DIGITAL DOCTORED VIDEO FORGERY
DETECTION TECHNIQUES

Govindraj Chittapur, Basaveshwar Engineering College, Bagalkot;  S. Murali, Maharaja College Of Engineering Mysore;

Abstract

We are proposing forensic techniques that are capable of detecting traces of tampering in digital Video without specialized hardware. These techniques operate under The assumption that video contain naturally occurring properties which are disturbed by Tampering, and which can be quantified, measured, and used to expose video fakes. In this context we are proposing techniques used in copy-paste and copy move interlaced video frames using statistical mean comparrison. These techniques provide a valuable forensic techniques for authenticating digital video.

Related Work on Video Forgery

Currently, most acquisition and manipulation tools use the JPEG and MPEG standard for image and video compression. As a result, one of the standard approaches is to use the blocking fingerprints introduced by MPEG compression, as reliable indicators of possible image tampering. Not only do these inconsistencies help determine possible forgery, they can also be used to detect the abnormalities due to addition or removal of frames in the video sequence, modified regions or masked regions in the frames. Many passive schemes have been developed for tampered region detection of in-painting JPEG images [4], Histogram equalization based contrast enhancement techniques [5], Blue screen special effects in videos [6], Markov model on motion residue video [7], Ballistics motion [8], Non-sampled contourlet Transformation and Gradients information [9], Advanced statistical and adaptive threshold [10], Correlation noise residue [11], Double MPEG compression [12], Detection duplication [13], Detecting double quantization [14], Photo image forgery techniques [15,17] Luminance Level Techniques [16], and, Anti-forensic techniques for frame add/delete in mpeg video[18]. Though these algorithms show good results they are complicated and take more time to compute. There is need to overcome these two drawbacks.
Methodology and Implementation

When a video sequence is captured, there is typically a great deal of redundancy between the successive frames of video. The MPEG video compression technique exploits this redundancy by predicting certain frames in the video sequence from others, then by encoding the residual difference between the predicted frame and the actual frame. Because the predicted difference can be compressed at a higher rate than a frame in its entirety, this leads to a more efficient compression scheme. Performing compression in this manner has its drawbacks, however, because error introduced from one frame will propagate to all frames predicted from it. To prevent error propagation, the video sequence is divided into segments, where each segment is referred to as a group of pictures (gp). Frame prediction is performed within each segment, but never across segments, thus preventing decoding errors in one frame from spreading throughout video sequence. Within each group of pictures, frames are divided into three types: intra-frames (I-frames), predicted-frames (P-frames), and bidirectional-frames (B-frames). Each gp begins with an I-frame, followed by a number of P-frames and B-frames. No prediction is performed when encoding I-frames; therefore each I-frame is encoded and decoded independently. During encoding, each I-frame is compressed through a loss process similar to JPEG compression. P-frames are predicatively encoded through a process known as motion estimation.

A predicted version of the current P-frame is obtained by first segmenting the frame into 16X16 pixel blocks known as macro blocks, then searching the previous P or I-frame, known as the anchor frame, for the macro block that best matches each macro block in the current P-frame. The locations of these macro blocks in the anchor frame are stored, along with how far each macro block must be displaced to create the predicted frame. These displacements are referred to as motion vectors. The residual error between the predicted frame and the current frame, known as the prediction error, is then compressed using the same JPEG like process that I-frames undergo.

Mean Frame Comparison Technique

In the given input video, read the content of pictures in terms of input video frames as well as read the content of source of original video frames where in Mean compare operation is performed on every frame of the video. The Mean comparison is performed in frame-by-frame fashion i.e. each and every pixel undergoes Comparison with pixel-by-pixel comparison and extracting the mean of each frame in frame set. On comparison of frames, if the mean value of frames in frame set value is equal then that area is masked in black. If there is any difference in the frame value between these groups of pictures then that area/region can be identified to be tampered. The result viewed will show a black masked area where there is no difference between these group of picture frames i.e. no difference between the pixel value of original and forged frames in videos. And the area where there is pixel frame difference will be highlighted which was a tampered area is been suspected; mathematical model for Mean Comparison is given as:

\[ f(z) = f(x) - f(y) \]

(1)

Where \( f(z) \) is the suspected and identified forged region of picture frames in digital videos where \( f(x) \) and \( f(y) \) are original and forged feature set videos.

Audio Forgery Detection

Video is made of Moving frames, each attached with an audio. So if changes in audio are made, it is also called forgery. We have implemented a methodology which detects audio forgery in a video. The methodology works as follows. Firstly, the video which is to checked whether it is forged or not is loaded. Then, audio is extracted from the video using some software’s and later it converted into wav file. Now the audio is segmented. These segments Ea features are extracted and written in a text file. Now these features are compared with the original segments. And forged segments are found out and classified. Now join only the forged segments and play it. Finally, only the forged audio is found.

Mathematically represented as,

\[ \text{Assume } F(x_1) \text{ as original and } F(x_2) \text{ as Forged.} \]
\[ F(x_1) = (F(a_1) + F(a_2) + \ldots + F(a_n)) \]
\[ F(x_2) = (F(a_1) + F(a_2) + \ldots + F(a_n)) \]

(2)

(3)

Compare the segments and extract only the forged parts and join them.

\[ F(y) = (F(a_1) + F(a_{n+1}) + \ldots + F(a_n)) \]

(4)

Here the Equation (4) shows the region of forged audio part of tested video i.e. \( F(y) \) is the forged part.

Results and Discussion

Videos have been captured from Sony digital camera, and algorithm implementation has been done in Mat Lab. Also, 100 different videos from various galleries including categories of indoor and outdoor scenes were used for testing. Forgery detection was quite successful in all categories of videos.
From the Figure (1), (2) and (3) explains about an example of Original Frames from tested video later on which is being forged with the help of video editing software with changing Contrast and some part of the frames are changed the content of frame information by applying skillful set where normal person won't be identified with his eyes as forgery one. We testes those videos with perception based and succeeded. With references of Figure (3) it explains the mean compression algorithm result and identified the forgery region in given forged input video as test image. Figure (4) explains the result of average mean of tested original frames (i) and same result can be extracted for forgery frames (ii), we succeed by considering mean comparison between tested original and forged videos.(iii) Explains audio forged region detection with the help of statistical mean frame with extracted feature detection method. Even though we computed for success Rate and Precision Rate for tested video Gallery.

The precision and recall rates (Equations (2) and (3)), have been computed based on the number of correctly detected tampered parts in forged videos, in an order to further evaluated the efficiency and robustness. The precision rate is defined as the ration of correctly detected parts to the sum of correctly detected parts plus false positive. False positive are those regions in the image, which are actually not tampered parts, but have detected by the algorithm as tampered parts.
The Recall rate is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false negatives. False negatives are those regions in the image, which are actually tampered parts, but have been not detected by the algorithm.

\[
\text{Recall Rate} = \frac{\text{Correctly detected parts}}{\text{Correctly detected parts} + \text{False Negatives}} \times 100\% \quad (3)
\]

With the help of equation (2) and (3) we succeeded to compute precision rate and recall rate of Mean comparison Algorithm.

Table 1 explains the predicitng success rate and precision rate of forgery frames applicable in video forgery set.

<table>
<thead>
<tr>
<th>TOOLS USED FOR FRAME SET FORGERY</th>
<th>NO OF FRAMES IN FORGERY TESTED VIDEO</th>
<th>PRECISION RATE</th>
<th>RECALL RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USING PAINT</td>
<td>50</td>
<td>92.2</td>
<td>92.6</td>
</tr>
<tr>
<td>USING PHOTO SHOP</td>
<td>50</td>
<td>45.4</td>
<td>37.7</td>
</tr>
<tr>
<td>HETROGINIOUS TOOLS</td>
<td>50</td>
<td>68.8</td>
<td>65.2</td>
</tr>
</tbody>
</table>

We are getting good result in frames forgery done with paint and heterogeneous image frame editing software’s by applying various frame enhancement and modification techniques and lesser in advance frame editing techniques supported by photo shop tool.

Conclusion

This Paper outlined the methodology used in detecting digital video tampering from images with known and unknown origin. While it is difficult to predict exactly how a malicious person will forge an video, a wide range of techniques have been presented to account for tamper methods. The detection system proposed mean frame comparison technique includes methods based on Mean and pixel comparison of each frames in video data frame set used with unknown image source. An experiment testing this method has been set-up that will help in determining the accuracy and correctness of the proposed tamper detection techniques, as well as when each fails. It has been conjectured that these methods will help in detecting various types of image forgeries, but one has to acknowledge that no “silver-bullet” exists to account for every type of forgery imaginable. To wrap up testing, an independent experiment is presented to help analyze the correctness of this system of techniques at accurately identifying blind frame set in videos as authentic or forged.

Precision rate and recall rate are based on subjective to the forger skills set; it is completely dependent on how forger can viewed and modifies frames in videos. Predication of such skill is challenging for every digital forensic investigator and technocrats.

Reference


Conference on Digital signal processing
doi: 10.1109/ICDSP.2011.6004875


