Abstract

Steganography is the science of hiding data by embedding it in cover files without altering it. The cover media may be text, image, voice or video streams in a digitized format. Steganography is used to prevent unauthorized users from becoming aware of the very existence of a message, let alone what it contains. These new techniques makes hidden message indistinguishable from the white noise. Even after suspicion of the presence of message, there is no proof of its existence. There are various methods to implement this, based on the cover file used. Image steganography is when an image is used as a cover file. Similarly, if video is used as the cover file, it is known as video steganography and similarly, text and audio techniques. The amount of data that can be effectively hidden in a given medium is restricted by the size of the medium itself. The fewer the constraints that exist on the integrity of the medium, the more potential it has for hiding data. This paper presents a survey on video steganography and its various techniques along with the applications, limitations and comparison.
References


7. Savkar Tushar, Dhanak Prasad, Jadhav Gaurav, Salunke Sachin, Application Of Data Hiding In Audio-video Using Anti Forensics Technique For Authentication And Data , National Conf. on Recent Innovations in Science Engineering & Technology(NCRISET), 16th Nov.-2014, Pune, India,


27. Arun Kejariwal, Paolo D’alberto Alexandru Nicolau Constantine, A Geometric Approach For Partitioning N-dimensional Non-rectangular Iteration Spaces, D. Polychronopoulos Center For Embedded Computer Systems University Of California At Irvine Irvine, Ca 92697, 2005


Index Terms

Computer Science  Security

Keywords

Discrete wavelet transform, Distortion technique, Hash-LSB Embedding payload, Network steganography, Steganography, Stego-Video.