Abstract

This paper presents various Data Hiding techniques of video in compressed domain. Data is embedded into digital media for the purpose of identification, annotation, copyright protection and tampering detection. The identification purpose mainly falls into the area of cloud computing-making sure that the sender is the one intended; annotation refers to the property of tagging or giving captions to the video; copyright protection, which is used to prevent the recreation of the video; tampering detection is the method in which the receiver checks whether the video is tampered or disturbed during the transmission by a third party. Several factors affect the data hiding process - the quantity of data to be hidden, whether the embedding technique can handle large payloads without affecting the quality of the video, embedding in a lossy compression environment and the extent to which the data hidden is subject to modification or removal by a third party. This paper discusses the various data hiding techniques of video in the compressed environment and compares the techniques based on the quantities mentioned above. Furthermore they are analyzed in terms of their method, robustness and capacity. A comparison graph is plotted based on the efficiency analysis of the data hiding techniques and conclusions
are drawn based on the analysis.

References


Index Terms

Computer Science Security

Keywords

Data hiding, Steganalysis, Video compression, Video encryption, Watermarking