Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN : 2455-7528

REVIEW PAPER ON IMPROVING OVER NOVEL FRAMWORK FOR SECURE THE LIVE VIDEO STREAMING OVER P2P NETWORK

Rahul Soni[1], Gajanand Sharma[2]

1Research Scholar, SGU,rahulsonikekri@gmail.com

2Assistant Professor, SGVU,gajanand.sharma@mygyanvihar.com

Abstract: The key problem that arises due Video editing is widely used not only in professional movie making, but also in many other areas such as home videos, educational videos, and marketing videos. With the popularization of video cameras, even more potential applications are developing. Even relatively straightforward applications may wish to edit the video to process it in some other way (for example, to re-render it as a cartoon). In general, such tasks need an understanding of the structure of the video content, as a basis both for editing and for more advanced and complex video processing operations. Forensic tools and forensic experts play the key role to examine the authenticity of video evidences. While examination, if it has been found as authentic (*i.e.* non-tampered or actual), experts generally embed watermark into authenticated videos such that whenever required its authenticity can be re-examined by retrieving the watermark.

The proposed paper aims to find out the effectiveness of new algorithm, comparison, suggestions, and a competitive approach to find out the best solution for improving the live video streaming . secure the high definition compressed structure video transmission over P2P Network Global performance metrics are developed and used to evaluate performance of Secure Video Transmission using tools like Mat lab, ns-2 or omnet++ and The analysis of designed model for secure the high definition structure compressed structure video transmission over P2P Network.

KEYWORDS: Analysis, p2p network, omnet++ , matlab ,Efficiency.

I. INTRODUCTION

Since, from the beginning of human civilization, visual information is the most often used medium to express knowledge, thoughts, evidences, etc. and represents one of the effective means for communication. It has a capability to convey the broader spectrum of information by Visual information because of its ease in acquisition, distribution, and storage. In the modern age, images and videos have become the main information carriers to disseminate knowledge and establish the bridge among several sources.

Video editing is widely used not only in professional movie making, but also in many other areas such as home videos, educational videos, and marketing videos. With the popularization of video cameras, even more potential applications are developing. Even relatively straightforward applications may wish to edit the video to process it in some other way (for example, to re-render it as a cartoon). In general, such tasks need an understanding of the structure of the video content, as a basis both for editing and for more advanced and complex video processing operations. The need to treat the whole video in a coherent manner has been emphasized in several previous publications. For example, a video-tooning approach pays particular attention to providing coherent segmentation in the space-time space to re-render the video as a cartoon animation. A recent paper on motion layer-based object removal in videos also proposed a motion-based video segmentation method as a preparatory step to object removal.

Developments in visual (video) technologies *viz.* compression, transmission, storage, retrieval, and video-conferencing have helped in many ways to the society. In the socioeconomic knowledge and scientific development, the images and videos available at various video sharing and social networking websites (*viz.* YouTube, Facebook, *etc.*) are playing a significant role [3]. Besides this, other applications like entertainment industry, video surveillance, legal evidence, political videos, video tutorials, advertisements, *etc.* signify their unprecedented role in today's context.

Forensic tools and experts play a key role to examine the authenticity of videos by detecting traces (if any) of tampering and detection of tampering with videos have posed challenges before the scientific community. Here, success or failure of tools and experts depends on how intelligently tampering has been carried out by the forger.

Further, success or failure of forger depends on how intelligently fake videos have been made to deceive forensic tools and the expert eye. In literature, there are many counter forensic (or anti-forensic) schemes available which facilitate forger to create fake videos to deceive forensic tools.

Video data has become more popular with the advancement of digital cameras and networking technologies with high speed bandwidths. As a result many systems make use of video data and rely on the accuracy of such data. On the other hand, an inevitable adverse effect of this critical nature of video data is video forgery. There are many software available all over the internet that facilitates video editing. With these resources, video editing has become increasingly easier and even novices can make an edited video stream within minutes. This can introduce many security concerns. So detecting video forgery has become a critical requirement to ensure integrity of video data. There are two major techniques for protecting video data against tampering, active and passive method.

II. BACKGROUND WORK

The internet is expanding at exponential rates; given the current scenario scientists evaluate that in a matter of few year times, the size ofvideo data will exceed thousands. With the rapid development of various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial, and military fields, which may include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important.

As S.Rajagopalet. Al, 2013 , points out in, Video data security is very important for multimedia commerce on the internet and real-time video multicast. However, traditional encryption algorithm for data secrecy such as DES, AES may not be suitable for multimedia applications because they are unable to meet the real-time constraints required by the multimedia applications. For video applications lightweight encryption algorithms are suitable. This paper analysis the possibility of deploying encryption algorithm in various stages of compression.

This joint compression and encryption of video data provides security for real time applications like video conferencing, surveillance camera data protection, etc. From the generic structure of a video encoder, the analysis of incorporating several encryption algorithm in the compression stages like transformation stage, in coding stages were presented.

As per LalitDhande.Et.Al ,2014 , more and more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content’s confidentiality. All previous methods embed data by reversibly memory space from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method by reserving memory space before encryption with a traditional RDH technique, and thus it is easy for the data hider to reversibly embed data in the image. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

Vijayaraniet. Al., 2015, Multimedia data mining is a popular research domain which helps to extract interesting knowledge from multimedia data sets such as audio, video, images, graphics, speech, text and combination of several types of data sets. Normally, multimedia data are categorized into unstructured and semi-structured data.

These data are stored in multimedia databases and multimedia mining is used to find useful information from large multimedia database system by using various multimedia techniques and powerful tools. This paper provides the basic concepts of multimedia mining and its essential characteristics. Multimedia mining architectures for structured and unstructured data, research issues in multimedia mining, data mining models used for multimedia mining and applications are also discussed in this paper. It helps in multimedia mining research.

III. METHODOLOGY

The objective of the proposed work for the Detection of frame drop has been considered to be developed for both spatio-temporal tampered and temporally tampered videos whereas frame swapping and frame copying have been considered to be developed only for temporally tampered videos. Frame drop and frame swapping have been considered to be addressed at frame level, whereas, frame copying has been considered to be addressed at scene level. To facilitate format independent tampering detection, all schemes have been developed for raw videos. Further, we considered to address quality assessment for spatio-temporal distortion (tampering) where frame drop has been considered temporal distortion. In summary, following are the set of objectives:

1. Development of a full reference (FR) algorithm to identify the structure of video and, Development of a full reference (FR) algorithm to identify the exact location of tampering in spatial-temporal tampered videos where temporal tampering has been caused due to frame drop.

2. Development a new framework which create a structure a video and improve the video frame security through which we reduce the video tempering.

3: Development of no reference (NR) algorithm (s) to classify a video as tampered video and identify the location of tampering in temporally tampered videos where temporal tampering has been caused either due to frame drop, frame swapping, or frame copying.

4: Development of a full reference (FR) video quality metric which is capable to measure quality degradation in spatial-temporal distorted (tampered) videos where temporal distortion has been caused due to frame drop.

Video: Tampering and Detection

In new area video tampering is relative with, image doctoring is as old as the art of photography itself where we have numerous incidences of serious cases of fake photographs. During tampering a video, objective of a forger is to create a tampered or doctored or fake video from real or actual or original video. These real videos are the source for creating tampered videos. Tampering can be done either on a single video (i.e. single source) or on multiple videos (i.e. many sources).we considered the single source based video tampering and developed schemes for tampering detection in such tampered videos. The seriousness of video tampering depends on how and where these tampered videos have to be used. Court trials are one of the most widely used application areas where these tampered videos are presented as evidence to mislead the court proceedings

Forensic tools and forensic experts play the key role to examine the authenticity of video evidences. While examination, if it has been found as authentic (i.e. non-tampered or actual), experts generally embed watermark into authenticated videos such that whenever required its authenticity can be re-examined by retrieving the watermark.

During examining videos, there may be following possibilities with forensic experts: (a) Forensic experts may need to blindly examine (i.e. trace the tampering if any) the videos i.e. no information is available about the original source video from which the tampered video was created, (b) Forensic experts may need to trace the tampering with a copy of watermark videos with reference to actual videos (with embedded watermark), and (c) Forensic experts may need to trace the tampering in actual videos (with embedded watermark).

Video by

Frame -Frame types

The basic principle for video compression is the image-to-image prediction. The first image is called an I-frame and is self-contained, having no dependency outside of that image. The following frames may use part of the first image as a reference.

An image that is predicted from one reference image is called a P-frame and an image that is bidirectional predicted from two reference images is called a B-frame.

> I-frames: Intra predicted, self-contained

> P-frames: Predicted from last I or P reference frame

> B-frames: Bidirectional; predicted from two references one in the past and one in the future, and thus out of order decoding is needed.

3. Video Quality Assessment

Based on reviewed literature, identified different types of quality assessment; modes of quality assessment; requirements of subjective experiments; and types of objective quality metrics.

Quality of a video can be measured in two ways viz. subjective assessment and objective assessment where quality assessments are generally conducted in three modes viz. full reference (FR) quality assessment, reduced reference (RR) quality assessment, and no reference (NR) quality assessment .

Subjective quality assessment involves human subjects to measure the video quality (in all modes i.e. FR, RR, and NR), whereas, objective quality assessment involves various objective quality metrics viz. Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), Video Quality Metrics (VQM), etc. to measure the video quality . MSE, PSNR and SSIM are used in FR mode whereas VQM can be used in both FR and NR modes.

The basis of human visual system (HVS) and have been employed for designing many objective metrics. Many requirements which need to be taken care of while conducting subjective experiments. These involve a set of reference (or source) and distorted videos; human subjects (trained, untrained or mixed); experiment procedures (viz. single stimulus continuous quality evaluation and double stimulus continuous quality evaluation); viewing conditions and setup; experiment sessions (around 30 to 40 minutes); scoring policy (viz. qualitative and quantitative); computation of the mean opinion score; and a subject rejection scheme.

Next section presents the critical review of some existing schemes related with video tampering detection and video quality assessmen

VI. REFERENCES

[1]Abomharaet. al., 2010, ―An Overview of Video Encryption Techniques‖, International Journal Of Computer Theory And Engineering, Vol. 2, No. 1, Page No.103-110.

[2]Suryadiet. al., 2012 ―Enhancement of Video Encryption Algorithm Performance Using Finite Field Z2 3-Based Chaotic Cipher‖, Journal Of Communication And Computer, Vol. 9 Page No.960-964.

[3]Rajagopalet. al., 2013, ―A Survey of Video Encryption Algorithms Implemented In Various Stages of Compression‖, International Journal Of Engineering Research & Technology, Vol. 2 No.2, Page No. 1-12

[4] Dhande et. al., 2014, ―Hide Inside-Separable Reversible Data Hiding in Encrypted Image‖, International Journal Of Innovative Technology And Exploring Engineering, Vol.3 No.9 Page No. 88-91.

[5]Dr. Dinesh Goyal et .al 2014 "Security of Multimedia Data in Cloud "International Journal of computer science & information technologies volume:5 ,issue:4.

[6] Chakravarthyet. al., 2014, ―A Three Way Reversible Encipherment Mechanisms for Robust Video Data Hiding Using Selective Embedding and Forbidden Zone Data Hiding‖, International Journal Of Computer Science And Information Technologies, Vol. 5 No.1,Page No. 873-875.

[7]]Ismail et. al., 2014―Selective Video Encryption System using AES (Rijndael) Algorithm for Low Cost FPGA Chip‖ Recent Advances in Computer Engineering, Communications and Information Technology, ISBN: 978-960-474-361-2, Page No. 318-323

[8]Vijayaraniet. al. ,2015, MULTIMEDIA MINING RESEARCH – AN OVERVIEW, International Journal of Computer Graphics & Animation (IJCGA) Vol.5, No.1, January 2015.

[9]Moideenet. al., 2014, ―A Novel Method for Data Hiding In Encrypted Image And Video‖, International Journal Of Emerging Technology And Advanced Engineering, Vol. 4 No. 2 Page No. 538-542.

[10] Ragabet. al., 2014, ―Encryption Quality Evaluation of Robust Chaotic Block Cipher for Digital Imaging‖ International Journal Of Recent Technology And Engineering, Vol. 2 No.6, Page No. 4-9.

[11]Aggarwal et. al., 2014, ―Design and Implementation of Video Encryption for Multimedia Applications‖, International Journal Of Engineering Research And Applications, Vol. 4 No. 2, Page No.29-34

AUTHOR’S INFORMATION

Rahul Soni is a research scholar at SGVU studying Software Engineering. He has published papers in national and international journals on Computing.

Gajanand Sharma is an assistant professor in SGVU, heading the Department of Computer Engineering and Information Technology with a vast knowledge of cryptography. He has published many works in different journals.