A SEED GENERATION TECHNIQUE BASED ON ELLIPTIC CURVE FOR PROVIDING SYNCHRONIZATION IN SECUERED IMMERSIVE TELECONFERENCING

VAHIDREZA KHOUBIARI

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

I dedicate my thesis to my family. A special feeling of thankfulness to my loving wife, “Sara” whose without her help and patience this work could not be done. To my parents whose words of inspiration and push for endurance ring in my ears.

ACKNOWLEDGEMENT

I would like to truly appreciate **Associate Prof. Dr. Mazleena Salleh** for taking the time out of her busy schedule to encourage and guide me through this project. Her deep knowledge and valuable experience inspired me and illuminated my path. Also I would like to thank **Dr. Majid Bakhtiari** for his great advices and technical points that he gave me without any expectation.

Beside I should be appreciative of authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and creative area.

ABSTRACT

Immersive Teleconferencing as one of the new progresses in video-conferencing allows users to see multiple partners in the conference simultaneously or watch a single event from different views. H.264/MVC standard provides a well-defined structure for implementing immersive teleconferencing that can merge pictures taken by several cameras into a single video stream at the encoder side and also show the encoded video stream from different views at the decoder side. For confidential and top secret circumstances like governmental, military and medical cases keeping the contents of conversations hidden from adversaries is critical. Therefore for these applications video content encryption is necessary. The encryption scheme used for video-conferencing besides high perceptual security must have suitable synchronization performance between two parties due to used key stream especially in noisy transmission environments. The problem with existing techniques is that their seed generations have no synchronization mechanism or they add the encrypted seed or its hash value to the bitstream as synchronization control information. To overcome the issue this study recommends a seed generation technique based on points located on elliptic curve to provide synchronization between teleconferencing parties due to applied key stream. The work proved that points located on elliptic curve have proper randomness characteristics to offer the appropriate security property. The results show that the proposed technique performs better synchronization in secured environment than current seed generation techniques.

ABSTRAK

Immersive Teleconferencing merupakan salah satu pembaharuan dalam persidangan video yang membolehkan para pengguna melihat beberapa rakan mereka di dalam satu persidangan secara serentak atau menonton sesuatu rancangan dengan menggunakan pandangan yang berbeza. Piawai H.264/MVC yang digunakan menyediakan struktur yang jelas untuk melaksanakan *Immersive Teleconferencing* membolehkan video yang diambil dari beberapa kamera digabungkan menjadi satu strim video di bahagian pengekod. Strim video yang telah dikodkan akan dipisahkan semula untuk menjadi satu pandangan yang berbeza di bahagian penyahkod. Untuk penggunaan yang sulit atau rahsia seperti dalam transaksi kerajaan, tentera mahupun perubatan, kandungan video perlu disembunyikan dari pihak musuh dan ini akan tercapai dengan penggunaan teknik penyulitan. Selain dari keperluan kawalan keselamatan yang tinggi dalam persidangan video, skema penyulitan yang digunakan juga mesti mempunyai prestasi sinkronisasi yang sesuai kerana penggunaan strim kekunci dan terutama sekali dalam talian penghantaran yang mempunyai hingar yang tinggi. Masalah dengan teknik yang sedia ada ialah ia tidak disokong dengan penjanaan benih yang mempunyai mekanisma sinkronisasi atau jika ada pun, nilai benih tersulit atau nilai cincangannya akan dihantar bersama strim bit sebagai kawalan maklumat sinkroni. Untuk mengatasi masalah tersebut, kajian ini mencadangkan teknik pembenihan berdasarkan titik-titik yang terletak pada lengkuk eliptik bagi menyokong penyelarasan diantara pihak-pihak yang bersidang. Kajian ini telah membuktikan bahawa titik-titik yang terletak pada lengkuk eliptik mempunyai ciri kerawakkan yang sesuai untuk keselamatan. Keputusan kajian menunjukkan bahawa teknik yang dicadangkan mempunyai prestasi yang lebih baik dari teknik yang sedia ada dari segi sinkronisasi dalam persekitaraan terselamat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

4CIF	4× CIF
AES	Advanced Encryption Standard
ATSC	Advanced Television Systems Committee
AVC	Advanced Video Coding
CABAC	Context-Adaptive Binary Arithmetic Coding
CAVLC	Context-Adaptive Variable-Length Coding
CBC	Cipher Block Chaining
CCR	Changed Compression Ratio
CFB	Cipher Feedback
CIF	Common Intermediate Format
CSPRNG	Cryptographically Secured Pseudo Random Number Generator
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DID	Dependency ID
DVB-C	Digital Video Broadcasting - Cable
DVB-S	Digital Video Broadcasting - Satellite
DVB-S2	Digital Video Broadcasting - Satellite - Second Generation
DVB-T	Digital Video Broadcasting - Terrestrial
DVB-T2	Digital Video Broadcasting – Terrestrial - Second Generation
DVD	Digital Versatile Disc
EBU	European Broadcasting Union

ECB	Electronic Codebook
ETR	Encryption Time Ratio
GOP	Group Of Pictures
HD	High-Definition Video
HDTV	High-Definition Television
HVS	Human Visual System
IEC	International Electrotechnical Commission
IPM	Intra Prediction Mode
ISDB-T	Integrated Services Digital Broadcasting-Terrestrial
ISO	International Organization for Standardization
ITU-R	International Telecommunication UnionRadiocommunication Sector
ITU-T	International Telecommunication UnionTelecommunication Standardization Sector
IV	Initial Vector
JMVC	Joint Multiview Video Coding
MPEG	Moving Expert Picture Group
MV	Motion Vector
MVC	Multiview Video Coding
MVD	Motion Vector Difference
NAL	Network Abstraction Layer
NALU	Network Abstraction Layer Unit
NIST	National Institute of Standards and Technology
NTSC	National Television System Committee
NUT	Network Abstraction Layer Unit Type
PAL	Phase Alternating Line
PPS	Picture Parameter Sets
PSNR	Peak Signal-to-Noise Ratio
QCIF	Quarter CIF

QID	Quality ID
QP	Quantization Parameter
SD	Standard Definition
SECAM	SéquentielCouleur À Mémoire(Sequential Color with Memory)
SNR	Signal-to-Noise Ratio
SPS	Sequence Parameter Sets
SVC	Scalable Video Coding
TID	Temporal ID
URL	Uniform Resource Locator
VCEG	Video Coding Experts Group
VCL	Video Coding Layer

LIST OF APPENDIX

CHAPTER 1

INTRODUCTION

1.1 Introduction

Video-conferencing has become one of the favorite communication technologies in recent years especially by increasing the popularity and bandwidth of internet connection around the world. One of the new progresses in this area is Immersive Teleconferencing. Immersive Teleconferencing allows users to see multiple partners in the conference simultaneously or watch a unique event from different views. For confidential and top secret cases like governmental, military and medical cases keeping the contents of conversations hidden from adversaries is critical, though it is necessary to encrypt them. Therefore the security of the applied encryption technique should be high enough while imposing low encryption overhead to the video stream to avoid packet size increasing in the transmission. One of the issues in this subject is synchronization between two parties especially in lossy or noisy environments which causes packet-error and packet-loss during transmission.

Rest of this chapter contains the problem background, problems statement, scope and objectives of the research.

1.2 Background of the Problem

ITU-T Video Coding Expert Groups (VCEG) and ISO/IEC joint working group, Moving Expert Picture Group (MPEG), developed the H.264/MPEG-4 AVC standard as a well-defined structure codec (ITU-T recommendation for H.264, series h). H.264/AVC converts the video source to a series of blocks which are compressed based on dependencies between pixels in a frame and pixels between other frames and also motion prediction. It has a wide range of coverage from low-bit to high definition formats and is widely used in digital TV, Blue-ray Discs, You-Tube, Mobile TV, Adobe Flash Player, videoconferencing, Microsoft Silverlight, online video streaming, terrestrial HDTV, satellite HDTV and etc. (Richardson, 2010).

Later ITU-T and ISO/IEC joint group developed a scalable extension for H.264/AVC which is called Scalable Video Coding (ITU-T recommendation for H.264, series h). SVC adds subset bitstreams to AVC that present different scalability based on users' hardware and network bandwidth. This scalability could be temporal (frame rate), spatial (resolution) and/or SNR (quality) (Schwarz, Marpe and Wiegand, 2007).

Recently ITU-T and ISO/IEC joint group developed Multiview Video Coding (MVC) as another extension of H.264/MPEG-4 AVC (ITU-T recommendation for H.264, series h). Like SVC, MVC adds subset bitstreams to AVC that present different views on a unique video stream. These views could be from a same scene/object or from different scenes or objects. It can be used for applications such as 3D video application, free-viewpoint video, immersive teleconferencing (Vetro, Wiegand and Sullivan, 2011).

Different encryption schemes based on H.264/AVC and/or SVC standard have been proposed to provide security for video bitstream (Stütz and Uhl, 2012). These encryption schemes can be categorized as:

i. Before Compression Encryption
ii. Compression Integrated Encryption
iii. Bitstream Encryption

Before Compression Encryption schemes encrypt the whole video stream, and then the encoder starts to compress the encrypted bitstream. The compression procedures of encoders are based on the relationship between adjacent blocks of each frame and also relationship between different frames. Encrypting the bitstream before compression disturbs these relationships and has a great negative influence on compression performance. Therefore this kind of encryption is suitable for hiding especial part of the video and is not appropriate to apply to the whole bitstream (Carrillo, Kalva, and Magliveras, 2008). Accordingly this kind of encryption is not suitable for real-time video applications like video-conferencing.

Compression Integrated Encryption schemes are applied to the video stream while encoder is compressing the original bitstream. There are eight kinds of compression integrated encryption scheme: Intra-Prediction, Inter-Prediction, Motion Vector, Secret Transform, DCT Coefficient, Secret Scan Order, Joint Encryption and CAVLC and Joint Encryption and CABAC. Bitstream or After Compression Encryptionschemes are applied to the compressed video stream after encoding. There are three kinds of bitstream encryption scheme: NALU Encryption, Container-Formats and Partial/Selective Encryption (Stützand Uhl, 2012). Different techniques for mentioned encryption scheme kinds have been proposed.

Several encryption performance evaluation parameters for multimedia encryption have been proposed and discussed comprehensively by (Lian, 2009). These parameters are: Security Requirement, Compression Efficiency and Encryption Efficiency which are discussed in Chapter 2. Synchronization performance in lossly or noisy transmission environments also can be added to above list especially for real-time video streaming applications like teleconferencing.

The proposed During Compression or After Compression encryption techniques for real-time application have some weaknesses in synchronization performance in lossy or noisy environments. Some techniques suggest using a unique key for the whole conversation to avoid losing synchronization. Using only one key makes the cipher vulnerable against some attacks such as known plaintext and chosen plaintext (Boztok Algin and Tunali, 2011). Some techniques send the encryption seed/key or its hash value for each group of packets to maintain synchronization during transmission. These methods do not have sufficient resilience against high lossy networks and also impose overhead to the bitstream (Boztok Algin and Tunali, 2011).

Immersive teleconferencing allows the user to see multiple partners simultaneously as shown in Figure 1.1. Pictures taken by multiple cameras are merged together by encoder and sent as a unique bitstream to the other side via network. In the other side the decoder separates the bitstream to multiple views. In some cases of immersive teleconferencing application such as governmental, military, medical and secret business conferencing, security and keeping the contents of conversation confidential is very important. H.264/MVC is one of the progressive standards for immersive teleconferencing applications development. In MVC different pictures from different cameras joint with each other and make a single bitstream. Therefore the size of the bitstream for a particular duration may be far bigger than AVC or even SVC, though a lightweight encryption scheme with very high security is needed. Because for a fraction of time there are more frames in a MVC bitstream than AVC or SVC's, the scheme should not impose a high level of overhead to the bitstream. Also both sides of conversation should be able to synchronize with each other in case of packet-error or packet-loss especially in lossy or noisy environment. The existing schemes for real-time AVC and SVC video encryption have some weaknesses in synchronization performance.

Therefore a research needs to propose a synchronization technique for real-time MVC video that can cover the issue.

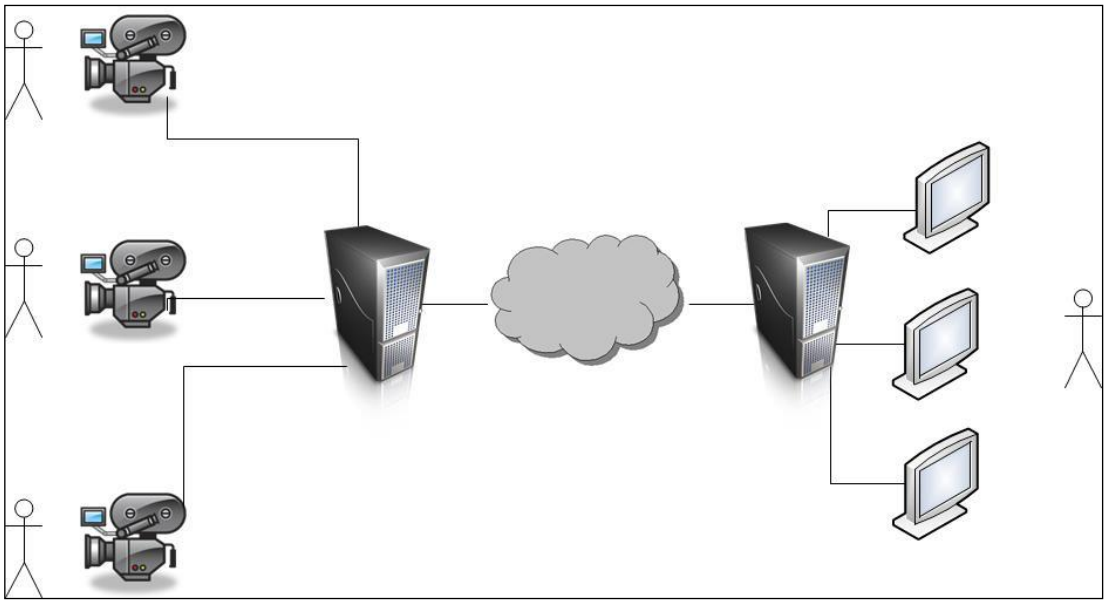

Figure 1.1: Immersive Teleconferencing

1.3 Statement of the Problem

In some cases of real-time video streaming based on H.264/MVC like confidential immersive teleconferencing hiding the video contents from adversary is critical. The existing schemes for H.264 extensions encryption have some weaknesses for real-time cases. These schemes do not have suitable synchronization performance in lossy or noisy transmission media (Mian, Jia and Lei, 2007). Even though these schemes have this performance they either impose significant overhead to the bitstream (Won, Bae and Ro, 2006) or reduce the security level (Wei *et al*., 2012).

1.4 Research Questions

This study will answer to the following questions:

i. What parameters are required to have a synchronization performance in secured real time video application?
ii. How could be an enhanced seed generation scheme that has suitable synchronization performance?

1.5 Purpose of the Study

The purpose of this study is to propose a seed generation and sharing scheme for multimedia encryption based on MVC extension of H.264 standard for immersive teleconferencing. This research proposes a seed generation and sharing scheme to have suitable synchronization performance in noisy or lossy environments while preserving the security of encryption with low encryption overhead imposition. Moreover this research compares existing real-time encryption schemes for H.264/AVC and SVC with the recommended scheme in terms of synchronization performance.

1.6 Objectives of the Study

Here are the objectives of the study:

i. To study the synchronization performance of current multimedia encryption schemes based on H.264/AVC and SVC for real-time applications.

ii. To propose and implement a seed generation scheme based on H.264/MVC to cover the current weaknesses in synchronization performance for real-time application.

iii. To validate and evaluate synchronization performance based on the proposed seed generation scheme.

1.7 Scope of the Study

This research presents the requirement and technical points of view of a seed generation and sharing technique for immersive teleconferencing encryption and outlines the implementation of this scheme with following specifications:

i. The technique is based on the MVC extension of H.264 standard.

ii. The technique is for peer-to-peer teleconferencing.

iii. The software program which is used in this research is designed with Microsoft Visual Studio C++.

iv. JMVC (Joint Multiview Video Coding) reference program willbeused for some security performance parameters evaluation.

1.8 Significance of the Study

This study proposes a seed generation and sharing scheme for Multiview Video Coding (MVC) extension of H.264 standard that could be used for immersive teleconferencing, either for communicating with multiple partners simultaneously or watching an event from different views. It could be a secured scheme with low encryption overhead while having suitable synchronization performance for lossy or noisy transmission media.

The scheme may be used for confidential and top secret immersive teleconferencing such as governmental, military or medical cases.

1.9 Thesis Organization

This chapter gives a brief overview of the problem background and scope of this study. In Chapter 2 first essential definitions for video coding and history of H.264 AVC, SVC and MVC will be discussed. Then different method of multimedia encryption and the parameters to evaluate them and different related works including their weaknesses with respect to synchronization will be proposed. The research methodology for this study will be proposed in Chapter 3. Chapter 4 includes design while Chapter 5 consists of implementation, results and for the proposed technique. Chapter 6 concludes the project.

REFERENCES

Arachchi, H. K., Perramon, X., Dogan, S. and Kondoz, A. M., 2009, *Adaptation–Aware Encryption of Scalable H.264/AVC Video for Content Security*, Signal Processing: Image Communication, 24(6), 468-483.

Bergeron, C. and Lamy-Bergor, C., 2005, *Compliant Selective Encryption For H.264/Avc Video Streams*, In Proceedings of the IEEE Workshop on Multimedia Signal Processing, MMSP'05, pages 1–4, October 2005.

Box, G. E., Jenkins, G. M. and Reinsel, G. C., 2011, *Time Series Analysis: Forecasting and Control*, (Vol. 734), Wiley.

Boztok Algin, G. and Tunali, E. T., 2011, *Scalable Video Encryption of H. 264 SVC Codec*, Journal of Visual Communication and Image Representation, 22(4), 353-364.

Carrillo, P., Kalva, H., and Magliveras, S., 2008, *Compression Independent Object Encryption for Ensuring Privacy in Video Surveillance*. In Proceedings of International Conference on Multimedia & Expo, ICME'08, pages 273–276. IEEE, June 2008.

Dufaux, F. and Ebrahimi, T., 2008, *H.264/Avc Video Scrambling for Privacy Protection*, In Proceedings of the IEEE International Conference on Image Processing, ICIP '08, San Diego, CA, USA, October 2008.

Engel, D., Stütz, T. and Uhl, A., 2009, *A Survey on JPEG2000 Encryption.* Multimedia Systems, 15(4):243–270, 2009.

European Broadcasting Union (EBU) Technical Report 3299, 2004, *High Definition Image Formats for Television Broadcasting*, Geneva, 2004.

Forouzan, B. A., 2007, *Cryptography & Network Security*, McGraw-Hill, Inc..

Hai-Wei, S. and Jin-Ping, L., 2009, *A Novel Stream Cipher for Video Compressed by H. 264*, In Computer Science-Technology and Applications, IFCSTA'09. International Forum on (Vol. 2, pp. 54-56), IEEE.

Hellwagner, H., Kuschnig, R., Stütz, T. and Uhl, A., 2009, *Efficient In-Network Adaptation of Encrypted H.264/Svc Content*, Elsevier Journal on Signal Processing: Image Communication, 24(9):740 – 758, July 2009.

Iqbal, R., Shirmohammadi, S., Saddik, A. and Zhao, J.,2008, *Compressed-Domain Video Processing for Adaptation, Encryption, and Authentication*. IEEE Multimedia, 15(2):38–50, April 2008.

Iqbal, R., Shirmohammadi, S., Saddik, A., 2007, *A Framework for MPEG-21 DIA Based Adaptation and Perceptual Encryption of H.264 Video*. In Roger Zimmermann, and Carsten Griwodz,editors, Proceedings of SPIE, Multimedia Computing and Networking 2007, volume 6504. SPIE, 2007.

Iqbal, R., Shirmohammadi, S., Saddik, A., 2006, *Secured MPEG-21 Digital Item Adaptation for H.264 Video*. In Proceedings of International Conference on Multimedia & Expo, ICME ’06, pages 2181–2184, Toronto, Canada, July 2006, IEEE.

ITU-T, Joint Collaborative Team on Video Coding - JCT-VC, Available at: http://www.itu.int/ITU-T/studygroups/com16/jct-vc/ [Accessed Sep. 2012]

ITU-T, Telecommunication Standardization Sector of ITU, 2012, *Series H: Audiovisual and Multimedia Systems, Infrastructure of Audiovisual Services – Coding of Moving Video*, Advanced Video Coding for Generic Audiovisual Services, Recommendation ITU-T H.264 (Jan. 2012).

Kapotas, S. K. and Skodras, A. N., 2010, *Rate Control of H.264 Encoded Sequences by Dropping Frames in the Compressed Domain*, IEEE 20th International Conference on Pattern Recognition (ICPR)

Kodikara Arachchi, H., Perramon, X., Dogan, S. and Kondoz, A.M., 2009, *Adaptation-Aware Encryption of Scalable H.264/Avc Video for Content Security*. Signal Processing: Image Communication, 24(6):468–483,2009. Scalable Coded Media beyond Compression.

Lei, B. Y., Lo, K. T. and Lei, H., 2010, *A New H.264 Video Encryption Scheme Based on Chaotic Cipher*. In Communications, Circuits and Systems (ICCCAS), 2010 International Conference on (pp. 373-377).IEEE.

Li C., Yuan, C. and Zhong, Y., 2009, *Layered Encryption for Scalable Video Coding*, 978-1-4244-4131-0/09/, IEEE.

Li, Y., Liang, L., Su, Z. and Jiang, J., 2005, *A New Video Encryption Algorithm for H.264*, In Proceedings of the Fifth International Conference on Information, Communications and Signal Processing, ICICS'05, pages 1121– 1124. IEEE, December 2005.

Lian, Sh., 2009, *Multimedia Content Encryption: Techniques and Application*, 1st ed., Taylor and Francis Group, Boca Raton. London, New York, 2009.

Lian, S., Sun, J., Liu, G. and Wang, Z., 2008, *Efficient Video Encryption Scheme Based on Advanced Video Coding*, Multimedia Tools and Applications, 38(1):75–89, March 2008.

Lian, S., Liu Z., Ren, Z. and Wang, H., 2006, *Secure Advanced Video Coding Based on Selective Encryption Algorithms*, IEEE Transactions on Consumer Electronics, 52(2):621–629, 2006.

Lian, S., Liu, Z., Ren, Z. and Wang, Z., 2005, *Selective Video Encryption Based on Advanced Video Coding*, In Proceedings of the Pacific-Rim Conference on Multimedia, Advances in Multimedia Information Processing, PCM '05, volume 3768 of Lecture Notes in Computer Science, pages 281–290. Springer, 2005.

Majumder, A., Gopi, M., Seales, B., & Fuchs, H., 1999, *Immersive Teleconferencing: A New Algorithm to Generate Seamless Panoramic Video Imagery*. In Proceedings of the seventh ACM international conference on Multimedia, pp. 169–178.

Marion, A., 1991, *An Introduction to Image Processing. London*, Chapman and Hall.

Mian, C., Jia, J. and Lei, Y., 2007, *An H.264 Video Encryption Algorithm Based on Entropy Coding*. In Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing, IIH-MSP'07, pages 41–44, Washington, DC, USA, 2007. IEEE Computer Society.

Park, S.W. and Shin, S.U., 2008, *Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding (SVC)*, NCM 2008, Sept. 2008, pp. 371-376.

Recommendation ITU-T H.264 | ISO/IEC 14496-10:2009, *Advanced Video Coding for Generic Audio-Visual Services*, March 2009.

Richardson, I. E., 2010, *The H.264 Advanced Video Compression Standard*, Wiley, Second Edition.

Schwarz, H., Marpe, D. and Wiegand, T., 2007, *Overview of the Scalable Video Coding Extension of the H.264/AVC Standard*, IEEE Transactions on Circuits and Systems for Video Technology

Shah, J. and Saxena, V., 2011, *Video Encryption: A Survey*, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011

Shahid, Z., Chaumont, M. and Puech, W, 2009,*Fast Protection of H.264/AVC by Selective Encryption of CABAC*, In Proceedings of the IEEE International Conference on Multimedia & Expo, ICME '09, Cancun, Mexico, June 2009.

Shannon, C. E., 1949, *Communication Theory of Secrecy Systems*, Bell Syst. Tech. J. 28, 656–715 (1949).

Shparlinski, I. E., 2009, *Pseudorandom Number Generators from Elliptic Curves*, Recent Trends in Cryptography: UIMP-RSME Santaló Summer School, July 11-15, 2005, Universidad Internacional Menéndez Pelayo, Santander, Spain, 477.

Spinsante, S., Chiaraluce, F. and Gambi, E., 2005, *Masking Video Information by Partial Encryption of H.264/AVC Coding Parameters*, In Proceedings of the 13th European Signal Processing Conference, EUSIPCO'05. EURASIP, September 2005.

Stütz, T. and Uhl, A., 2008, *Format-Compliant Encryption of H.264/AVC and SVC*, Tenth IEEE International Symposium on Multimedia

Stütz, T. and Uhl, A., 2012, *A Survey of H.264 AVC/SVC Encryption*, IEEE Transactions on Circuits and Systems for Video Technology, March 2012

Su, P., Hsu, C. and Wu, C., 2010, *A Practical Design Of Content Protection For H.264/AVC Compressed Videos By Selective Encryption And Fingerprinting*, Multimedia Tools and Applications, January 2010.

Thomas, T., Bull, D. and Redmill, D., 2009, *A Novel H.264 Svc Encryption Scheme for Secure Bit-Rate Transcoding*, In Proceedings of15the Picture Coding Symposium, PCS'09, Chicago, IL, USA, May 2009.IEEE.

Tong, L., Dai, F., Zhang, Y. and Li, J., 2010, *Prediction Restricted H.264/AVC Video Scrambling for Privacy Protection*. Electronic Letters, 46(1):47–49, January 2010.

Varlakshmi, L. M., Sudha, G., and Jaikishan, G., 2012,*An Efficient Scalable Video Encryption Scheme for Real time applications,* Procedia Engineering, 30, 852-860.

Vetro, A., Wiegand, T. and Sullivan, G. J., 2011, *Overview of the Stereo and Multiview Video Coding Extensions of the H.264/MPEG-4 AVC Standard.* Proceeding of the IEEE, Vol. 99, No. 4, April 2011

Voydock, V. L. and Kent, S. T., 1983, *Security Mechanisms in High-Level Network Protocols*. ACM Computing Surveys (CSUR), 15(2), 135-171.

Watkinson, J., 2012, *The MPEG Handbook,* Elsevier.

Wei, Z., Wu, Y., Ding, X. and Deng, R. H., 2012, *A Scalable and Format-Compliant Encryption Scheme for H.264/Svc Bitstreams*, Signal Processing: Image Communication Volume 27, Issue 9, October 2012, Pages 1011‑1024

Wiegand, T., Sullivan G. J., Bjontegaard, G. and Luthra, A., 2003, *Overview of the H.264/Avc Video Coding Standard*, IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 7, pp. 560–576.

Wikipedia, 2012, *Peak Signal-to-Noise Ratio (PSNR),* Available at:http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio [Accessed Sep. 2012]

Won, Y. G., Bae, T. M. and Ro, Y. M., 2006, *Scalable Protection and Access Control in Full Scalable Video Coding*, Springer-Verlag Berlin Heidelberg

Yeung, S. A., Zhu, S. and Zeng, B., 2009, *Partial Video Encryption Based on Alternating Transforms*, IEEE Signal Processing Letters, 16(10):893–896, October 2009.

Zou, D. and Bloom, J., 2010,*H.264 Stream Replacement Watermarking with CABAC Encoding,* In Proceedings of the IEEE International Conferenceon Multimedia and Expo, ICME ’10, Singapore, July 2010.