ENHANCING THE ROBUSTNESS OF DIGITAL VIDEO WATERMARKING FOR COPYRIGHT PROTECTION AGAINST COLLUSION ATTACK

ALI BOROUJERDIZADEH

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

DECEMBER 2012

ABSTRACT

In the digital world, due to the ease of creating, publishing and tampering of works, copyright protection became a major issue. This issue is much significant in movie industry which cause millions of dollars loses. With new technologies almost everybody are able to produce, edit and share videos. Thanks to the Internet the sharing of works also, become a breeze. Hence, there should be a mechanism to prove the ownership and make sure of the integrity. Watermarking is one of the effective ways to help copyright protection. According to this problem, this project is defined to enhance the current copyright protection. We narrow down the project to a specific attack. Collusion attack is the main problem for video watermarking for copyright protection. In this attack, colluders try to estimate and remove the watermark by comparing as many as watermarked materials. By increasing in number of watermarked materials, the estimation becomes more accurate. The proposed method is a frame-by-frame video watermarking. To address the collusion attack, each frame receives a different watermark. Since each frame has a unique watermark, it is impossible for the attack to estimate it. In this project Block Truncation Coding (BTC), Discrete wavelet transform (DWT) and Singular value decomposition (SVD) are combined to achieve the required robustness against the attack as well as maintaining quality. The BTC is used in watermark generation. DWT and SVD are used to prepare the frames and embed the watermark. The robustness is tested using Bit Error Rate (BER) and the quality is checked using Peak signal-to-noise ratio (PSNR). The results of the project, in compare with related works, shows that the proposed method is robust against all types of collusion attack, and at the same time, the quality of the video is remain in a satisfactory level. Meanwhile, it is proved that the method is robust against some other attacks as well.

ABSTRAK

Dalam dunia digital, disebabkan kesenangan mencipta, menyebarkan dan menggangu kerja-kerja, hakcipta terpelihara menjadi satu isu besar. Isu ini menjadi banyak terlibat dalam industri perfileman yang menyebabkan kerugian jutaan dollar. Dengan teknologi baru, hampir kesemua manusia kini mampu menghasil, mengubahsuai, dan berkongsi video. Terima kasih kepada internet, perkongsian kerja menjadi lebih mudah. Oleh itu, terdapat satu mekanisma untuk membuktikan hakmilik dan integriti. Watermaking adalah satu cara yang efektif untuk menolong perlindungan hakmilik. Berdasarkan masalah ini, projek ini didefinasikan untuk meningkatkan perlindungan hakmilik semasa. Kita kecilkan skop projek kepada satu serangan. Collusion attack masalah utama untuk video Watermaking untuk perlindungan hakmilik.Dalam serangan ini,peniru cuba untuk menganggarkan dan membuang watermark dengan membandingkan sebanyak mungkin bahan-bahan watermark. Dengan meningkatkan bahan-bahan watermark, anggaran menjadi lebih tepat. Caranya adalah dengan frame-by-frame video watermaking. Berdasarkan collusion attack, setiap frame menerima watermark yang berbeza. Setiap frame mempunyai watermark yang unik untuk mengelakkan serangan dari berlaku. Dalam projek Block Truncation Coding (BTC), Discrete wavelet transform (DWT), dan Singular value decomposition (SVD) digabungkan untuk mendapat perlindungan yang secukupnya daripada serangan dan juga mengekalkan kualitinya. BTC digunakan dalam generasi watemark. DWT dan SVD digunakan untuk menyediakan frame dan mengabungkan watermark.Ketahanan diuji dengan Bit Error Rate (BER) dan qualiti diuji menggunakan Peak Signal-to-noise ratio (PSNR). Hasil projek dibandingkan dengan hasil kerja lain yang menunjukkan tujuan cara ketahanan daripada semua jenis collusion attack, dan pada waktu yang sama, qualiti video adalah sentiasa dalam tahap kepuasan.Sementara itu, ia membuktikan cara ketahanan terhadap serangan lain juga.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

BER	Bit Error Rate
BTC	Block Truncation Coding
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HVS	Human Visual System
IDE	Integrated Development Environment
iDWT	Inverse Discrete Wavelet Transform
iSVD	Inverse Singular Value Decomposition
LSB	Least Significant Bit
PSNR	Peak signal-to-noise ratio
SVD	Singular Value Decomposition

CHAPTER 1

INTRODUCTION

1.1 Overview

This chapter has eight main sections. The first section is the overview, which is explaining the content of the chapter. The second section is problem background. This section gives a brief background of the situation of the problem. Third section talks about the issues. Background of the issue is focusing on all issues that are recognized on the topic. Then we continue with problem statement to declare which problem is going to be solved in this work. The next two sections, express the objectives and aim of the project. In scope section, we narrow down the experiment to a feasible level. The last section explains the expected outcomes.

1.2 Problem Background

According to the current information explosion rate, one of the major issues that producers are facing is ownership identification and proofing it, in other word copyright (Lee and Jung, 2001). In addition, digital media, which become the main mean of information sharing, make the issue even worse. The reason is the original work can be copied, modified and exchanged over peer-to-peer networks while this can happen repeatedly with the same quality despite the analog copying which is lossy. The main copyright consideration is copying the movies though out the

internet (Cisco, 2011). Nevertheless, watermarking which is an information hiding method is hired to address this issue (Barni *et al.*, 2000; Eskicioglu and Delp, 2001).

Watermarking is able to help about ownership identification and approval, in addition to copy control and modify prevention. As soon as the second step of watermarking is applied to a medium, it becomes a carrier. The three steps are generating the watermark, embedding it and retrieving (Bruce, 2001). In the digital world there are many different types of carriers such as text, image, audio, video etc. (Lee and Jung, 2001); even human DNA can be used as carrier (Heider and Barnekow, 2008).

Watermarking is a compound of data payload, fidelity and robustness. The trade-off between these three factors is very important. By data payload, we are talking about the amount of information (the number of bits). Fidelity describes the watermarking only allowed to change the carrier imperceptibly. The ability of watermark to remain unchanged against attack is called robustness (Doërr and Dugelay, 2003).

1.3 Issues

The main issue in watermarking with the purpose of copyright protection is the security. Robust watermarking creates a channel to communicate or store information inside the carrier. In order to copy control, this channel should be secure. In other words, the aim is preventing unauthorized user from detecting, adding, modifying or removing the watermark (Kalker, 2001). Moreover, the security is not limited to robustness only. Capacity, imperceptibility and prevailing design issues are also part of the security which has to be addressed (Li *et al.*, 2006).

Although video watermarking is based on the same techniques, applied on images but it has its very own issues. As videos usually have a bigger size in comparison with other media and they have inherent redundancy information which

is repeated between sequential frames, removal attacks still remains a big problem in video watermarking (Gosavi and Warnekar, 2010). Among these removal attacks, collusion attack is the trading one (ed eric Deguillaume *et al.*, 2012).

The next major issue in video copyright watermarking is the number of producers. Each of these producers needs a specific watermark to make sure of the owner identification and proofing.

1.4 Problem Statement

According to the CISCO's white paper, since 2011 video has the leading account for internet traffic usage. Moreover it is predicted that the 90% of the internet traffic will be video in three years (Cisco, 2011). Therefore, the copyright, which is currently main issue, probably gets worse. As the watermarking can address this issue, this project tries to design a new watermarking method based on the current methods in the way that the new method be able to improve copyright protection by enhancing the robustness against collusion attack.

Collusion attack is one of the major threats for copyright. In this attack, one or more colluders try to collect as many as possible watermarked material. Then by comparing these materials, it is possible to estimate the watermark. If the estimation is accurate enough a watermark removal can perform. This attack has a very close relation with the number of watermarked materials that are collected by colluders. By increasing the number of collected material, the possibility of the attack is also increases. Therefore, addressing the collusion attack by providing more robust watermarking methods, can improve the copyright protection.

1.5 Objectives

- To study following watermarking methods over video for copyright purposes:
  - Block Truncation Coding (BTC)
  - Singular Value Decomposition (SVD)
  - Discrete Wavelet Transform (DWT)
- To propose an enhanced robust model of digital video watermarking to address the collusion attack and eventually copyright protection.
- To evaluate proposed digital video watermarking method in terms of robustness against collusion attack.

1.6 Research question

- What are the current watermarking solutions for copyright protection of digital video?
- How it is possible to improve the copyright protection for digital video using watermarking?
- How to evidence the improvement and prove that the attack is disabled?

1.7 Project Aim

In this project, we try to compare three current main digital video watermarking for copyright protection methods in order to find out their characteristics, strengths and weaknesses. Then design an enhanced watermarking model for protecting copyright over digital video. Finally, evaluate the method to show the improvement.

1.8 Project Scope

- Limit the watermarking application to copyright protection.
- Using Matlab® IDE (one of the strongest tools in image processing) to implement the design.
- Limit the experiments to only H.264 video format.
- Assumes that the watermark is a 100*100 pixel black and with image.
- The watermark is the output of the watermark preparation instead of the original image since the compression method is loosy.
- Using Bit Error Rate (BER) to evaluate the robustness.
- Using Peak signal-to-noise ratio (PSNR) to evaluate the quality.
- Limit the evaluation to intra-video collusion in terms of attacks.
- The evaluation is based on Checkmark.

1.9 Expected Outcome

We expect to get to know BTC, SVD and DWT methods very well. Design an enhanced model for digital video watermarking for copyright protection. Then show the real improvement in terms of the targeted issues.

REFERENCES

Akiyama, T., Motoyoshi, F., Uchida, O., Nakanishi, S. and Goikoetxea, A. (2006). Hybrid Digital Watermarking for Color Images Based on Wavelet Transform,

Bangaleea, R. and Rughooputh, H. (2002). Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterisation, 293-298 vol. 291.

Barni, M., Bartolini, F., Caldelli, R., De Rosa, A. and Piva, A. (2000). A robust watermarking approach for raw video,

Bas, P. and Macq, B. (2001). A new video-object watermarking scheme robust to object manipulation, 526-529 vol. 522.

Behseta, S., Lam, C., Sutton, J. and Webb, R. (2009). A Time Series Intra-Video Collusion Attack on Frame-by-Frame Video Watermarking. *Digital Watermarking*, 31-44.

Bhatnagar, G. and Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces. 31*(5), 1002-1013.

Bhowmik, D. and Abhayaratne, C. (2012). 2D+ t Wavelet Domain Video Watermarking. *Advances in Multimedia. 2012*.

Boneh, D. and Shaw, J. (1998). Collusion-secure fingerprinting for digital data. *Information Theory, IEEE Transactions on. 44*(5), 1897-1905.

Bruce, A. M. (2001). A review of digital watermarking. *Department of Engineering, University of Aberdeen*.

Chang, X., Wang, W., Zhao, J. and Zhang, L. (2011). A survey of digital video watermarking, 61-65.

Chen, X. and Lian, S. (2011). On the Collusion-Resistance of the Fingerprinting Algorithm Based on Additive Watermarking. *Journal of Multimedia. 6*(4), 369-375.

Chen, Y. H. and Huang, H. C. (2010). A new shot-based video watermarking, 53-58.

Chetan, K. and Raghavendra, K. (2010). DWT Based Blind Digital Video Watermarking Scheme for Video Authentication. *International Journal of Computer Applications IJCA. 4*(10), 19-26.

Cisco (2011). *Forecast and Methodology, 2010–2015*: CISCO.

Craver, S., Memon, N., Yeo, B. L. and Yeung, M. M. (1998). Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications. *Selected Areas in Communications, IEEE Journal on. 16*(4), 573-586.

Craver, S. A., Memon, N. D., Yeo, B. L. and Yeung, M. M. (1997). Can invisible watermarks resolve rightful ownerships?, 310.

Doërr, G. and Dugelay, J. L. (2003). A guide tour of video watermarking. *Signal processing: Image communication. 18*(4), 263-282.

Du, J., Lee, C. H., Lee, H. K. and Suh, Y. (2002). BSS: A new approach for watermark attack, 182-187.

ed eric Deguillaume, F., Csurka, G. and Pun, T. (2012). Countermeasures for Unintentional and Intentional Video Watermarking Attacks.

El'Arbi, M., Koubaa, M., Charfeddine, M. and Ben Amar, C. (2011). A dynamic video watermarking algorithm in fast motion areas in the wavelet domain. *Multimedia Tools and Applications. 55*(3), 579-600.

Eskicioglu, A. M. and Delp, E. J. (2001). An overview of multimedia content protection in consumer electronics devices. *Signal Processing: Image Communication. 16*(7), 681-699.

Fu, D. and Wang, J. (2009). Based on H. 264 of the video watermarking technology. *Computer Applications. 29*(04), 1174 - 1176.

Fung, C. W. H. and Godoy Jr, W. (2011). A New Approach of DWT-SVD Video Watermarking, 233-236.

Ge, W. (2010). Collusion-resistant blind video watermarking based on H264, V11-19-V11-13.

Gosavi, C. S. and Warnekar, C. S. (2010). Study Of Multimedia Watermarking Techniques. *International Journal of Computer Science and Information Security. 8*, 64 - 72.

Havyarimana, V. and Li, Q. (2010). Efficient Anti-Scalable Anti-Collusion Fingerprinting. *International Journal of Advancements in Computing Technology. 3*(3), 40-48.

Healy, D. and Mitchell, O. (1981). Digital video bandwidth compression using block truncation coding. *Communications, IEEE Transactions on. 29*(12), 1809-1817.

Heider, D. and Barnekow, A. (2008). DNA watermarks: A proof of concept. *BMC Molecular Biology. 9*(1), 40.

Hernández, J. R. and Pérez-González, F. (1999). Statistical analysis of watermarking schemes for copyright protection of images. *Proceedings of the IEEE. 87*(7), 1142-1166.

Holliman, M. J., Macy, W. W. and Yeung, M. M. (2000). Robust frame-dependent video watermarking, 186.

Huang, C. H. and Wu, J. L. (2004). Attacking visible watermarking schemes. *Multimedia, IEEE Transactions on. 6*(1), 16-30.

Jayamalar, T. and Radha, V. (2010). Survey on Digital Video Watermarking Techniques and Attacks on Watermarks. *International Journal of Engineering Science and Technology. 2*(12), 6963-6967.

Kalker, T. (2001). Considerations on watermarking security. *IEEE Fourth Workshop on Multimedia Signal Processing*. Cannes , France, 201 - 206.

Kamlakar, M. A., Gosavi, C. S. and Patankar, A. J. (2012). Single Channel Watermarking For Video Using Block Based SVD. *International Journal of Advances in Computing and Information Researches. 1*(2), 1-5.

Kanocz, T., Tokar, T. and Levicky, D. (2009). Robust frame by frame video watermarking resistant against collusion attacks, 99-102.

Koubaa, M., Elarbi, M., Ben Amar, C. and Nicolas, H. (2012). Collusion, MPEG4 compression and frame dropping resistant video watermarking. *Multimedia Tools and Applications*, 1-21.

Lee, S.-J. and Jung, S.-H. (2001). A survey of watermarking techniques applied to multimedia. *Industrial Electronics, ISIE*. Pusan , South Korea, 272 - 277.

Li, Q., Memon, N. and Sencar, H. T. (2006). Security issues in watermarking applications - a deeper look. *MCPS '06 Proceedings of the 4th ACM international workshop on Contents protection and security*. New York, NY, USA, 23-28.

Lin, Y. W., Li, G. L., Chen, M. J., Yeh, C. H. and Huang, S. F. (2010). Repeat-Frame Selection Algorithm for Frame Rate Video Transcoding. *International Journal of Image Processing (IJIP). 3*(6), 341.

Ling, H., Lu, Z. and Zou, F. (2004). New real-time watermarking algorithm for compressed video in VLC domain, 2171-2174 Vol. 2174.

Liou, D. M., Huang, Y. and Reynolds, N. (1990). A new microcomputer based imaging system with C3 technique, 555-559 vol. 552.

Liu, R. and Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *Multimedia, IEEE Transactions on. 4*(1), 121-128.

Liu, T. and Qiu, Z. (2002). The survey of digital watermarking-based image authentication techniques, 1556-1559 vol. 1552.

Liu, T., Zhang, H. J. and Qi, F. (2003). A novel video key-frame-extraction algorithm based on perceived motion energy model. *Circuits and Systems for Video Technology, IEEE Transactions on. 13*(10), 1006-1013.

Lu, W., Sun, W. and Lu, H. (2011). Novel robust image watermarking based on subsampling and DWT. *Multimedia Tools and Applications*, 1-16.

Maity, S., Sil, J., Maity, S. P. and Delpha, C. (2011). Optimized spread spectrum watermarking for fading-like collusion attack, 1-5.

Maity, S. P., Maity, S., Sil, J. and Delpha, C. (2012). Collusion Resilient Spread Spectrum Watermarking in M-band Wavelets using GA-Fuzzy Hybridization. *Journal of Systems and Software*.

Meerwald, P. and Uhl, A. (2008). Blind motion-compensated video watermarking, 357-360.

Miyazaki, A. and Okamoto, A. (2001). Analysis of watermarking systems in the frequency domain and its application to design of robust watermarking systems, 506-509 vol. 502.

Mohammed, A. A. and Hussein, J. A. (2009). Efficient Video Watermarking Using Motion Estimation Approach, 593-598.

Niu, K., Yang, X. and Xiang, L. (2010). Hybrid quasi-3d dwt/dct and svd video watermarking, 588-591.

Omidyeganeh, M., Khalilian, H., Ghaemmaghami, S. and Shirmohammadi, S. (2010). Robust digital video watermarking in an orthogonal parametric space, 2258-2263.

PAN, J. S., HUANG, H. C., Jain, L. C. and ZHAO, Y. (2012). Recent advances in information hiding and applications.

Pei, W., Zhendong, Z. and Li, L. (2008). A video watermarking scheme based on motion vectors and mode selection, 233-237.

Piva, A., Bartolini, F. and Barni, M. (2002). Managing copyright in open networks. *Internet Computing, IEEE. 6*(3), 18-26.

Piva, A., Caldelli, R. and De Rosa, A. (2000). A DWT-based object watermarking system for MPEG-4 video streams, 5-8 vol. 3.

Polikar, R. (1999). The story of wavelets. *Physics and modern topics in mechanical and electrical engineering*, 192-197.

Potdar, V. M., Han, S. and Chang, E. (2005). A Survey of Digital Image Watermarking Techniques. *IEEE International Conference on Industrial Informatics (INDIN)*, 709 - 716.

Preda, R. O., Oprea, C., Pirnog, I. and Perişoară, L. A. (2012). Robust Digital Video Watermarking in the Spatial and Wavelet Domain, 78-83.

Qiao, L. and Nahrstedt, K. (1998). Watermarking methods for MPEG encoded video: Towards resolving rightful ownership, 276-285.

Rajab, L., Al-Khatib, T. and Al-Haj, A. (2008). Hybrid dwt-svd video watermarking, 588-592.

Reyes, R., Cruz, C., Nakano, M. and Pérez, H. (2008). Video Watermarking Algorithm Resilient to MPEG-2 Compression and Collusion Attacks.

Sherekar, S., Thakare, V. and Jain, S. (2008). Role of Digital Watermark in e-governance and e-commerce. *International Journal of Computer Science and Network Security. 8*(1), 257-261.

Sherekar, S., Thakare, V. and Jain, S. (2009). Critical Review of Perceptual Models for Data Authentication, 323-329.

Sherekar, S., Thakare, V., Jain, S., Miss Ashwini, D. B., Tijare, P., Deshpande, M. S. A., Boob, M. A. N., Dakhane, D., Mapari, N. and Telang, A. (2011). Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks. *International Journal Of Computer Science And Applications. 4*(2).

Singh, P. and Sharma, N. S. (2012). A COMPARATIVE STUDY: BLOCK TRUNCATION CODING, WAVELET, EMBEDDED ZEROTREE AND FRACTAL IMAGE COMPRESSION ON COLOR IMAGE. *International journal of Electronics*.

TU, S.-F. and HSU, C.-S. (2004). A BTC-based watermarking scheme for digital images. *Information & Security. 15*(2), 216 - 228.

Ujwala, B. and Chetan, K. (2010). An efficient DCT based fingerprinting scheme for thwarting collusion attacks, 1-6.

Voloshynovskiy, S., Pereira, S., Iquise, V. and Pun, T. (2001). Attack modelling: towards a second generation watermarking benchmark. *Signal processing. 81*(6), 1177-1214.

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J. and Su, J. K. (2001). Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *Communications Magazine, IEEE. 39*(8), 118-126.

Voyatzis, G. and Pitas, I. (1999). The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE. 87*(7), 1197-1207.

Wall, M., Rechtsteiner, A. and Rocha, L. (2003). Singular value decomposition and principal component analysis. *A practical approach to microarray data analysis*, 91-109.

Wang, C. X., Nie, X., Wan, X., Wan, W. B. and Chao, F. (2009). A Blind Video Watermarking Scheme Based on DWT, 434-437.

Wayner, P. (2009). *Disappearing cryptography: Information hiding: Steganography & watermarking*. (3rd ed.). Burlington, MA: Morgan Kaufmann.

Wong, W. and Delp, E. J. (2000). Security and Watermarking of Multimedia Content. *Eds.SPIE*. San Jose, CA,

Wu, D., Kong, W., Yang, B. and Niu, X. (2009). A fast SVD based video watermarking algorithm compatible with MPEG2 Standard. *Soft Computing-A Fusion of Foundations, Methodologies and Applications. 13*(4), 375-382.

Yang, P., Yang, L. Y. and Zhang, Y. J. (2011). Research of Digital Watermarking Algorithm Based on SVD and DWT. *Applied Mechanics and Materials. 65*, 385-388.

Yongliang, L., Gao, W. and Liu, S. (2004). Secure watermark detection schemes, 631-633 vol. 632.

Yongliang, L., Gao, W., Yao, H. and Song, Y. (2002). Secure watermark verification scheme. *Advances in Multimedia Information Processing—PCM 2002*, 477-484.

Zeng, W. and Liu, B. (1999). A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. *Image Processing, IEEE Transactions on. 8*(11), 1534-1548.

Zhang, X. and Guo, L. (2010). Research and design of video watermarking DCT algorithm based on MPEG-4 compressed domain, 319-322.

Zhao, H., Wu, M., Wang, Z. J. and Liu, K. J. R. (2003). Nonlinear collusion attacks on independent fingerprints for multimedia, V-664-667 vol. 665.

Zhou, H., Xu, T. and Wu, X. (2006). Resist the collusion attack of a digital video watermarking algorithm. *Computer Applications. 26*(04), 812 - 814.