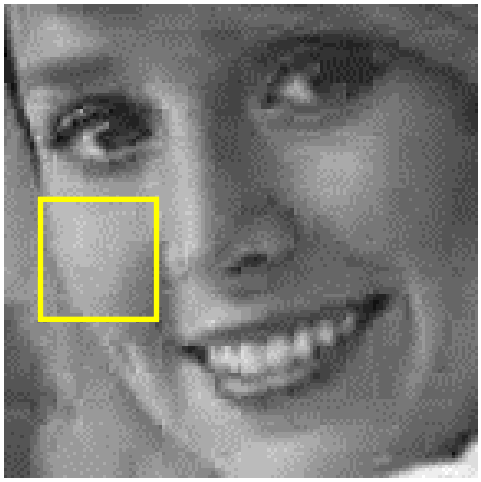
4 (e)



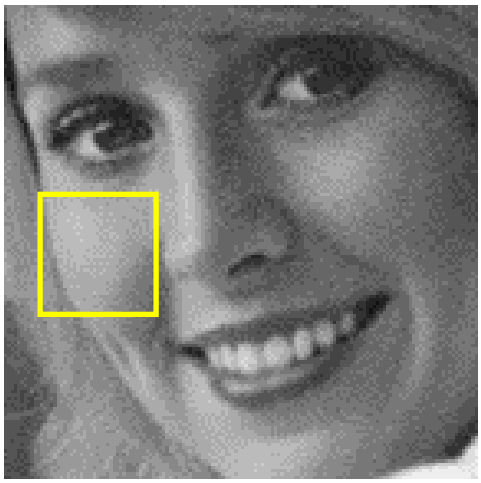
4 (f)

Fig.4. (a) Original Stream and Bridge Image (b) Histogram of (1,1) DCT Subband for (a) Image. (c) Histogram of (1,1) DCT Subband of JPEG Compressed Image (d) Histogram of (1,1) DCT Subband of Bicubic Interpolated Image (e) Histogram of (1,1) DCT Subband of bilinear interpolated image (f) Histogram of (1,1) DCT Subband of Nearest Neighbor Interpolated Image.

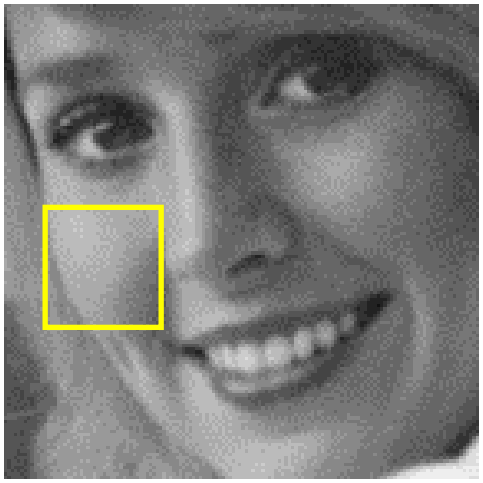
One of the artifacts of JPEG compressed images is blocking artifact as shown in Figure 5(a) inside the red rectangle. Figures 5(b)-5(d) show the bicubic, bilinear and nearest neighbor interpolated images respectively. As evident from these figures the blocking artifacts either have been removed or have been reduced significantly. Bicubic interpolated image (Fig. 5(b)) also looks best in comparison to bilinear and nearest neighbor interpolated images.



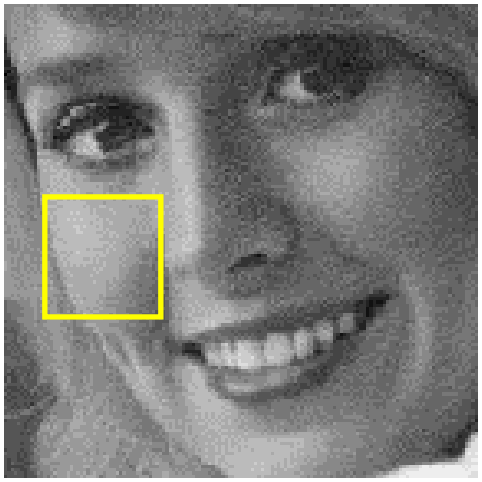
5 (a)



5 (b)



5 (c)



5 (d)

Fig.5. (a) A portion of Girl (Elaine) JPEG Compressed Image 5(b)-(d) Bicubic, Bilinear and Nearest Neighbor Interpolated Images Respectively

V. Conclusion And Future Work

As the JPEG compression artifacts are basis of many image forgery detection methods. So by removing these artifacts forgery detection becomes more challenging and sometimes impossible. In this paper we apply different interpolation methods and verify experimentally that JPEG compression artifacts are removed by using interpolation methods successfully. We have also verified the quality of the various antiforensic images with different state of the art quality assessment methods. We found that bicubic interpolation gives the best result for all quality assessment methods followed by bilinear interpolation and nearest neighbor interpolation methods.

This method successfully removes JPEG artifacts but it leaves traces of interpolation. To remove traces of interpolation, random selection of interpolation method can be used for each pixel. Also many other state of the art interpolation methods can be used with random selection to remove the traces of interpolation and can get the image of better quality.

References

[1] Z. Fan, R. L. de Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation, IEEE Transaction on Image Processing, vol. 12, no. 2, pp. 230–235, Feb. 2003.

[2] H. Farid, Exposing digital forgeries from JPEG ghosts, IEEE Transaction on Information Forensics and Security, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[3] X. Feng, G. Doërr, JPEG recompression detection, Proceedings of the SPIE-Media Forensics and Security II, vol. 7541 of , 75410J, Jan. 2010.

[4] F. Huang, J. Huang, Y. Q. Shi, Detecting double JPEG compression with the same quantization matrix, IEEE Transaction on Information Forensics and Security, vol. 5, no. 4, pp. 848–856, Dec. 2010.

[5] A. Bianchi, T. De Rosa, A. Piva, Improved DCT coefficient analysis for forgery localization in JPEG images, in proceeding of the international conference on

Acoustics, Speech, and Signal Processing, Prague, Czech Republic, May 2011.
[6] M. Stamm, S. Tjoa, W. S. Lin, K. J. Ray Liu, Antiforensics of JPEG compression, in proceeding of the international conference on Acoustics, Speech, and Signal Processing, pp. 1694–1697, 2010.
[7] H. Li, W. Luo, J. Huang, Countering anti-JPEG compression forensics, in Proceeding of the 19th. IEEE International Conference on Image Processing, pp. 241-244, IEEE, 2012.
[8] Milani S, Tagliasacchi M, Tubaro S, Antiforensic attacks to Benford's law for detection of double compressed images, in proceeding of the international conference on Acoustics, Speech, and Signal Processing, pp 500-505, 2013.
[9] C. Pasquini and G. Boato, JPEG compression anti-forensics based on first significant digit distribution, Proceeding of the IEEE international workshop on multimedia signal processing, pp 500-505, 2013.
[10] W. Fan, K. Wang, F. Cayre, Z. Xiong, JPEG anti-forensics using non-parametric DCT quantization noise estimation and natural image statistics, in Proceeding of the ACM international Workshop Information Hiding and Multimedia Security, pp. 117–122, 2013.
[11] J. He, Z. Lin, L. Wang, X. Tang, Detecting doctored JPEG images via DCT coefficient analysis, in Proceeding of the European Conference on Computer Vision (ECCV), vol. 3953, pp. 423-435, Mar. 2006.
[12] Z. Lin, J. He, X. Tang, C.K. Tang, Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis, Pattern Recognition, vol. 42, no.11, pp. 2492-2501, 2009.
[13] Y.-L. Chen, C.-T. Hsu, Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection, IEEE Transaction on Information Forensics and Security, vol. 6, no. 2, pp. 396-406, Jun. 2011.
[14] S. Ye, Q. Sun, E.-C. Chang, Detecting digital image forgeries by measuring inconsistencies of blocking artifact, in Proceeding of the IEEE International Conference of Multimedia Expo, pp. 12-15, Jul. 2007.
[15] Zheng Er-gong, Ping Xi-jian, Passive-blind forensics for a class of JPEG image forgery, Journal of Electronics information technology, vol.32, no.2, p.394, 2010.
[16] W. Li, Y. Yuan, N. Yu, Passive detection of doctored JPEG image via block artifact grid extraction, Signal Processing, vol. 89, no. 9, pp. 1821-1829, 2009.
[17] M. Barni, A. Costanzo, L. Sabatini, Identification of cut & paste tampering by means of double-JPEG detection and image segmentation, Proceeding of the IEEE International Symposium of Circuits System, pp. 1687-1690, Jun. 2010.
[18] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: From error visibility to structural similarity, IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, Apr. 2004.
[19] A. Mittal, A. K. Moorthy, A. C. Bovik, No-Reference Image Quality Assessment in the Spatial Domain, IEEE Transactions on Image Processing, 2012.
[20] S.Kumar, J. V. Desai, and S.D. Mukherjee. "Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors.", IJIGSP Vol.7, No.6, May 2015.
[21] M. K. Johnson, H. Farid, Exposing digital forgeries in complex lighting environments, IEEE Transaction on Information Forensics and Security, vol. 2, no. 3, pp. 450-461, Sep. 2007.
[22] J. Lukas, J. Fridrich, M. Goljan, Detecting digital image forgeries using sensor pattern noise, Proceeding of the SPIE Electronic imaging, security, stegnography, and watermarking of multimedia contents VIII, vol. 6072. 2006.
[23] P. Ferrara, T. Bianchi, A.D. Rosa, A. Piva, Image forgery localization via fine-grained analysis of CFA artifacts, IEEE Transaction on Information Forensics and Security, vol 7, no 5, pp. 1566-1577, 2012.
[24] D. Fu, Y. Q. Shi, W. Su, A generalized Benford's law for JPEG coefficients and its applications in image forensics, Proceeding of the SPIE, vol. 6505, pp. 39–48, Jan. 28 – Feb. 1, 2009.
[25] W. Fan, K. Wang, F. Cayre, Z. Xiong, JPEG AntiForensics with improved tradeoff between forensic undetectability and image quality, IEEE Transaction on Information Forensics and Security, vol.9, no.8, August 2014.
[26] Kaimal, A.B., Anitha, J., Manimurgan, S., A modified anti-forensics technique for removing detectable traces from digital images, proceeding of the international Conference on computer, communication and informatics, pp.1-4, 2013.
[27] J.A. Parker, R.V. Kenyon, D.E. Troxel, Comparison of interpolating methods for image re-sampling, IEEE Transactions on Medical Imaging, pp. 31–39, 1983.
[28] R. Keys, Cubic Convolution Interpolation for DigitalImage Processing, IEEE Transaction on Acoustics, speech and signal processing, vol ASSP-29, No. 6, Dec 1981.
[29] A G. Weber, "The USC-SIPI Image Database: USC SIPI Report 315", California, October 1997.
[30] P. Sutthiwan, Y.Q. Shi, "Anti-forensics of double JPEG compression detection," in Proceedings International Workshop of Digital Forensics Watermarking, 2011, pp. 411-424.

Author's Profiles

Saurabh Agarwal has received his B.Tech from Barkatullah University, Bhopal in Computer Science and Engineering and his M.Tech from Uttar Pradesh Technical University, Lucknow in Software Engineering.

He is pursuing Ph.D in Department of Computer Engineering, Netaji Subhas Institute of Technology, New Delhi, India.

Satish Chand did his M.Sc. in Mathematics from Indian Institute of Technology, Kanpur, India and M.Tech. in Computer Science from Indian Institute of Technology, Kharagpur, India and Ph.D. from Jawaharlal Nehru University, New Delhi, India. Presently he is working as a Professor in Computer Engineering Division, Netaji Subhas Institute of Technology, Delhi, India. Areas of his research interest are Multimedia Broadcasting, Networking, Video-on-Demand, Cryptography, and Image processing.