CHAPTER 6

Comprehensive Image Index for Detection of Multiple Tampering Using 3-tupled Hash Function

Most of the existing hashing techniques extract one single feature of the image and develop single index hash function for image tampering detection. However, single feature tampering is very rare and any tampering operation results in multiple tampering. Proposed technique uses a 3-tupled Comprehensive Image Index (CII) which incorporates indices corresponding to structural tampering, brightness level tampering and contrast manipulations. CII enables us to detect existence or otherwise of the three tampering operations mentioned above simultaneously.

6.1 Comprehensive Image Index (CII)

Concept of this work was taken from paper titled “Universal Image Quality Index” (UIQI) by Zhou Wang and Alan C Bovik [118]. The authors defined a mathematical index to express the quality of an image and which is independent of viewing conditions and individual observer. This index has lower mathematical computational requirement and does not change with viewing conditions and observer and therefore it is termed as “universal”.

UIQI is defined as below:
If \( x = \{ x_i | i = 1, 2, ..., N \} \) and \( y = \{ y_i | i = 1, 2, ..., N \} \) be image under consideration
and reference image respectively, UIQI is defined as

\[ Q = \frac{\text{Cov}(X, Y)}{\sigma_x \sigma_y} \cdot \frac{2\bar{x}\bar{y}}{\bar{x}^2 + \bar{y}^2} \cdot \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2}, \]  

(6.1)

where,

\[ \bar{x} = \frac{1}{N} \sum_{i=1}^{N} x_i \]  

(6.2)

\[ \bar{y} = \frac{1}{N} \sum_{i=1}^{N} y_i \]  

(6.3)

\[ \sigma_x^2 = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})^2 \]  

(6.4)

\[ \sigma_y^2 = \frac{1}{N-1} \sum_{i=1}^{N} (y_i - \bar{y})^2 \]  

(6.5)

\[ \text{Cov}(X, Y) = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}). \]  

(6.6)

First component in the equation for \( Q \) is correlation coefficient and varies between −1 and +1. It has been shown in chapter 3 that correlation coefficient represents the structural content of the image. The second component is calculated using mean pixel value and hence represents the brightness level of the image. The third component is calculated using variance (i.e., variation from mean brightness value) and hence represents the contrast of the image. These three components together give almost the complete information about the image which can be relevant to image tampering detection. It has been discussed later in this chapter that how these three components are complete in describing the image. As an image can be primarily described by structure, brightness level and contrast, the three components of UIQI mentioned above can be used as representative parameters of the image.

An image can primarily be described by the ingredients (a) Structure, (b) Brightness level and (c) Contrast of the image. UIQI as defined above includes all these ingredients. Hence, UIQI can be used as representative which describes the image comprehensibly. We will relate correlation coefficient and structure of the image through a linear equation and call it structural index. If we represent above three ingredients through appropriate indices \( \eta_1, \eta_2 \) and \( \eta_3 \) respectively then Compre-
hensive Image Index (CII) can be represented as $\eta = (\eta_1, \eta_2, \eta_3)$. It is evident that $\eta_1$ represents Structural Index, $\eta_2$ represent Brightness Level Index and similarly, $\eta_3$ represents Contrast Index of the image.

### 6.1.1 Structural Index, $\eta_1$

Structural content of the image is represented through edges present in the image to a large extent [119]. Tampering in an image is basically alternation, removal or insertion of edge/edges fully or partially. It is found that edge are very appropriate and complete description of an image. $Y$ component of $YCrCb$ description of the image will be used to extract the edge features of the image as $Y$ only contains the structural information. An edge detector will be used to detect the edges and its output will be used to calculate image’s structural index.

In proposed technique, a gradient filter has been used. It measures rate of change of pixel values in $X$ and $Y$ directions which can be represented by $I_x$ and $I_y$ respectively. Thus

$$I_x = \frac{dI}{dx},$$  \hspace{1cm} (6.7)

and

$$I_y = \frac{dI}{dy}. $$ \hspace{1cm} (6.8)

The resultant rate of change of pixel values at any point $(x,y)$ is therefore given by

$$I_{xy} = \sqrt{(I_x^2 + I_y^2)}. $$ \hspace{1cm} (6.9)

As value of $I_{xy}$ represents features of an image, it will be used to generate hash value. Correlation coefficient $\rho$ between two images $A$ and $B$ is defined as

$$\rho = \frac{\text{Cov}(X,Y)}{\sigma_x \sigma_y}, $$ \hspace{1cm} (6.10)

where $X$ and $Y$ are random variables expressing pixel values in images $A$ and $B$ respectively.
It should be noted that $\rho$ varies between $-1$ to $+1$ and should be linearly transformed to get positive values of structural index $\eta_1$. It is done by using the following linear equation:

$$\eta_1 = \rho + 1. \quad (6.11)$$

### 6.1.2 Brightness Level Index, $\eta_2$

Many a times, change in the brightness level of image is carried out with bona fide intention of improving its visual quality. However, it may be changed to hide some information in the image or cover up a tampering. Such brightness change is generally global or locally global. An index to describe brightness level for purpose of tampering detection is denoted by $\eta_2$. It is defined with respect to same reference image as mentioned in case of $\eta_1$ as:

$$\eta_2 = \frac{2\bar{x}\bar{y}}{\bar{x}^2 + \bar{y}^2}, \quad (6.12)$$

where $\bar{x}$ and $\bar{y}$ are mean brightness level of image $A$ and $B$ respectively. It can be noted that $\eta_2$ varies between $0$ and $1$. It is also observed that for small change in the mean brightness level $\bar{x}$, index $\eta_2$ changes very marginally. But for higher value of change, there may be noticeable change in $\eta_2$.

### 6.1.3 Contrast Index, $\eta_3$

Contrast enhancement is a popular image processing technique which is used for bona fide improvement of contrast of the image. But in certain situations contrast enhancement may be done to hide some tampered portions in the image. Contrast enhancement is mathematically expressed as

$$P = CI^\gamma, \quad (6.13)$$

where, $I =$ Pixel value of original image, $P =$ Pixel value of altered image, $\gamma$ is the index which decides level of enhancement and $C$ is a constant.
Image Contrast Index \( \eta_3 \) gives range of maximum variation from mean brightness value and decides the contrast in the image. As expected it is expressed through standard deviation \( \sigma \). It is being measured with respect to same reference image as used in case of other two indices and is given by

\[
\eta_3 = \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2}
\] (6.14)

where \( \sigma_x \) and \( \sigma_y \) are standard deviation for images \( A \) and \( B \) respectively. It is seen that (a) \( \eta_3 \) varies between 0 and 1 and (b) for small change in \( \sigma_x \) there is very minimal change in \( \eta_3 \) for a given reference image with standard deviation \( \sigma_y \). However for major change in contrast (say for \( \gamma = 2 \) in eqn. (6.13)), there may be significant change in \( \eta_3 \).

Low value of change in mean brightness level has very minimal effect on \( \eta_2 \). Similarly, low value of change in contrast (\( \gamma = 1.2 \) say) does not have any significant bearing on \( \eta_2 \). This fact shows that for small change in mean brightness level and/or contrast change, which amount to content preserving manipulations, proposed method is robust. In cases where change in brightness level and/or contrast level of the image is significant, the corresponding changes in \( \eta_2 \) and \( \eta_3 \) will be large which amounts to malicious tampering. This also suggests that these indices should prompt a threshold level for \( \eta_2 \) and \( \eta_3 \) which will be categorized as content preserving manipulations and malicious tampering separately.

### 6.1.4 Definition of Comprehensive Image Index

Comprehensive Image Index, \( \eta \), is represented as

\[
\eta = (\eta_1, \eta_2, \eta_3),
\] (6.15)

where \( \eta_1 \) is structural index, \( \eta_2 \) is mean brightness index and \( \eta_3 \) is contrast index. These three indices define the image comprehensively. The justification for selection of these parameters to describe the features of the image is discussed below.
An image can be described using (a) shape descriptors (b) texture descriptors and (c) colour descriptors. In present case, we are only concerned with structural tampering detection therefore only the gray scale image will be considered. Hence colour descriptor is ignored and only gray scale pixel values will be taken into account. Shape of an image is described by the edges present in it. Exterior as well as interior shape of the image can be effectively picked up through its edges. This is done using a gradient detector and its output generates the hash value representing the shape descriptors.

The textured descriptors are contained in pixel values of the image. This information can be described using contrast and brightness values of the pixels. Thus, hash function containing information about edges, contrast and brightness value gives complete description of the image. Therefore selection of comprehensive image index incorporating above three factors has been chosen for purpose of composite structural tampering detection.

For structural tampering detection, Edge Index $\eta_1$ is suitable and $\eta_2$ and $\eta_3$ are not very significant. However, if a structural tampering is carried out in conjunction with contrast and brightness manipulations to hide it, all the three indices $\eta_1$, $\eta_2$, and $\eta_3$ become relevant.

The three features represented through $\eta_1$, $\eta_2$, and $\eta_3$ give almost complete description of image. However, the three features are not orthogonal. But orthogonality is not really so much a required property for tampering detection. Interdependence of three variables to some extent does not, in any way, limit our capacity to draw conclusion about type and amount of tampering an image.

In view of the above, a more generalized technique is proposed which will generate a 3-tupled hash value each representing three indices $\eta_1$, $\eta_2$ and $\eta_3$ together. It will be represented as $(\eta_1, \eta_2, \eta_3)$. In order to detect the tampered area in an image, the image will be suitably divided into number of blocks. 3-tupled
hash value corresponding to each block, i.e., \((h_1, h_2, h_3)_{ij}\) where \((i, j)\) represent the location of the block in the image, will be found out. These hash values when arranged at their respective block locations, will constitute the hash matrix \(H\) of the image under consideration. When rows of the matrix are arranged in a single row, they form a hash vector which is a comprehensive representation of the image. It is converted into a binary string and may be provided to the receiver either along with the image or separately which can be used to check the authenticity of the image.

After computation of hash matrices, a distance function \(D\) is defined to compare the distance between the original and tampered images. Value of \(D\) tells us if the tampering in the image has taken place or not. If the distance is zero then there is no tampering in the image. If distance is non-zero but very small then tampering is of content preserving type but if the distance is substantial then tampering belongs to malicious tampering category. In proposed method distance function chosen is Euclidean distance and this is computed by finding out the absolute difference between hash matrices of original and tampered image.

### 6.2 Robustness of CII against content preserving manipulation (CPM)

When talking about robustness against CPM, it is always desirable to quantify the threshold level up to which a particular technique is robust. The efficiency of technique lies in ignoring content preserving manipulation at the same time detecting even the minutest tampering operations. In the proposed method, 3-tupled hash value generated for the image will include indices for brightness level change and contrast variation along with structural index. This will give an exact quantification of the manipulation with respect to three different parameters. For ensuring robustness against brightness and contrast change parameters \(\eta_2\) and \(\eta_3\) are so defined that small changes in brightness and contrast respectively do not alter their values much. Chosen formulation for \(\eta_2\) and \(\eta_3\) also ensures that effect of
changes in $\eta_2$ and $\eta_3$ on $\eta_1$ is very minimal. Hence detection of structural tampering through CII is robust against CPMs.

From hash matrix $H$, three hash matrices each corresponding to indices $\eta_1$, $\eta_2$ and $\eta_3$ respectively, can be generated. Set of these three matrices are computed for original image and the suspected image for tampering detection. Absolute difference of respective matrices $|H_o - H_t|$ corresponding to the three types of tampering operations, i.e., structural tampering, change in brightness level and change in contrast level, is then computed to find out the amount and area of tampering.

6.3 Proposed algorithm for multiple tampering detection through CII: 3-tupled hash vector representation

Structural information in an image is described by the edges in it. Therefore, any tampering in the structure of the image will be affecting the position and amount of the edges. Here, an edge detector, as described in eqns. (6.7), (6.8) and (6.9) which is primarily a gradient filter, will be used to extract the edges and develop an index for the same. Normally, a colour image is described through YCrCb representation but only $Y$ component contains the structural information and will be used for our purpose. An $M \times M$ image will be used in the proposed method for image tampering detection. The algorithm comprises of following steps:

1. $M \times M$ image is divided into blocks of size $q \times q$. Here, $q$ is chosen such that $M$ is an integral multiple of $q$.

2. Edge detector is applied to the blocks to extract edges in it. It is done by using a derivative filter and actual pixel value gradient is computed for all pixels in the image. The output of edge detector is a matrix of $q \times q$ size and it is used to find out correlation coefficient of the block with a reference image of the same size.
3. Value of correlation coefficient $\rho$ varies between $-1$ to $+1$ and it is suitably scaled using a linear equation to avoid negative values. The value for the block so calculated, gives its hash value.

4. These hash values are arranged at their respective block location to give hash matrix for the image corresponding to structural index $\eta_1$.

5. Following the block generation method mentioned above, hash matrices corresponding to brightness level and contrast index are also found out. The reference image used in all the three cases is same.

6. Above process gives a hash value $[h_{ij}(\eta_1), h_{ij}(\eta_2), h_{ij}(\eta_3)]$ representing hash values for all the three indices for the block $(i, j)$.

7. Steps 1 to 8 are carried out for original and tampered image [116].

Algorithm described in sub-section 2.2 along with eqns. (6.10, 6.11, 6.12, 6.14) are used to find 3-tupled CII for each block in the image. 8-neighbourhood sum is used to find corresponding hash value given by the eqn. (6.16). This process is carried out for original and tampered images.

$$h_{ij} = \eta_{i-1,j} + \eta_{i,j} + \eta_{i+1,j} + \eta_{i,j+1} + \eta_{i-1,j+1} + \eta_{i+1,j+1} + \eta_{i-1,j-1} + \eta_{i+1,j-1},$$

(6.16)

where $i, j = 1, 2, 3, ..., t$.

$$\begin{pmatrix}
h_{11}(\eta_1), h_{11}(\eta_2), h_{11}(\eta_3) & h_{12}(\eta_1), h_{12}(\eta_2), h_{12}(\eta_3) & \ldots & h_{1t}(\eta_1), h_{1t}(\eta_2), h_{1t}(\eta_3)
h_{21}(\eta_1), h_{21}(\eta_2), h_{21}(\eta_3) & h_{22}(\eta_1), h_{22}(\eta_2), h_{22}(\eta_3) & \ldots & h_{2t}(\eta_1), h_{2t}(\eta_2), h_{2t}(\eta_3)
\vdots & \vdots & \ddots & \vdots
\vdots & \vdots & & \vdots
h_{t1}(\eta_1), h_{t1}(\eta_2), h_{t1}(\eta_3) & h_{t2}(\eta_1), h_{t2}(\eta_2), h_{t2}(\eta_3) & \ldots & h_{tt}(\eta_1), h_{tt}(\eta_2), h_{tt}(\eta_3)
\end{pmatrix},$$

Experiment was carried out on a set of 100 images. Indices $\eta_1$, $\eta_2$ and $\eta_3$ were obtained for original as well as tampered images. The graph in fig. (6.3) shows that $\eta_1$ responds to structural tampering. It can be observed that structural index for original and tampered images, i.e., $\eta_1(o)$ and $\eta_1(t)$ are separated sufficiently.
Figure 6.1: The central block is at $i^{th}$ row and $j^{th}$ column of the blocks of the image. The four neighboring blocks are obtained shifting by half block width to the left ($i,j-1$), right ($i,j+1$), up ($i-1,j$), down ($i+1,j$) and four corner blocks at ($i-1,j-1$), ($i+1,j+1$), ($i-1,j+1$) and ($i+1,j-1$).

and can be distinguished easily. It implies that detection method is sensitive in locating the tampering in an image.

The other two indices, i.e., brightness level index and contrast index are carefully defined so that they respond to small variations very marginally. Small change in brightness level of image, changes $\eta_2$ value insignificantly. Similarly, small change in contrast ($\gamma = 1.2, 0.9$ in gamma correction equation) does not alter $\eta_3$ much and can be easily ignored. Nevertheless, this small change in $\eta_2$ and $\eta_3$ is listed in the hash value and consequently in hash matrix. For higher value of change in brightness level and contrast, $\eta_2$ and $\eta_3$ change noticeably while doing the tampering detection. Absolute difference between hash matrices of original and tampered image corresponding to three indices $\eta_1$, $\eta_2$ and $\eta_3$, is found out. Let the difference be given by distance function $D$. Then,

$$D = |H_t - H_o|. \quad (6.17)$$

In component form
\begin{align*}
  D_{(1)} &= |H_t(\eta_1) - H_o(\eta_1)|, \\
  D_{(2)} &= |H_t(\eta_2) - H_o(\eta_2)|, \\
  D_{(3)} &= |H_t(\eta_3) - H_o(\eta_3)|,
\end{align*}

where $D_{(1)}$ is absolute difference between hash matrices of tampered and original image corresponding to structural index $\eta_1$. Similarly, $D_{(2)}$ and $D_{(3)}$ are absolute differences corresponding to $\eta_2$ and $\eta_3$.

Three components hash calculations serve following purposes:

1. It helps in deciding if the tampering is structural in nature or occurred due to brightness level change and/or contrast change.

2. Low values of $D_{(2)}$ and $D_{(3)}$ amount to content preserving manipulations and we can ignore them by setting a threshold $D_T$.

3. If value of $D_{(2)}$ and $D_{(3)}$ is large then we can conclude that tampering done through brightness level change or contrast variation, has been done with malicious intention. It is interesting to note that if $D_{(1)}$ and $D_{(3)}$ both are large then contrast change could have been carried out to cover structural tampering. Similarly conclusions can be drawn with other combinations of $D_{(1)}$, $D_{(2)}$, and $D_{(3)}$. If $D_{(1)}$ and $D_{(2)}$ both are large, it could mean that structural tampering has been done followed by brightness change to cover it. If only $D_{(2)}$, and $D_{(3)}$ are large with no change in $D_{(1)}$, it may mean that purpose of tampering is to improve the visual quality of the image without any malicious intention.

### 6.4 Independence of indices $\eta_1$, $\eta_2$ and $\eta_3$

Image processing operations associated with $\eta_1$, $\eta_2$ and $\eta_3$ are not independent. For example, structural tampering affects the pixel values which change mean brightness level resulting into change in $\eta_2$. On the other hand, contrast enhance-
ment changes the pixel values in accordance with $P = CI^\gamma$, resulting into change in $\eta_1$ and $\eta_3$. Similarly, drastic change in mean brightness level may suppress relatively weak edges and thus affecting $\eta_1$. It will suffice to say that $\eta_1$, $\eta_2$ and $\eta_3$ are not independent and affect each other in general. However, in our analysis, final combined effect of various tampering operations is taken into account to calculate $\eta_1$, $\eta_2$ and $\eta_3$.

To demonstrate the performance of proposed algorithm in conjunction with an edge detector, a set of 100 images of $40 \times 40$ is taken. For calculating $\eta_1$, the edges in the image are extracted using gradient edge detector. The correlation coefficient $\rho$ of output matrix with reference image is found out which in turn gives $\eta_1$. Indices $\eta_2$ and $\eta_3$ are calculated before application of edge detector using formulae shown in eqns. (6.12) and (6.14) respectively. Above process is repeated for same set of images but after tampering them. Index $\eta_1$ is plotted for different amount of structural tampering which is shown in fig. (6.3). Similarly, $\eta_2$ is plotted for different values of brightness level and $\eta_3$ is plotted for different values of gamma correction. It is observed that for low level of these tampering operations, $\eta_2$ and $\eta_3$ change very marginally. Also minor changes in brightness level and contrast does not have any noticeable impact on $\eta_1$. However, as the amount of tampering increases, the respective indices move away significantly from those of the original image. This observation demonstrates the robustness of proposed algorithm as well as the sensitivity of detection for all three types of tampering operations.

Extraction of edges using gradient filter ignores noise as it is basically low frequency signal. The output of gradient filter is zero to these low frequency components. This quality of gradient filter makes it robust against low frequency brightness and contrast manipulations.
6.5 Similarity Value Vector

Having done the tampering detection, it is desirable to develop an index to quantify amount of tampering in an image. For this, Similarity Value Vector will be defined as follows. Rows of $t \times t$ hash matrix are arranged one by one in a single row to generate hash vector $H$ of the image. For two images $A$ and $B$ with their respective hash vectors $H^a$ and $H^b$, a ratio $R_i$ is defined as

$$R_i = \frac{\exp\left[\min\left(H^a_i, H^b_i\right)\right]}{\exp\left[\max\left(H^a_i, H^b_i\right)\right]},$$

(6.21)

where $i = 1, 2, 3, \ldots, t^2$. $R_i$ assumes a value 1 if $i$th component of two hash vectors $H^a_i$ and $H^b_i$ have same value implying that there is no tampering in that block. Similarity Value for images $A$ and $B$ is defined as

$$S\left(H^a, H^b\right) = \prod_{R_i \in R_S} \frac{R_i}{\prod_{R_i \in R_L} R_i},$$

(6.22)

Numerator in eqn. (6.22) is product of $m$ minimum most $R_i$ ratios, denominator being product of $m$ maximum most $R_i$ ratios. For accurate calculation of $S$, number $m$ should be more than or equal to the number of tampered blocks. An iterative method can be used to arrive at an appropriate value of $m$. It is observed that $S$ varies between 1 and 0. If two images are same, their $S$ value is 1 and it moves away towards 0 when amount of tampering is increased. As there are three types of tampering operations represented through $\eta_1$, $\eta_2$ and $\eta_3$, there will be 3-tupled Similarity Value Vector $(S_1, S_2, S_3)$ for a pair of two images.

By virtue of having a 3-tupled Similarity Value Vector, proposed technique becomes very comprehensive and is superior to many other existing techniques which normally work around single parameter detection. The technique not only ignores content preserving manipulations easily but also responds adequately to any manipulation crossing into malicious tampering zone by detecting and quantifying it properly through Similarity Value Vector.
6.6 Experiments and Results

A set of 100 images was taken and proposed algorithm was used to calculate indices $\eta_1$, $\eta_2$ and $\eta_3$. Hash matrices $H(\eta_1)$, $H(\eta_2)$ and $H(\eta_3)$ were calculated for original and tampered images. Absolute distances $|H_t(\eta_1) - H_o(\eta_1)|$, $|H_t(\eta_2) - H_o(\eta_2)|$ and $|H_t(\eta_3) - H_o(\eta_3)|$ were computed to detect all three types of tampering separately as shown in Table (6.2). Robustness and sensitivity of the technique was tested for a set of 20 images as shown in fig. (6.3).

Robustness was tested for set of 30 images. For detection of brightness level change, experiment was conducted by altering pixel values by $+20$, $-20$, $+90$ and its effect on $\eta_2$ was observed. It was found that for small brightness changes, there is almost no change in $\eta_2$ but when brightness level change becomes $+90$, $\eta_2$ changes significantly as shown in fig. (6.4). Effect of change in contrast index $\gamma$ on $\eta_3$ was studied by changing $\gamma$ values to 0.2, 1.5 and 5.0. Again for small change in...
<table>
<thead>
<tr>
<th>No.</th>
<th>Original Image</th>
<th>Tampered Image</th>
<th>$S_1$ value</th>
<th>$S_2$ value</th>
<th>$S_3$ value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image1" alt="Original Image" /> <img src="image2" alt="Tampered Image" /></td>
<td><img src="image3" alt="Tampered Image" /></td>
<td>0.31445</td>
<td>0.09140</td>
<td>0.06012</td>
</tr>
<tr>
<td>2</td>
<td><img src="image4" alt="Original Image" /> <img src="image5" alt="Tampered Image" /></td>
<td><img src="image6" alt="Tampered Image" /></td>
<td>0.33450</td>
<td>0.07108</td>
<td>0.05912</td>
</tr>
<tr>
<td>3</td>
<td><img src="image7" alt="Original Image" /> <img src="image8" alt="Tampered Image" /></td>
<td><img src="image9" alt="Tampered Image" /></td>
<td>0.43453</td>
<td>0.06049</td>
<td>0.04828</td>
</tr>
</tbody>
</table>

Table 6.1: Similarity Value Vectors ($S_1$, $S_2$, $S_3$) have been shown for three images. ($S_1$, $S_2$, $S_3$) speaks about similarity value for structural, brightness level and contrast tampering in the image simultaneously.

Figure 6.3: Average Structural indices for 20 images have been plotted in this graph for the original image and tampered image showing the effect of structural tampering on $\eta_1$. 

85
\( \gamma \), there was no significant change in \( \eta_3 \). However, change in \( \eta_3 \) became noticeable when \( \gamma \) value was changed drastically. These are shown in fig. (6.5).

![Graph showing brightness level indices](image1.png)

Figure 6.4: Brightness Level indices for 20 images have been plotted in this graph for the original image, with change in brightness level by +20, +50, and +90 for showing effect of change in brightness level on \( \eta_2 \).

![Graph showing contrast indices](image2.png)

Figure 6.5: Contrast indices for 20 images have been plotted in this graph for the original image, with \( \gamma \) changed to 1.5, 0.2 and 5.0 for showing effect of \( \gamma \) change on \( \eta_3 \).

### 6.7 Conclusion

The aim of proposed content based hashing technique was to offer a comprehensive method to detect multiple image tampering. This was done through generation of 3-tupled hash functions which incorporates indices for structural, brightness level and contrast tampering. For the first time, tampering detection was carried out around three different parameters and it worked satisfactorily. Issue
of robustness and sensitivity was dealt with in quantitative terms. Ingress of content preserving manipulation into malicious tampering zone in case of change in brightness/contrast level drastically, was handled through a 3-tupled hash vectors. This concept makes the proposed technique comprehensive which can detect multiple tampering operations simultaneously.

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Image</th>
<th>Tampered Image</th>
<th>Localization of tampering using $\eta_1$</th>
<th>Localization of tampering using $\eta_2$</th>
<th>Localization of tampering using $\eta_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
</tr>
<tr>
<td>2</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
</tr>
<tr>
<td>3</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
</tr>
</tbody>
</table>

Table 6.2: Simultaneous detection of structural, brightness level and contrast tampering has been shown for three images through generation of 3-tupled hash matrix.