Summary and Conclusion

5. SUMMARY AND CONCLUSION

Advancements in low-cost digital cameras and sophisticated image editing software have increased the amount of images being manipulated or modified either in an intentional or unintentional fashion. Image forgery, is a field that is gaining more attention, especially in the past few years, because more and more businesses and organization are accepting digital image as official and legal document. Image forgery is much widespread in applied like tabloid magazine, fashion Industry, scientific journals, court rooms, main media outlet and photo hoaxes received in email.

Digital image forgery detection techniques are classified into active and passive approach. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image. Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance. There are three techniques widely used to manipulate digital images.

1) Tampering–Tampering is manipulation of an image to achieve a specific result
2) Splicing (Compositing) - A common form of photographic manipulation in which the digital splicing of two or more images into a single composite
3) Cloning (Copy-Move) is creating duplicate of an image onto another image

This study focuses on passive techniques to detect the most splice or composite type of tampering.

This research work uses the camera properties to detect tampered images and is working under the fact that different cameras have dissimilar properties and any tampering operation will reflect in a change in these features.

The proposed automatic algorithm performs tamper detection in three steps, feature selection, feature extraction and one-class classification. The system extracts four types of features to form feature database.

(i) color features (mean, correlation, centroid and energy ratio)
(ii) image quality features (Mean Square Error, Mean Absolute Error, Corrected Infinite Norm)
(iii) Wavelet features (Mean, Variance, Skewness, Kurtosis, linear prediction error of coefficient amplitude)
(iv) Bicoherance features (mean bicoherance amplitude, bicoherence phase entropy).

To improve the detection process, dimensionality reduction is performed on the features extracted. For this purpose, Fisher classifier algorithm is used. Careful analysis revealed that when the dimension of the feature space exceeds 87, the accuracy improvement converges. Therefore, only the first 87 features are selected for detection.

The third stage, uses two one-class classification algorithms to detect tampered and genuine images. One class classifiers are designed to describe only one class of target object (tamper) and discriminate them from all other possible patterns. The two classifiers used for this purpose are Radial Basis Function Neural Network and Support Vector Machine. These two classifiers were selected due to its popularity in pattern recognition and classification.

The tamper detection process is performed in two steps, training and testing. During training, the training images are segmented into 128 x 128 blocks and the features are extracted for each block. These features are used

for training the classifiers. During testing, the same features are extracted and the trained classifier is used to detect the presence or absence of manipulation.

The CASIA TIDE dataset was used during the evaluation steps of the research work. Three different cameras, Canon, Nikon and Sony, were selected and the splice tampering was performed using three main variations. The first is to splice images

(i) using different camera combinations
(ii) using different image transformations
(iii) using different shape methods

Nine different camera combinations, namely, Canon-Canon, Canon-Nikon, Canon-Sony, Nikon-Nikon, Nikon-Canon, Nikon-Sony, Sony-Sony, Sony-Canon and Sony- Nikon were formed. During photomontage creation, four different types of transformations (Resize, Deform, Rotate, Do Nothing) were used with four different shapes (Circle, Rectangle, Triangle and Arbitrary). Thus, a total of 1725 (800 authentic and 925 spliced color images) were used during experimentation.

On evaluating the system in terms of accuracy, the following findings could be observed.

(i) Maximum efficiency was produced by SVM one-class classifier with both tamper and authentic image identification
(ii) The system is efficient in identifying tampered images formed using rectangle shape followed by triangle. Poor performance was obtained when arbitrary shape was used during splice creation.
(iii) Considering transformations, best performance was achieved when no transformation was used during the creation of tampered images.
(iv) The system found rotate transformation tampering easily followed by resizing modifications.

(v) Further, the system was efficient in identifying tampered images correctly when both the slices were taken from the same camera.

Thus, from various results, it can be concluded that the four features, color, image quality, wavelet and bicoherance, when combined with SVM one class classifier, is efficient in identifying tampered and untampered images and can be used in important applications like legal, media and World Wide Web.

FUTURE RESEARCH DIRECTIONS

The following can be considered to improve the proposed tamper detection system.

1. The present study deals with camera photograph images only. In future scanned photograph can be considered which would require first a classification algorithm to identify camera and scanned images followed by tamper detection algorithm.
2. Other type of tampering like removal, replacement, replication of objects can also be probed.