Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Qualitative Research Approach to Ensure the Copyright of Multimedia data by using Watermarking Techniques

Muhammad Akram
College of Computer Science & Information Systems, Najran University, Saudi Arabia

Ahmad M. Taleb
College of Computer Science & Information Systems, Najran University, Saudi Arabia

Md. Kafil Uddin
College of Computer Science & Information Systems, Najran University, Saudi Arabia

Abstract— Multimedia security is a challenging task in worldwide distributed environments and due to the violation of copyright digital media industry is suffering huge financial loss. Widely used compression standard for video file is MPEG, and on the basis of motion prediction MPEG data consists of three different types of frame i.e. I-frame, P-frame and B-frame. Digital watermarking is a technique used to protect the multimedia contents from illegal use. In-visible digital watermarking is an effective way to protect copyrights of multimedia by embedding a special and invisible pattern in data which contains the information about the identity of the owner. Most of the watermarking techniques are marking only I-frame to protect the copyright of multimedia files. These technique are providing reasonable security of data but still not fully able to protect the contents from illegal distribution. This paper involves to study the different frame of MPEG compression standard and to explore the different security concerns in multimedia data. Also we have identified the common security requirements, mechanism, security measures, important parameter and attacks for video data. Moreover to investigate and evaluate the existing watermarking techniques and to address its applications.

Keywords— Water-marking algorithms, security measures, security mechanism, security requirements, security parameters and attacks

I. INTRODUCTION

Rapid growth of digital world provides many advantages over analog world i.e. fast and noise free communication, use of software as a substitute of hardware processing and fast and easy update of existing systems etc. Beside various advantages of digital world there are some disadvantages too. For example, rapidly growing distributed environments make easy access to multimedia products. On the other hand it make difficult to protect the copyrights of multimedia contents and make fast and easy distribution of illegal copies. This causes huge financial loss to digital media industry.

Privacy of data is possible with different techniques like providing limited and authenticated access to data and/or using encryption [1]. However illegal distribution of the data cannot be controlled by only these techniques. Hence one solution can be to identify and trace back illegal copies of the data. This is possible by embedding the owner's information in the data itself. Adding copyright label, origin, status, destination of data or other verification messages to digital data is called Digital Watermarking sometimes also known as fingerprinting [1], [2] . Invisible digital watermarking is an effective way to protect copyrights of multimedia by embedding a special and invisible pattern in data which contains the information about the identity of the owner. This information can later prove ownership, identify illegal copy, trace the marked document's distribution through the network, or simply inform users about the rights-holder or the permitted use of the data. An effective watermark must be non-removable even after the modification of the data and must not add perceptible distortion.

Currently multimedia security is a challenging task in worldwide distributed environments. Most of the digital multimedia data is stored in compressed formats in order to reduce the storage size. Therefore it is important to embed the watermark in compressed data instead of decompressing it first [1]. MPEG is widely known compression standard for video data. On the basis of motion prediction MPEG data consist of three frame types: I-frame, P-frame and B-frame. Combination of different frame types is called GOP (Group of pictures). One GOP usually consists on 12-15 frames [2]. Most of current MPEG watermarking techniques mark only I-frame which is typically one frame in a GOP. Watermarking algorithms of this category are weak in robustness and can be affected by different attacks [3]. For example "Frame type changing" attack can affect the watermark easily. Frame Re- Synchronization can be used to prevent against this attack [4] but it involves high complexity. The alternate is to embed the watermark in every frame of GOP. This technique can prevent against various attacks but can also affect the quality of video because P/B-frames generally do not have adequate volume to embed watermark. Hence, an improvement in current watermarking technologies seems to offer effective protection of multimedia data. Research in this project is an effort to study MPEG video standard and different existing watermarking algorithms to identify the security requirements, security parameter, mechanism used, measures to take to protect copyright information and different type of attacks that can affect the copyright information of multimedia data.

This paper is organized into six sections. The subsequent section briefly explain the MPEG compression standard. Section III discuss about main security requirements for multimedia data protection, mechanism used and measures. Section IV talks about the classification of watermarking algorithms and study of existing algorithms with their benefits. Section V explain the required parameters and different type of attacks on watermarking algorithms.

II. MOVING PICTURE EXPERT GROUP (MPEG)

In 1988[5] International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) formed a group of expert peoples and named it Moving Picture Experts Group (MPEG). The purpose of this group was to develop the standards for audio and video data.

Literature review enable us to identify the three different types of frames which involves in MPEG data. Those three frames are: [6]

i. I frame: also called intra-coded frames,
ii. P frame: also called predictive frames,
iii. B frame: also called bi-directional frames.

As an example display order of MPEG frames is shown in figure 1 below [7]:

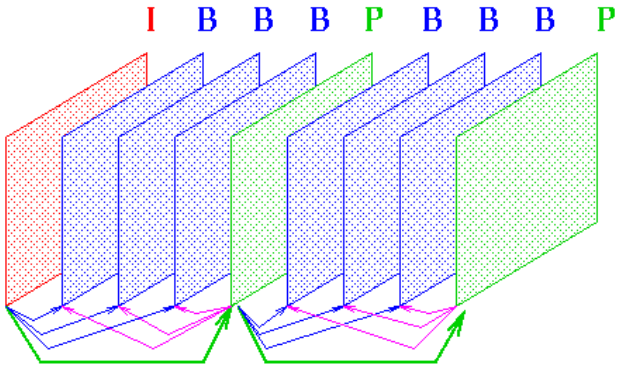

Fig 1: Display order of MPEG frames

- Because I-frames are intra-coded, so they did not depend upon any other frames during reconstruction process.
- P-frames always depends on the last I-frame or last P-frame which means that during reconstruction of P-frames, it is very important to get the data from last I-frame or last P-frame, moreover reconstruction will be impossible without collecting data. As shown in figure 1 above there are two P-frames: Prediction of first P-frames is depending on first I-frame and second P-frame is depending on last P-frame. Dependency is shown using arrows.
- B-frames are bidirectional and prediction of these frames depends on last and next I-frame or P-frame. Moreover reconstruction will be impossible without collecting data from both sides of B-frames. Six B-frames are shown in the figure above, arrows shows the dependency of B-frame on back and forward I-frames and P-frames.

Motion vector is an important part of MPEG which plays a vital role in the prediction. Motion vector define the movement of information/data from one frame to another frame. Motion vector is further divided into of two parts [7], (i) horizontal part and (ii) vertical part with some positive or negative values. If value is positive then movement will be towards right or downwards and if value is negative then movement will be towards left and upwards.

III. SECURITY REQUIREMENTS, MECHANISM AND MEASURES FOR MULTIMEDIA DATA

Security measures have a close relationship with security requirements and security mechanism. To implement security services, it is very important first to identify the security requirements. After identification of security requirements; next step is to achieve them; which are achieved by taking security measures and security measures need some security mechanism.

A. Security Requirements

Some common security requirements for multimedia system are: [8]

1) *Confidentiality:* refers to keep the information secret from unauthorized receivers. It ensure that only authorized receiver can read the information. Encryption techniques/cipher-system can be used to achieve confidentiality.

2) Integrity: refers to the data alteration during transmission. It ensure that during transition contents are modified or not. It can be achieved by using hash function, digital signature, fragile watermarking, robust digital water marking.

3) *Data origin authenticity:* refers that data is coming from authentic origin. Data origin authenticity can be achieved by message authentication code, fragile watermarking, digital watermarking etc.

4) *Entity authenticity:* refers that data is coming from authentic entity. It can achieved by using some authentication protocol, public key cryptography etc.

5) *Nonrepudiation:* refers to the mechanism which proves that the sender really send message or not. Nonrepudiation can be achieved by message authentication code, digital signature, time stamping etc.

Above security requirements are common for most of the systems. To take security measures for any system it is very important to consider the above security requirements.

B. Security Mechanisms

Mainly used security mechanism are cryptographic mechanism and digital water-marking. In this paper we will concentrate on water-marking mechanism for multimedia data. Many researchers have proposed variety of watermarking techniques, which will be discussed in next section.

C. Security Measures

To achieve a best security solution, security measures plays a vital role. Security measure needs a mechanism to implement the identified security requirements. In this paper we will focus on watermarking mechanism to ensure the copyright protection of multimedia data.

IV. MULTIMEDIA WATERMARKING

Watermarking is a process which is used to embed a signal (i.e. digital signature, copyright label, watermark etc.) in multimedia data [9]. Multimedia watermarking algorithms can be classified into [8]:

- copyright watermarking
- fingerprint watermarking
- copy control and broadcast watermarking
- annotation watermarking
- integrity watermarking

Moreover literature review enables us to identify that embedded watermarks can be detected later from multimedia data for the purpose to;

- verify the origin,
- verify the owner,
- extract the modification,
- protect against illegal recoding
- ensure the copyright of multimedia data.

Main requirements for any watermarking algorithm are robustness, imperceptibility, and capacity of data hiding. Also robust water marking is always a top most requirement for any watermarking technique. S. Voloshynovskiy et. al. [10] has proposed the generalized diagram for robust watermarking, which is shown in figure 2 below:

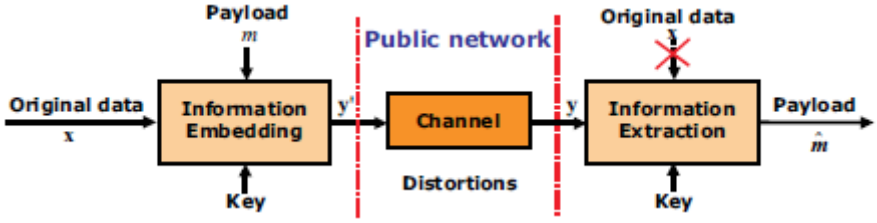

Fig 2: Diagram for robust watermarking [10]

When data is hidden inside of any multimedia contents then hidden data/message is always under threat against various attacks. Literature review enable us to classify the attacks into;

- intentional
- unintentional

Few attacks are briefly discussed in section V. Purpose of robust watermarking is to provide a solution for reliable communication of message in body of multimedia content. In figure 2 above; the main purpose is to embed an invisible message "*m*" inside the contents of multimedia data "*x*" with secret key "*K*". More details can be found in [10], but important is to embed a 64bit invisible message in original image by considering the distortion criteria in public network and strong robustness against different type of attacks. In above diagram without knowledge of algorithm, robustness security requirement will provide the resistance against message removal from multimedia data.

Many other researchers also has proposed different solution for robust and secure watermarking. According to Hartung et al. [11] embed the watermark into the MPEG without to increase bit rate by marking only discrete cosine transform (DCT). Also this proposed method is less complex and more robust if compared with methods for complete decoding followed by watermarking technique in pixel domain and re-encoding.

B. G. Mobasseri [12], has proposed a two layer operation for watermarking. To watermark a multimedia data he used direct sequence spread spectrum. In this technique without information of seal, it is not possible to corrupt or to remove the watermark from multimedia data. Performance is robust if somebody try to perform subsampling or frame recording. Also copyright information can be retrieved easily from short video segments.

Deguillaume et al. [13] proposed technique for video watermarking, which is based on DFT. It consists of 3-dinmentional chunk of scenes in video files. To ensure the security of system, this technique allows to hide "watermark" and "template" inside multimedia video contents using owner key.

Reference [14] and [15] proposed watermarking technique to ensure that copyright information is hidden properly and in secure way. This technique is based on slight modification of motion vectors in MPEG data. This watermarking technique is suitable and can be used on compressed and uncompressed video. It also provides the little influence on decoding speed and perceptive effect of MPEG data. Also this proposed method can be used to embed the watermark in short video files.

V. PARAMETERS AND ATTACKS ON WATERMARKS

When researchers are going to propose watermarking algorithm, it is very important also to considers parameters and type of attacks that can affect water marking system. In section IV, we stated some classification of watermarking. Mentioned classification also have some important parameters to be considered and these watermarks can be affected by some different type of attacks.

Jana Dittmann et al.[8] produced a table which explain different type of parameters and attacks on above discussed classification of watermarking, which are briefly discussed below. But in this paper our main focus is to ensure the copyright protections of multimedia data, so mostly we will concentrate only on copyright watermarking technique.

A. Copyright watermarking:

Parameters and attacks on copyright watermarks is shown in figure 3. It is important to consider the parameters and attacks before going to propose any copyright watermarking algorithms.

As shown in figure 3, the important parameter for copyright watermarks are: must be robust at high level, must provide high level security, must have capacity for owner identification, verification process must be done at private level and done at public level if required, use of blind methods, and must be invisible.

Also researchers be familiar with different type of attacks when proposing any solution for watermarking, these attacks can be classified into mosaic attacks, stirmark attacks, geometrical attacks, histogram attacks, template attacks and forgery attacks.

B. Fingerprint watermarking:

Fingerprint watermark have same parameters as discussed in copyright watermark but only difference is that in this method non-blind technique will be more suitable then blind method. Also attack are similar as copyright watermark, but need to consider one more attack called coalition attack.

C. Copy control and broadcast watermarking:

Parameters in copy control and broadcasting are similar as fingerprint watermarking but in this technique will be less complex. Also researchers need to consider same number of attack which are discussed in fingerprint watermarking.

D. Annotation watermark:

In this watermarking technique robustness and security is not very much important. Remaining parameters are similar as discussed in copyright watermarking. Also in most of the cases annotation watermarking technique is not under threat against any attack.

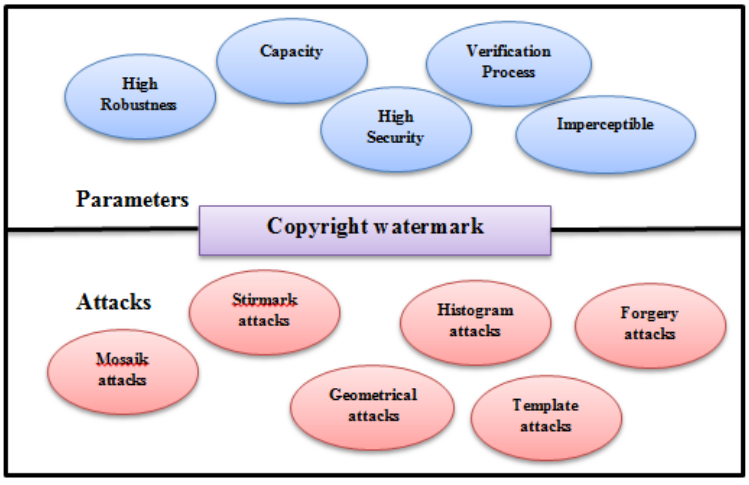

Fig 3: Parameters and Attacks on copyright watermarks

VI. CONCLUSION

This research focus to ensure the copyright of multimedia data by using watermarking techniques. We found that an invisible digital watermarking technique is an effective way to protect copyrights information of multimedia data. Moreover this protection can be achieved by embedding a special and invisible pattern in data which contains the information about owner. Further watermarking algorithms are classified into copyright watermarking, Fingerprint watermark, Copy control and broadcast watermarking, Annotation watermark, integrity watermarking. In this paper our main focus was copyright watermarking and we identified different required parameters (*i.e. robustness, security, verification, capacity of owner identification etc.*) and attacks (*i.e. intentional and unintentional*) that can affect the copyright information in multimedia data. We studied different proposed watermarking technique, all proposed techniques have some merit and demerits but it is concluded that it is very important first to identify the security requirements that we must need to address according to current environment. Then select the suitable mechanism to embed the watermark in multimedia file because later this watermark can be used to verify the origin, to verify the owner, to extract the modification done and to protect against illegal recoding.

ACKNOWLEDGEMENTS

The research team would like to gratefully acknowledge the financial support of the Deanship of Scientific Research in Najran University, Najran, Kingdom of Saudi Arabia.

REFERENCES

[1] F. Hartung, "Digital Watermarking and Fingerprinting of Uncompressed and Compressed Video", PhD Dissertation, University of Erlangen, 2000.

[2] Key words: i) Digital watermarking ii) MPEG video, web page: http://en.wikipedia.org/

[3] E. Hauer, M. Stabenach, "Robust Digital Watermark Solution for Intercoded Frames of MPEG Video Data", in *Proceedings of the SPIE Security, Steganography, and Watermarking of Multimedia Contents VII*, edited by: Delp, Edward J., III; Wong, Ping W., volume 5681, 2005, pp. 381-390.

[4] S. Moradi and S. Gazor, "Evaluation of Robust Interframe MPEG Video Watermarking", presented in *Canadian Conference on Electrical and Computer Engineering*, Canada, May 1-4, 2005.

[5] John Watkinson, "The MPEG Handbook: MPEG-1, MPEG-2, MPEG-4", Second Edition, An imprint of Elsvier, ISBN: 024080578X.

[6] Ehab S. Al-Shaer, Giovanni Pacifici, Management of Multimedia on the Internet: 4th IFIP/IEEE International Conference on Management of Multimedia Networks and Services, MMNS 2001, Chicago, IL, USA, October 29 - November 1, 2001. Proceedings.

[7] MPEG video compression technique http://vsr.informatik.tu-chemnitz.de/~jan/MPEG/HTML/mpeg_tech.html [Accessed: November 21, 2012]

[8] Jana Dittmann, Petra Wohlmacher, Klara Nahrstedt, Mutimedia and Security Using Cryptographic and Watermarking Algortihms, Multimedia, IEEE, Volume 8, Issue 4, Oct-Dec 2001, ISSN: 1070-986X, pages 54-65.

[9] Alekhika Mohanty, Study and Implementation of Watermarking Algorithms, A project report submitted to fulfill the requirements for degree of M Tech by Research in Electronics and Communication Engineering, Department of ECE, National Institute of Technology, Rourkela, India, April 2006.

[10] S.Voloshynovskiy, O. Koval F. Deguillaume and T. Pun, "Multimedia security: open problems and solution", Aspects of Network and information security, pages 143-150, IOS Press 2008.

[11] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video", *Signal Processing* vol. 66, pp. 283-301, 1998.

[12] B. *G.* Mobasseri, "Direct sequence watermarking of digital video using m-frames", *Proc. ICIP'98,* Chicago, pp. 4-7, Oct. 1998.

[13] F. Deguillaume, G. Csurka, J. J. K. 0. Ruanaidh, and T. Pun, "Security and Watermarking of Multimedia Contents", *SPIE Proceedings IS&T/SPIE'S 11th Annual Symposium*, vol. 3657, pp. 23-29, 1999.

[14] Jun Zhang, Henri Maitre, Jiegu Li and Ling Zhang, "Embedding watermark in MPEG video sequence", Multimedia Signal Processing, 2001 IEEE Fourth workshop, ISBN: 0-7803-7025-2, pages 535-540, Oct 2001.

[15] Yuanjun Dai, Lihe Zhang and Yixian Yang, "A new method of MPEG video watermarking technology", Communication Technology Proceddings, 2003. ICCT 2003, ISBN: 7-5635-0686-1, pages 1845-1847 vol 2, 2003.

