ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

A Survey of Data Hiding using Digital Watermarking Framework for Real-Time Multimedia Communication

Monisha.M.S [1], Chidambaram.S [2]

P.G. Student, Dept. of ECE, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India[1]

Associate Professor, Dept. of ECE, Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India [2]

ABSTRACT: Source origin authentication and data integrity are vital areas for real-time multimedia systems. Traditional methods are not appropriate to overawe the forgery presented in multimedia data transmission. Digital watermark is a key for secure the authorized persons information during transactions. This research work gives the survey of data hiding in Real Time multimedia communications, furthermore all over the world the multimedia transactions takes place through the internet. Multimedia communication through the internet that makes threatening from an illegal person can change the original information. Copyright is a major concern during communication. Therefore we should attentive for more effective copyright protection, such as using data hiding techniques into multimedia content during communication. Therefore with the help of data hiding methods to enhance the authentication, confidentiality and integrity of the transfer multimedia content in real time communications. We are discussed here different data hiding techniques using digital watermarks in real time multimedia communications.

KEYWORDS: Data Hiding, Digital Watermark, Real-Time Multimedia communications, Threatening, Copyright, Authentication.

I. INTRODUCTION

With the widespread use of multimedia information, digital content have emerged as a growing among (piracy). In current years, multimedia has enormously increased during public transaction networks. Transactions are mainly including audio visual applications such as the video phone, military transactions, video conference, video e-mail, audio message, video streaming, digital TV, HDTV (high-definition TV), VoD (Video on Demand), distance learning, and distance cooperation research and monitoring, images in different standards. First our main problems relating to the consistency and secure of the data transmission and storage in the processing area [5]. The major problem in the distributed environment has not been fully predictable for regarding the protection for multimedia content development. The connection of the network based on different properties such as resolution, storage capacity, and processing ability. In Multimedia watermarking has evolved very rapidly for the duration of last year's[6]. Today most of the information has been transmitted in the form of digitalization. As a result, protection of multimedia content must be addressed [3].

II. DATA HIDING

Information hiding implies imperceptibility embedding information (message) into the host signal (images, video, audio, text etc.). Currently all types of media files probably uses watermark [2].Digital rights management is the integration framework consisting of security and protection needed for creation, storage, and transfer for evaluated of multimedia content. Traditional techniques for digital content protection such as encryption and scrambling unaccompanied, cannot provide the sufficient protection for multimedia content.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Therefore we produce robust content protection to overcome these situation. To this end data hiding is the primary technique to develop content protection, content authentication, ownership protection, and content usage. Data hiding technologies such as Digital Watermarking, Steganography, and fingerprinting [1].

- **Digital watermarking**

A process of undetectable embedding data (watermark) into an electronics media in order to provide content protection. Watermarking which is used to track the ownership and copyright of electronic media.

- **Steganography**

Searching of process to hide the presence of hidden messages. Such methods include invisible ink, microdot, digital signature, convert channel and spread spectrum communication.

- **Digital Fingerprinting**

Method of inserting unique labels or identification numbers into digital content prior to distribution. DRM policies is commonly used the digital fingerprinting technology to enforce it. It is used to trace the unauthorized user activity they are not have the capable to getting original information

Data hiding scheme are evaluated based on three independent parameter performances, Embedding capacity, robustness, fidelity[1].

III. DIGITAL WATERMARKING

Digital watermarking which is insert a watermark message (hidden) in a core object such that the hidden message is inseparable [4, 9]. Traditional watermark applied only in the text form. Nowadays watermarking applies to all types of multimedia communications. Main drawback in watermarking is difficult to remove watermark from the host message without damaging the data.Digital watermarking schemes can be broadly classified into four categories namely: robust, fragile, semi-fragile, and reversible [7].

Digital signature that is one of the digital watermark in the form of signature which is used an electronic protocols for the authentication of electronic documents whereby a receiver of a message can verify the identity of the sender and the integrity of the message [8].

A. *APPLICATIONS*

Digital watermarking is being used in various applications. In general:

- **Covert communication**

It is one of mainly application for steganography. People would like to send the information to each other without being detected such as military and intelligence applications.

- **Authentication**

It is necessary to verify the authenticity of input data, i.e., to detect whether the information are unique, forged, or reformed version of the original. This type of application fragile watermarks is used.

- **Identification of ownership**

To identify the original ownership of digital media for that robust watermarking algorithm are developed. In this situation an authorized user have the legal proof that they are the real owner.

B. *CLASSIFICATION OF DIGITAL WATERMARKING APPLICATIONS*

In this paper we are focusing only the third class is security methods for real-time multimedia communication. Here the embedder and receiver both are known the hidden message. If original host data available or unavailable at the decoder side then the problem is blind decoding or non-blind decoding. Figure 1 shows the classification of digital watermarking application [1].

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

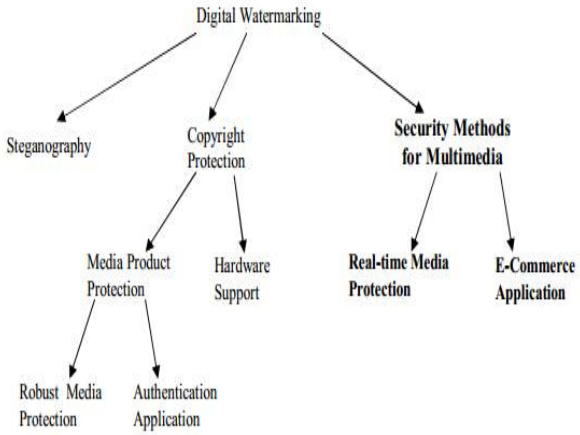

Fig 1. Classification of digital watermarking applications

IV. REAL TIME MULTIMEDIA COMMUNICATION

Real time multimedia communication make public some special properties stemming from both multimedia data and real time communication[1].

- End user cannot recognise limited distortion in multimedia data, accordingly, some bit errors and packet losses occurring during communication do not flaw the whole visual/audio quality
- Packet losses may happen any time due to implementation of real-time multimedia communication and controlling protocols.
- The communication security compromises should be as small as possible, because of the enormous amount of multimedia data

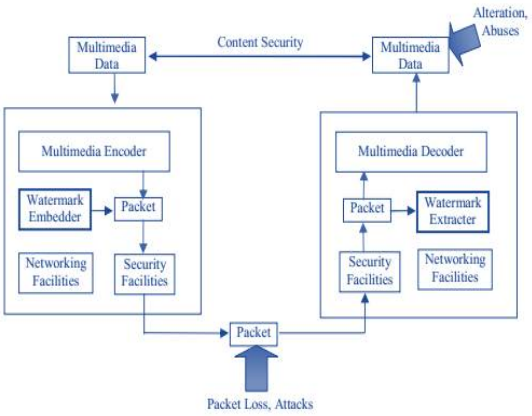

Fig 2. Content Security in Real-Time Multimedia Communication

The above fig 2. Illustrates attacks to the content security of real-time multimedia communication. Packet loss and mischievous attacks are subjected to the multimedia traffic, during the course of transmission.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

V. A WATERMARKING FRAMEWORK FOR REAL-TIME MULTIMEDIA COMMUNICATION

The digital watermarking technique can be viewed as modulating a strong signal with a weak noise. If the noise value is predefined using threshold values, here noise is below predefined threshold (HAS is a reference measurement for audio watermarking and HVS is a threshold for image watermarking), person cannot noticed the distortion produced by digital watermark. A typical watermarking framework is first proposed by I. Cox [2.9], as illustrated in Figure 3. The digital watermark (W) and Multimedia data (Do) are insert to the embedder, and the sending copy is embedded with the help of key. At the detector side received copy (D2) is received with the help of key decrypted and finally get the Digital watermark (W').

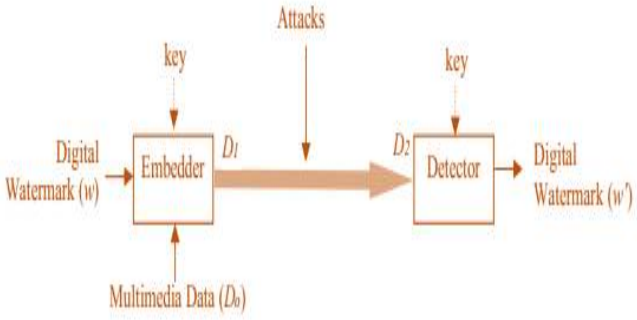

Fig 3. General frame work for data hiding system

Where,
D_1 - Watermarked Media,
D_2 - Received copy.

VI. OUTLINE OF A SECURITY MECHANISM USING DIGITAL WATERMARKS

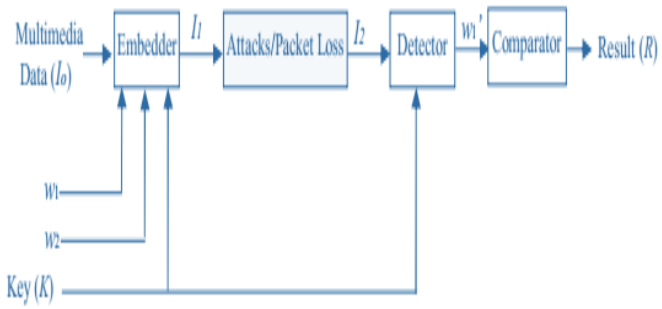

Fig 4.Secure Real-time Communication with Digital Watermarking

Where,
w_1 – public, w_2 - watermark,w_1' - public digital watermark.

Digital watermarking provides a different method to make sure the safety of multimedia data during communication in flexibly available channel. Without degrading the overall quality of the transmitted data a digital watermark can assure the multimedia data integrity and authenticity. Figure 4 shows the outline of a security mechanism using digital watermarks. Digital watermarking operates on the multimedia data to hide/extract information.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

VII. LAYERED STRUCTURE OF DATA HIDING REAL TIME MULTIMEDIA SYSTEM

A layered structure of the security framework using digital watermarking technique is illustrated in Figure 5.

- **Watermark operation** extracts watermark bit from the watermarked data or embeds watermark bits in the host signal
- **Transmission layer** deals with any packet loss which may during the transmission and the bit error for stored media.
- **Security infrastructure** provides the traditional cryptographic service for the framework, and it may be implemented by SSL. The cryptographic service includes secure channel management and digital certificate authentication.
- **Content security** handles the security of the whole multimedia session to protect multimedia data from reuse and abuse.
- **Application layer** extends the content security, and one potential application is “voice cheque”

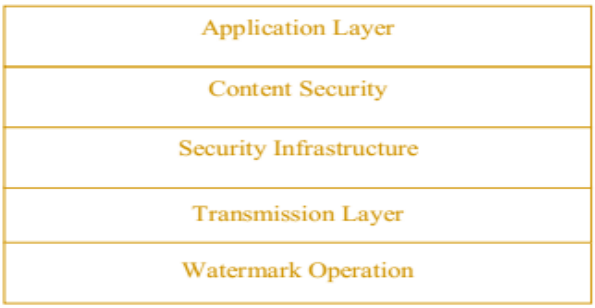

Fig 5. Layered structure of data hiding real time multimedia system

VIII. CONCLUSION

In previous security techniques, source origin authentication is attained by hashing. Yet, hash function was originally developed only for authenticity and integrity problems of text messages. Therefore, it does not suitable to take a consideration, obviously the special properties of multimedia data nor real-time communication. Hashing is a onetime security method, it does not correlated with timing, and there are some serious drawbacks while using these hashing function. Finally we conclude these with a comparison into the digital watermarking. Using digital watermarking enormous applications are present in the real-time multimedia communication.

REFERENCES

1. Digital Watermarking-Based AuthenticationTechniques for Real-Time MultimediaCommunication, Dec 2005.
2. Kunal D Megha1, Nimesh P Vaidya2, Ketan Patel, “Digital Watermarking: Data Hiding TechniquesUsing DCT-DWT Algorithm,”International Journal Of Advanced Research In Computer And Communication EngineeringVol. 2, Issue 6, pp 2397-2402, June 2013.
3. Jung-HeeSeo, Hung-Bog Park, “Data-Hiding Method Using Digital Watermark In The Public Multimedia Network,” International Journal Of Information Processing Systems, Vol.2, No.2, pp 82-87, June 2006.
4. Arun Kumar, S.M. Riyazoddin,“Analysis of Data Hiding Techniques in Encrypted Images - A Survey,” Global Journal of Computer Science and Technology Graphics & Vision, Vol. 13, Issue 4 pp. 39-43, 2013.
5. Ruban R, S. Santhosh baboo, “A Secure and Robust Reversible WatermarkingAlgorithm Using Fuzzy Matching – Quad TreeSegmentation (F-QTS) Technique for Digital Images”,International Journal of Computer Applications Vol. 108, No. 9, December 2014.
6. G.Voyatzis, I. Pitas, “The Use of Watermarks in the Protection of Digital Multimedia Products,” pp 1-33, 2000.
7. Chang-Tsun Li, Digital Watermarking For Multimedia Security Management pp 1-16.
8. LiehuaXie and Gonzalo R. Arce,, “A Class of Authentication Digital Watermarks for Secure Multimedia Communication”, IEEE Transactions On Image Processing, Vol. 10, No. 11, November 2001.
9. Hartung, Martin Kutter, Multimedia Watermarking Techniques Frank Proceedings Of The IEEE, Vol. 87, No. 7, pp 1079-1107, July 1999.