Acronyms

**JPEG**: The Joint Photographic Experts Group

**DCT**: Discrete Cosine Transform

**FPR**: False positive rates

**TPR**: True positive rates

**TNR**: True negative rates

**TIFF**: Tagged Image File Format

**ROC**: Receiver operating characteristics

**NEROC**: Nash equilibrium receiver operating characteristics

**UCID**: Uncompressed Colour Image Database
Abstract:

Due to increasing reliability on digital images to communicate visual information, a number of forensic techniques have been developed to verify the authenticity of digital images. Amongst the various techniques, the techniques that make use of image’s compression history and its associated compression fingerprints are successful. Anti-forensic techniques capable of fooling forensic algorithms have been considered. It's well known that JPEG image compression can result in quantization artifacts and blocking artifacts. There are plenty of forensic techniques making use of image's compression fingerprints to verify digital images. One typical anti forensic method is adding anti-forensic dither to DCT transform coefficients and erasing blocking artifacts to remove compression history. In this paper, a countering anti-forensic method has been proposed based on estimating the noise added in the process of erasing blocking artifacts, which has only one-dimensional feature and time-saving.
**Introduction:**

The widespread availability of the Internet, along with the development of affordable, high quality digital cameras has resulted in an environment where digital images have supplanted traditional film-based photographs as the primary source of visual information in several scenarios. Unfortunately, the ease with which digital images can be manipulated by photo editing software has created an environment where the authenticity of digital images is often in doubt. Researchers can make a preliminary judgment of the authenticity of digital images, by checking whether an image is previously compressed. This can be used as the auxiliary decision-making of digital image forensics, where JPEG compression detection is an important part of digital image forensics. Image compression fingerprints are of particular forensic significance due the fact that most digital images are subjected to compression either by the camera used to capture them, during image storage, or for the purposes of digital transmission over the Internet. Techniques have been developed to determine whether an image saved in a lossless format has ever undergone JPEG compression [1 - 5]. The quantization table used during compression can be estimated to detect the evidence of jpeg compression.

In section-1 of this project report, a brief description of JPEG compression and its anti-forensics is given. Section-2 emphasizes on, how anti-forensic dither is added to the DCT coefficient of the compressed image [6]. Section-3 summarizes the de-blocking theorem. Section-4 illustrates the evaluation of the blocking detection and the noise level detection. Section-5 consists of the performance characteristics and the Nash Equilibrium Performance curves, based on the experimental results from the implementation of the various steps involved in retaliation based on the noise level estimation.

**1. JPEG compression and its ANTI-FORENSICS:**

**JPEG compression:**

![JPEG Compression Diagram](image-url)
JPEG [17] is the Joint Photographic Experts Group compression scheme for still images. JPEG is very well known ISO/ITU-T standard created in late 1980's. JFIF [18] is the JPEG File Interchange Format used for exchanging image files compressed using JPEG compression. JPEG compression is based on psycho-visual studies of human perception. To convert to a smaller file size, this type of compression drops the least-noticeable picture information. JPEG (Joint Photographic Experts Group) [17] is very well known ISO/ITU-T standard created in late 1980's. There are several modes defined for JPEG including baseline, progressive and hierarchical. JPEG compression can be divided into four steps: color mode conversion and sampling, DCT, quantization, and entropy coding. JPEG compression starts by segmenting an input image into several non-overlapping 8×8 pixel blocks, then it uses the 2-D DCT to transform each block data into 64 DCT coefficients. In quantization step, each coefficient value is quantized by a parameter $Q_{i,j}$. This procedure results in DCT coefficient quantization fingerprint and the tampering artifacts. Even though there are many works for the artifacts detecting brought by JPEG compression [1 - 5] for digital image forensics, an anti-forensic method [6] can deceive detectors by first adding anti-forensic dither to DCT coefficients to imitate the original uncompressed histograms and erases blocking artifacts to remove the compression history by boundary blurring. As only adding the anti-forensic dither cannot remove the blocking artifact, [6], to erase the compression history, the forger must remove blocking artifact by first median filtering an image and then adding low-power white Gaussian noise to each of its pixel values. Both the window size of the median filter and the variance of the noise can affect the de-blocking effect. In order to detect the forged images, noise level estimation [7] has been employed to estimate the noise added in the de-blocking process. For a particular image, the noise level of the image is estimated and compared with a threshold to determine whether it is forged.
ANTI-FORENSICS OF JPEG COMPRESSION:

The segmentation of an input image into several non overlapping 8 × 8 pixel block in JPEG compression result in pixel domain discontinuity which is called blocking artifact, especially in the boundaries of these segments.

Fig. 2: JPEG compression process and its anti-forensic modified process. [6].

The figure 2 shows how an image is JPEG compressed and how it is anti-forensically modified. The blocks above the dotted line are the JPEG compression process, and blocks below the dotted line shows the anti-forensic process.

In order to remove the quantization artifact for a JPEG compressed image, i.e. to make the sub band coefficient value distribution match an original one, the anti forensic dither is added to the DCT coefficient.
Fig.3 consists of JPEG compressed image using a quality factor of 90(a), 70 (b), 30 (C), and 10 (d) followed by the addition of anti-forensic dither to its DCT coefficients.

The anti-forensic dither is described as follows:

The distribution of coefficient values within a particular AC DCT sub band can be modeled as the Laplace distribution [8-10].

For an uncompressed image, assume $X$ to be the DCT coefficient at the block position $(i, j)$:

$$P(X = x) = \frac{\lambda}{2} e^{-\frac{|x|}{\lambda}}$$

($\lambda$ - Laplacian parameter generated by maximum likelihood estimation)

AC coefficients of each sub band are distributed as discrete Laplace distribution. The distribution for the coefficients at the $(i,j)$-th position, using the quantization step $Q_{i,j}$:

$$P(Y = y) =
\begin{cases} 
\frac{\lambda Q_{i,j}}{2} & \text{if } y=0 \\
1-e^{-\lambda |y|} \sinh\left(\frac{\lambda Q_{i,j}}{2}\right), & \text{if } y=kQ_{i,j} \\
0, & \text{otherwise}
\end{cases}$$

$$Y = Q_{i,j}\text{round}\left(\frac{X}{Q_{i,j}}\right)$$

Let $N = N_0 + N_1$ be the total number of observations of the current DCT
Sub band, where $N_0$ - number of coefficients taking zero values,
$N_1$ - number of nonzero coefficients,

$$S = \sum_{k=1}^{N} |y_k|$$

The model parameter can be calculated using the equation

$$\hat{\lambda} = -\frac{2}{Q_{i,j}} \ln(\gamma) \quad (3)$$

And here $\gamma$ is defined as:

$$\gamma = \frac{-N_0 Q_{i,j}}{2NQ_{i,j} + 4S} +$$
$$\sqrt{\frac{N_0^2 Q_{i,j}^2 - (2N_1 Q_{i,j} - 4S)(2NQ_{i,j} + 4S)}{2NQ_{i,j} + 4S}} \quad (4)$$

To hide the compression evidence, [6] dither is introduced into the AC coefficients to approximately restore the histogram of each sub band, By:

$$Z = Y + D, \quad (5)$$

Where $Z$ is the anti-forensically modified coefficient and $D$ is the additive dither. The noise distribution for the coefficient $Y$ of zeros value at the $(i, j)$-th position, is given by:

$$P(D = d | Y = 0) = \begin{cases} \frac{1}{c_0} e^{-\hat{\lambda}|d|}, & \text{if } \frac{-Q_{i,j}}{2} \leq d \leq \frac{Q_{i,j}}{2} \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

where $c_0 = \frac{2}{\hat{\lambda}}(1-e^{-\hat{\lambda}Q_{i,j}/2})$

The distribution of the anti forensic dither added to nonzero quantized DCT coefficients is given by:
Quality factor:

Image quality is the measure of how accurately our image matches the source image which is observed by visible factors like brightness and evenness of illumination, contrast, resolution, geometry, colour fidelity and colour discrimination of an observed image. Although there are not any standardized quantization Matrices, most implementations of JPEG compression use a set of quantization matrices indexed by a quality factor from the set \{1, 2, \ldots, 100\}. These matrices are used in the reference implementation provided by the Independent JPEG Group and they are called as standard matrices [19]. A parameter called Q factor is used to “tune” the quality of the JPEG image. It vary from range between 1 to 100. A factor 1 produces the image with maximum compression (i.e. smallest) but with worst quality. The factor of 100 produces the image with least compression (i.e. largest) but best quality. The optimal Q factor depends on the content of image and varies as per the size of image.

\[
P(D = d \mid Y = q_k) = \begin{cases} 
  1 & \text{if } \frac{-Q_{i,j}^L}{2} \leq d \leq \frac{Q_{i,j}^L}{2} \\
  0 & \text{otherwise} 
\end{cases}
\]

where \( c_1 = (1/\hat{\lambda})(1-e^{-\hat{\lambda}Q_{i,j}}) \).

Fig. 4: JPEG compressed image using a quality factor of 65.
Fig. 4 (a) shows the Histogram of (2, 2) DCT coefficients taken from an uncompressed version of the image, (b) the same image after JPEG compression. DCT quantization artifacts are clearly visible in the histograms obtained from the JPEG compressed image. These artifacts are absent from the histograms of anti-forensically modified DCT coefficients.

Fig. 5: Anti-forensically modified image.
Fig. 6: Histogram of an anti-forensically modified copy of the JPEG compressed image. The histograms of the anti-forensically modified coefficients closely match those obtained from the uncompressed image which infers that the anti-forensically modified image can be passed off as never-compressed.

Fig. 7(a): An uncompressed image
Fig. 7: An uncompressed image (a). Histogram of coefficient values from the (2,2) DCT sub band taken from image [a], (b), the same image after JPEG compression (c), and an anti-
forensically modified copy of the JPEG compressed image. The histograms in fig. 7 indicate that, for an image which is JPEG compressed but anti-forensically modified. In the anti-Distribution of AC coefficient values also obeys the Laplace distribution and the quantization fingerprint is removed by adding anti-forensic dither. The experimental results [6] show that no evidence of quantization [4] is presented after adding the forensics dither. Even though evidence of quantization can be removed by adding the anti-forensic dither, blocking artifacts cannot be removed.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>H</td>
</tr>
</tbody>
</table>

Fig. 8: For each block the numbers $Z'(i, j) = |A + D - B - C|$ and $Z''(i, j) = |E + H - F - G|$ are computed. Difference within a block and spanning across a block boundary are explained in the fig. 8, involving same pixel pattern but spanning around multiple blocks. For each block $(i, j)$, we compute:

$$Z'(i, j) = |A + D - B - C| \quad Z''(i, j) = |E + H - F - G|$$

(8)

By examining the difference between two histograms, the blocking artifacts are detected:

$$K = \sum_{n} |h_1(n) - h_2(n)|$$

(9)

Where $h_1$ is the histogram of $Z'$ each image block, and $h_2$ is the histogram of $Z''$. Two histograms for an uncompressed image and a JPEG compressed image are shown in Fig. 9(a) and Fig. 9(b). It is observed that the difference ($K$) between $h_1$ and $h_2$ is very small for an uncompressed image, whereas for a JPEG compressed image, $K$ is remarkably large. Hence, the statistic $K$ can be used to determine whether an image is JPEG compressed. For an image to be classified as a JPEG compressed one, $K$ should be greater than the threshold $t_1$. 
Moreover, for an uncompressed image, $h_1(1) > h_1(0)$ and $h_2(1) > h_2(0)$ and for a JPEG compressed image, $h_1(1) > h_1(0)$ and $h_2(1) > h_2(0)$ may not meet or not meet at the same time.

Fig. 9: $h_1$ and $h_2$ obtained from (a) an uncompressed image, (b) the same image after JPEG compression using a quality factor of 75.
By median filtering, difference between $h_1$ and $h_2$ is removed to remove blocking artifacts (as shown in Fig. 9(c). But, median filtering cannot remove the blocking artifacts completely because of $h_1(1) < h_1(0)$ and $h_2(1) < h_2(0)$. Hence, a zero mean Gaussian random noise is added after median filtering. Fig. 9(d) shows that adding noise after median filtering can achieve the de-blocking purpose.

3. Summary of the De-blocking Algorithm:

$$v_{i,j} = med_z(u_{i,j}) + n_{i,j}$$  \hspace{1cm} (10)
Where \( u_{ij} \) represents the pixel value at location \((i, j)\) in an unmodified image, and \( v_{ij} \) denotes its de-blocked counterpart, \( \text{med}(\cdot) \) denotes a two-dimensional median filter with a square window of size \( s \) pixels, and \( n_{ij} \) is a zero mean Gaussian random noise with variance \( \sigma^2 \). By adjusting the window sizes and variance \( \sigma^2 \), better anti-forensic results can be achieved.

\[
\sigma^2
\]

**TABLE I BLOCKING ARTIFACT DETECTION ACCURACY**

Table I shows the results of blocking artifact detection accuracy from experiments by varying the window size(s) and the variance \( \sigma \) for FPR (False positive rates) varies in a given interval and the optimal threshold to obtain the Accuracy Rate = \((\text{TPR} + \text{TNR}) / 2\). TPR is true positive rates and TNR is true negative rates. The results show that the above method can remove the blocking artifact effectively.

<table>
<thead>
<tr>
<th>Quality factor</th>
<th>JPEG compressed image</th>
<th>Anti-forensic modified image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>s=3, ( \sigma=3 )</td>
<td>s=3, ( \sigma=2 )</td>
</tr>
<tr>
<td>95</td>
<td>93.05%</td>
<td>51.38%</td>
</tr>
<tr>
<td>75</td>
<td>99.48%</td>
<td>51.64%</td>
</tr>
<tr>
<td>55</td>
<td>99.65%</td>
<td>52.95%</td>
</tr>
</tbody>
</table>

4. RETALIATION BASED ON THE NOISE LEVEL ESTIMATION:

Recently, several methods related to noise level estimation have been proposed. Some methods used the changes in kurtosis values of images to estimate the noise level [11]. In other method, the noise level is estimated from the selected weak textured patches using PCA [7]. Here weak textured patches are selected using PCA to estimate the noise level, since it is more accurate than the method using kurtosis values of images to estimate the noise level. A block-based approach uses statistical analysis of a histogram of local signal variances to compute an estimation of image noise variance. It uses high-pass directional operators to determine the homogeneity of blocks besides using average noise variances.
The noise level estimation can be summarized as the following major steps:

1. Decomposing the test image into overlapping patches. The default patch size is $7 \times 7$ pixels.
2. Estimating an initial noise level $\sigma_e$ from the covariance matrix as:

   \[
   \sigma_e^2 = \lambda_{\min}(\sum_{y'})
   \]

   (11)

   Where $\Sigma_{y'}$ is the covariance matrix of the selected patches and $\lambda_{\min}$ is the minimum Eigen value of $\Sigma_{y'}$.
3. Selecting the weak textured patches from the test image using a threshold that varies with $\sigma_e$.
4. Estimating a new noise level $\sigma_e$ using the selected patches. The process of step 3 and 4 is iterated until $\sigma_e$ is stable. Here $\sigma_e$ is used to denote the estimated noise level of a test image.
Fig. 11 Performance of the noise level estimation using the two methods.

**Countering Anti-forensics and Its Evaluation:**

Using the algorithm from [7], noise level estimation method is applied to counter the anti-forensic method [6]. In order to forge an image, the forger must add the Gaussian noise to erase the blocking artifacts. That is, forged images may present a higher noise level than original images. Therefore, effective way of detecting forgery is by estimating the noise level of the image and this assumption is proved by the experimental results showed in the Fig.12 (a). The blue “+” represents the original image of TIFF format, and green “*” represents the images after anti-forensics ($s = 2, \sigma = 2$) [6]. It can be seen that most of the original images’ noise level are lower than 0.5. Since the noise level is very sensitive to JPEG compression, the noise level decreases to nearly zero, when images are JPEG compressed. The forged images are first JPEG compressed, and then low-power white Gaussian noise is added so that the estimated noise level is near to $\sigma$. Complex textured images can have a higher noise, since noise level estimation is related to the texture and size of an image. The larger size image can have more accurate detection rate than that of small size images.
Fig. 12(a): The noise level estimation in which images come from UCID with the resolution of $512 \times 384$.

Fig. 12 (b): The noise level estimation in images which are in TIFF format with the resolution of $1024 \times 768$.

From the plots 12(a) and 12(b), it is inferred that the noise level estimation is more accurate when the image size is larger.
5. EVALUATION:
An assumption is considered such that the forger adopts the anti-forensic method proposed in [6] and can only adjust the added noise variance $\sigma$. A reasonable variance of the noise is selected to cover the tampering trace and not to introduce new artifacts. Here blocking detection is performed first following the noise level detection.

a) Blocking detection:
The forger performs blocking detection $\delta_b$ based on the statistics $K$, $h_1(1)$ - $h_1(0)$ and $h_2(1)$ - $h_2(0)$. For an uncompressed image, $K$ is relatively small and $h_1(1) > h_1(0)$ and $h_2(1) > h_2(0)$. For a JPEG compressed image is larger. Moreover, $h_1(1) > h_1(0)$ and $h_2(1) > h_2(0)$ may not meet or not meet at the same time. Hence for a test image $I$, the blocking detection in the first stage can be expressed as hypothesis testing problem.

$$\hat{\delta}_b(I) = H_0^{(1)}$$

where $I$ is an uncompressed image, i.e. $I$ is original.

$$\hat{\delta}_b(I) = H_1^{(1)}$$

Where $I$ is a JPEG compressed image and $H_0^{(1)}$ denotes the first stage.

The acceptance region of $H_0^{(1)}$ is:

$$I: K < t_1 \text{ and } h_1(1) > h_1(0) \text{ and } h_2(1) > h_2(0)$$

(12)

Where $t_1$ is chosen according to the false alarm rate.

$b)$ Noise level detection:
Noise level of the images is estimated and accepted in $H_0^{(1)}$. When $I$ is forged; the noise level $\sigma_e$ is higher with respect to $I$ that is originally uncompressed. Thus, the noise level detection can be expressed as a hypothesis testing problem.

$$H_0^{(2)} : I \text{ is an originally uncompressed image. (} I \text{ is original).}$$
$H_1^{(2)}$ : $I$ is a forged image, i.e. $I$ is JPEG compressed and anti-forensically modified. (I is forged). Upper index "$^{(2)}$" denotes the second stage. The acceptance region of is:

$$I: \sigma_e(I) < t_2 \quad (14)$$

Where $t_2$ is chosen according to the false alarm rate defined as:

$$P_{fa}^{(2)} = P(\sigma_e(I) > t_2 | I \text{ is original}) \quad (15)$$

The total detection rate of the blocking detection and the noise level detection can be denoted as:

$$P_d = P(\delta_b(I) = H_1^{(1)} \cup \sigma_e(I) > t_2) | I \text{ is forged}) \quad (16)$$

The total probability of false alarm rate is defined as:

$$P_{fa} = P_{fa}^{(1)} + P_{fa}^{(2)} \quad (17)$$

For a given $P_{fa}^{(1)}$ and $P_{fa}^{(2)}$, a tradeoff is made between $P_{fa}^{(1)}$ and $P_{fa}^{(2)}$ to seek an optimal $P_d$.

Obviously, the optimal $P_{fa}^{(1)}$ would vary with $\sigma$. From the forger’s side, there is a tradeoff in choosing the added noise variance $\sigma$. The optimal $\sigma$ would vary with $P_{fa}^{(1)}$. The utility of the investigator is denoted as:

$$U_1(P_{fa}^{(1)}, \sigma) = P_d(P_{fa}^{(1)}, \sigma) \quad (18)$$

And the utility of the forger is denoted as:

$$U_2(P_{fa}^{(1)}, \sigma) = -P_d(P_{fa}^{(1)}, \sigma) \quad (19)$$
Based on this analysis, interplay between the investigator and the forger is realized as the set of strategies that the investigator can use, and the set of strategies that the forger can use, where corresponds to a too strong noise which would introduce significant visual distortions.

6. EXPERIMENTAL RESULTS:

A. The Performance:
Experiments were performed on 250 images from the Uncompressed Color Image Database (UCID) [12]. All the images are converted to 8-bit gray-scale images and the 250 uncompressed images are first JPEG compressed at a given Quality factor and then the DCT coefficient quantization fingerprints are removed from the JPEG compressed images by adding anti-forensic dither to the DCT coefficients using the anti-forensic method [6]. Afterwards, each image is de-blocked with the algorithm proposed in [6] and the window size of the median filter and standard variance of the noise are chosen accordingly. Finally, the noise levels of the original images and the forged images are estimated using the countering technique and a threshold is selected to classify the two group images. For a particular image to be classified as an original one, image's noise level should be lower than the threshold, else it is a forged image.

Fig. 13: ROC curves with proposed method for different quality factors

ROC (receiver operating characteristic curves) have been plotted for different quality factors of 55, 75 and 95 respectively, with parameters \((s = 3, \sigma = 3)\) which shows that the TPR increases with the quality factor.
The detection accuracy with different quality factors are listed in Table II and different parameters, and it can be observed that proposed countering anti-forensic method can achieve average detection accuracy above 95%. Proposed method is more effective, since the lower quality factor needs larger $\sigma$ to remove the blocking artifacts.

<table>
<thead>
<tr>
<th>Quality factor</th>
<th>$S=3, \sigma=3$</th>
<th>$S=3, \sigma=2$</th>
<th>$S=2, \sigma=2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>95</td>
<td>99.48%</td>
<td>99.14%</td>
<td>98.95%</td>
</tr>
<tr>
<td>85</td>
<td>99.48%</td>
<td>99.29%</td>
<td>97.05%</td>
</tr>
<tr>
<td>75</td>
<td>99.48%</td>
<td>99.33%</td>
<td>98.99%</td>
</tr>
<tr>
<td>65</td>
<td>99.48%</td>
<td>99.36%</td>
<td>98.77%</td>
</tr>
<tr>
<td>55</td>
<td>99.48%</td>
<td>99.36%</td>
<td>97.91%</td>
</tr>
</tbody>
</table>

### TABLE II
DETECTION ACCURACY WITH THE PROPOSED METHOD

The detection accuracy of the method [13] is less than 80%, whereas the proposed method detection accuracy is over 95%. The advantage of our proposed method is that only one-dimensional feature set is used and has low computational complexity, whereas detection method in [14] is more time-consuming since it is based on a 100-dimensional feature set.

<table>
<thead>
<tr>
<th>D</th>
<th>QF=95</th>
<th>QF=85</th>
<th>QF=65</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>71.26%</td>
<td>75.90%</td>
<td>75.79%</td>
</tr>
<tr>
<td>100</td>
<td>99.40%</td>
<td>99.61%</td>
<td>99.70%</td>
</tr>
<tr>
<td>Implemented</td>
<td>99.10%</td>
<td>99.22%</td>
<td>99.32%</td>
</tr>
</tbody>
</table>

### TABLE III
DETECTION ACCURACY

2) The Nash Equilibrium Performance:

While applying the proposed theory, it can be observed from the experimental results, that if the attacker knows the existence of this method, optimal strategy is to add less noise after median filtering. For the forger side, choosing the reasonable strength of the noise helps them to avoid the detection of blocking artifact and leaves less other detectable traces and this restricts the process of anti-forensics. For the investigator side, the strategy is how to allocate the FPR between the blocking detection and the noise level detection.

Nash equilibrium strategies are considered by solving the following equation [15]:

$$\left( P_f^{(1)} , \sigma^* \right) = \arg \max_{P_{fa}^{(1)}} \min_{\sigma} U_1 \left( P_{fa}^{(1)} , \sigma \right)$$

(20)
The Fig. 14 shows the performance when the total probability of false alarm rate $P_{fa}$ is 0.2 and JPEG quality factor is 50. X-axis - false alarm rate $P_{fa}$ (1) used in the blocking detection, Y-axis - noise standard variance $\sigma$.

The Nash equilibrium is $(0.02, 0.4)$ and the Total Detection rate $P_D$ is 86.7%. $\hat{P}_{fa}^{(1)} = 0.02$ denotes that the optimal strategy of the investigator is choosing $\sigma^* = 0.4$. $P_{fa}^{(1)} = 0.02$, and $\sigma^* = 0.4$ means that choosing $\sigma = 0.4$ can achieve the purpose for the forger. In this experiment, results show that the optimal noise strength ranges between $\sigma = 0.4$ and $\sigma = 0.8$. 
In the case of forger selecting the optimal noise strength, the performance of the proposed method is showed in the Fig. 15 NEROC (Nash equilibrium receiver operating characteristic) curves.

CONCLUSIONS:
A retaliation method has been proposed applied to anti-JPEG compression method and implemented based on noise level estimation by assuming that the forger adopts the anti-forensic method proposed in [6] and achieved the NEROC curves for different quality factors. Though anti-forensic technique can remove JPEG compression trace, it also introduces other detectable artifacts. In this paper, the experimental results show that proposed method is effective over a range of quality factors. Since the proposed method only uses one-dimensional feature set it is a time-saving process. In this paper, we limited our
analysis to only 250 images out of 1338 images from the Uncompressed Color Image Database (UCID) [12]. The proposed model would be suitable for analyzing similar interplays between forensics and anti-forensics.

References:


