Visuelle Evaluierung, Skalierung und Transport von sicheren Videos*

Heinz Hofbauer

Fachbereich Computerwissenschaften
Universität Salzburg
hhofbaue@cosy.sbg.ac.at

Abstract: Diese Kurzfassung der Dissertation gibt eine Stand-der-Technik-Analyse eines effizienten Video-on-Demand Systems. Unter effizient verstehen wir in diesem Zusammenhang einerseits die Optimierung des Speicherverbrauchs am Server als auch die Minimierung von Verzögerungen beim Ausliefern an Verbraucher, die durch Skalierung und Verschlüsselung des Videomaterials zur sicheren Übertragung entstehen. Zusätzlich stellen wir theoretische und praktische Überlegungen an, wie man ein effizientes und sicheres System mittels Wavelet-basierter Videocodecs verwirklichen kann.

1 Einleitung

Durch die weite Verbreitung von Breitbandinternet im Heim und im mobilen Bereich werden *Video-on-Demand* (VoD) und Streamingsysteme immer beliebter. Konsumenten von VoD wollen diese Systeme überall nutzen, Stichwort "ubiquitous computing", von Smartphones mittels 3G-Verbindung bis zu Heimkinosystemen über Breitbandinternet. Dies verlangt von VoD-Anbietern dass Videos in diverser Form gespeichert werden, also in verschiedener Auflösung und Qualität, angepasst an das jeweilige Endgerät und die mögliche Verbindungsgeschwindigkeit. In weiterer Folge bedeutet das einen gesteigerten Speicherverbrauch und damit höhere Kosten für Anbieter.
Für dieses Problem gibt es eine Lösung, den *Universal Multimedia Access* (UMA), [VCE03]. Gemeint ist damit, dass ein Video auf eine Art gespeichert wird, die eine Adaption an die eventuellen Anforderungen eines Benutzers aus dem gleichen Quellmaterial erlaubt. Damit wird der benötigte Speicherbedarf gesenkt und die Möglichkeit gewährleistet, auf neue Anforderungen einzugehen die im Ursprungssystem nicht vorgesehen waren.
Der Nachteil dieser Systeme ist die benötigte Rechenleistung zur Adaption der Videos. Allerdings führt dies nicht zu einem Flaschenhals beim Anbieter, da moderne Netzwerktechnologien erlauben, diese Adaption *Just-in-Time* (JIT), also erst an der letztmöglichen Stelle im Netzwerk, zu erledigen. Durch diese *multimedia aware network elements* (MANE), [KKRH08], ist theoretisch sogar eine Einsparung der Bandbreite beim Anbieter möglich, da verschiedene Endnutzer mit einem einzigen Strom seitens des Anbieters bedient werden

*Englischer Titel der Dissertation "Visual Evaluation, Scaling and Transport of Secure Videos" [Hof13]

können, indem die Adaption JIT im Netzwerk ausgeführt wird.

Waveletbasierte Video Codecs sind durch ihre inhärente Skalierbarkeit gut für diese Anwendung geeignet und bieten die gleiche Qualität wie herkömmliche Video-Codecs. Der *Motion Compensated Embedded Zero Bit Codec* (MC-EZBC), [CW04, WGW04], ist ein moderner Video-Codec der auf Wavelets basiert und damit den Anforderungen von UMA grundsätzlich genügt.
Die Lösung für das UMA-Problem einfach einen Waveletbasierten Codec zu verwenden klingt offensichtlich, wird aber vorerst dadurch verhindert, dass MANEs und die dazugehörigen Netzwerkprotokolle nur standardisierte Formate, nämlich H.264, verstehen. Zusätzlich wollen Anbieter von VoD Systemen auf eine sichere Art mit ihren Endnutzern kommunizieren, um Piraterie zu vermeiden, was eine JIT-Skalierung im Netzwerk ausschließt, da die MANEs vollen Zugriff auf das übertragene Video zur Adaption benötigen.

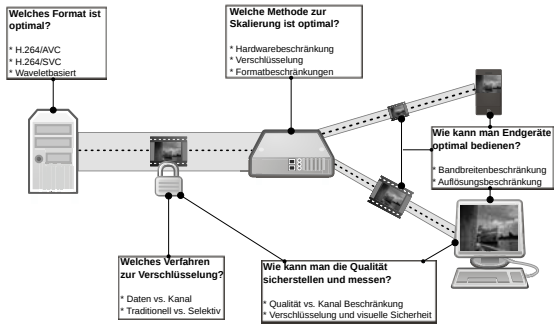

Abbildung 1: Übersicht über ein VoD-Setup mit Darstellung der Fragestellungen (und Probleme), die in einem solchen System auftreten.

In der kumulativen Dissertation geht es also darum, folgende Probleme (siehe auch Abb. 1) zu lösen: Es muss gewährleistet werden, dass MC-EZBC Videoströme über die existierenden Transporttechnologien übertragen werden können; Es müssen Methoden zur sicheren Ende-zu-Ende-Verbindung entwickelt werden, die eine JIT Skalierung erlauben; und es müssen Methoden zur Evaluierung der Sicherheit des Visuellen Inhalts von Videos entwickelt und evaluiert werden.
Da eine detaillierte Beschreibung der Methodologien den Rahmen des Artikels bei weitem übersteigen würde, beschränken wir uns darauf, zu jedem der obig gestellten Fragen einen Überblick über die aktuellen Verfahren zu geben und unseren Beitrag zu umreißen. Damit sich der geneigte Leser zu jedem Gebiet vertiefen kann werden wir ausführlich auf die Literatur verweisen.

2 Wavelet-basierte Videocodecs und existierende Transporttechnologien

2.1 Videokodierung und UMA

Herkömmliche Videokodierung zielt auf eine bestimmte Auflösung und Bitrate ab. Die Kodierung erfolgt hauptsächlich durch Ausnutzung von Redundanzen im Bildbereich und Ähnlichkeiten von zeitlich nahe beisammen liegenden Bildern. Wenn ein VoD-Anbieter nun mehr als eine Zielplattform bedienen will, z.B., Heimkino mit 1080p Auflösung, re-

guläre Fernseher mit PAL-Auflösung und Handys mit 720p, dann muss für jede Zielplattform ein Video, das explizit dafür kodiert ist, gespeichert werden. Serverseitig führt das zu einem nicht unerheblichen Mehraufwand an Speicherplatz. Eine Lösung für dieses Problem wäre das Prinzip des UMA, welches nur ein skalierbares Ursprungsvideo speichert und aus diesem für jede Zielanwendung ein angepasstes Video extrahieren kann.

Der derzeitige Standard für Videokodierung, H.264/AVC [ISO05, ITU07], ist nicht skalierbar und daher für UMA nicht geeignet. Es gibt jedoch eine Erweiterung von H.264/AVC die skalierbar ist, nämlich H.264/SVC [ITU12, SMW07]. Es gibt jedoch einen Nachteil bei der Nutzung von H.264/SVC als Ursprungsvideo. Es erlaubt nämlich nur Skalierung auf Ziele, die beim Erstellen des Ursprungsvideos explizit eingestellt wurden. Damit ist es insofern nicht zukunftssicher, als dass neue Zielanwendungen entweder nicht optimal bedient werden können, oder eine neu Kodierung aller Ursprungsvideos nach sich zieht. Zusätzlich entstehen durch weitere mögliche Zielanwendungen zusätzliche Speicherkosten. In Folge können auch Leitungskapazitäten nicht optimal genutzt werden, da ein Teil der Leitung für unnötige Skalierung verschwendet wird.

Eine Alternative zu H.264/SVC sind Waveletbasierte Videokodierungsverfahren. Diese nutzen ebenso wie H.264 die räumlichen und temporalen Redundanzen in einem Video aus. Durch die Kodierung mittels Wavelets sind sie allerdings automatisch skalierbar. Zwar gibt es bei der räumlichen und zeitlichen Skalierung eine Einschränkung auf dyadische Faktoren, dafür ist die Qualitätsanpassung stufenlos möglich. In unseren Arbeiten haben wir den MC-EZBC von Woods et al. [WGW04] verwendet. Durch die Art der Kodierung ist also sichergestellt, dass Ursprungsvideos zukunftssicher gespeichert werden können. Zudem kann mit der stufenlosen Qualitätsanpassung sichergestellt werden, dass die verfügbare Kapazität eines Übertragungskanals optimal genutzt werden kann.
Es bleibt noch die Frage zu klären, ob der MC-EZBC grundsätzlich eine vergleichbare Qualität wie H.264 liefert. Lima et al. [LMA+07] haben Waveletbasierte Codecs mit H.264/AVC verglichen und kamen zum Schluss, dass zwischen beiden Codecs keine großen Qualitätsunterschiede merklich sind. Da wir die Waveletbasierten Codecs anstelle von H.264/SVC verwenden wollen, haben wir dies gesondert getestet [HSU09]. Wir haben festgestellt, dass es bei einer geringen Anzahl von Skalierungszielen für H.264/SVC keinen merklichen Qualitätsunterschied festzustellen gibt. Erhöht man allerdings die Anzahl von Skalierungszielen, verringert sich bei gleichbleibendem Speicherverbrauch die Qualität von H.264/SVC gegenüber dem MC-EZBC. Wir können also festhalten, dass für UMA die Waveletbasierten Codecs von Vorteil sind, da sie bei gleichem Speicher Verbrauch optimale Leitungsnutzung erlauben und zukunftssicher sind.

2.2 Transport von Waveletbasierten Videos

Die Nutzung von Wavelets als Codec für VoD-Systeme hat allerdings auch Nachteile, nämlich die Tatsache, dass die Hardware und Software für den Transport der Videos durch das Netzwerk und für die Skalierung auf dem Standard (H.264) aufbaut. Es gibt diesbezüglich auch einiges an Literatur, sowohl für den Transport [WHP+07, Apo06] als auch für die Skalierung [KKH10, TPP08, KKRH08].

Um das System optimal zu gestalten, geht es allerdings nicht nur um den Transport der Videos, sondern auch um die Skalierung im Netzwerk. Dadurch kann man die Kanalkapazität besser nutzen, indem man die Skalierung ins Netzwerk verschiebt und nur dann skaliert wenn es tatsächlich nötig ist. Beispielsweise kann die Kanalkapazität bei drahtlosen Anwendungen schwanken, z.B. durch die Anzahl der Benutzer in einer Funkzelle. In diesem Fall ist es möglich, ein Video bis zum Übergang auf den drahtlosen Kanal mit der maximal möglichen Qualität zu schicken. Die Anpassung an die aktuelle Kapazität kann dann auf dem Zugriffspunkt erfolgen, um dem Anwender immer die optimale Qualität zu liefern. Damit die Skalierung im Netzwerk passieren kann müssen die MANEs eine Information geliefert bekommen, die beschreibt, wie die gelieferten Daten aufgebaut sind.

Eine Art, die gelieferten Daten zu beschreiben ist, einen parallelen Datenstrom zu verwenden, der die Videodaten beschreibt. Die standardisierte Weise dies zu tun basiert auf MPEG-21 "Digital Item Adaptation" [ISO07] und wird passenderweise als "generic Bitstream Syntax Description" (gBSD) bezeichnet [PHH+03]. In [HU09a] haben wir ein Beschreibungsmodell entwickelt, mit dem sich ein auf Waveletbasiertes Video mittels gBSD gut beschreiben lässt. Zudem haben wir untersucht, wie gut dieses in der Praxis verwendbar ist. Das Problem mit gBSD ist, dass die Größe der Beschreibung linear mit der Anzahl der Skalierungspunkte steigt. In einem Anwendungsfall, in dem eine feingranulare Skalierung nötig ist, etwa das Beispiel zur drahtlosen Übertragung von oben, kann gBSD deshalb nicht effizient verwendet werden.

Eine andere Option ist die standardisierte Art zum Transport von Multimediadaten zu verwenden, nämlich das "Real-time Transport Protocol" (RTP) [SCFJ03] und das "Real Time Streaming Protocol" (RTSP) [SRL98], welches wiederum auf RTP basiert. Für H.264/AVC gibt es durch [WHS+05] eine Beschreibung wie RTP und RTSP zu nutzen sind. Kuschnig et al. [KKRH08] haben diese Beschreibung auf H.264/SVC erweitert. Grundsätzlich funktioniert dass, indem ein H.264/SVC Strom in "network abstraction layer units" (NALUs) aufgebrochen wird und diese als Basis für die Skalierung auf den MANEs verwendet werden. Wenn wir also eine Möglichkeit finden können, einen Waveletbasierten Strom in solche NALUs zu zerlegen, die bezüglich Skalierung die gleichen Eigenschaften aufweisen wie vergleichbare H.264/SVC-NALUs, so können wir die bestehende Hard- und Software für diese Art des Transports nutzen. In [HHK+11] haben wir eine solche Zerlegung auf Basis des MC-EZBC erzeugt. Allerdings ist sie so allgemein, dass sie mit kleineren Anpassungen für alle Waveletbasierten Ströme nutzbar ist. Zudem haben wir Untersuchungen zur Effizienz angestellt, die zeigen, dass der Aufwand für diese Art des Transports und der Skalierung geringer ist als die Nutzung von gBSD.

3 Sichere Methoden für Ende-zu-Ende Verbindungen mit Skalierung

3.1 Datenverschlüsselung

Die traditionelle Art der Verschlüsselung basierend auf der Arbeit von Shannon [Sha49] würde eine sichere Ende-zu-Ende Verbindung erlauben. Da für die Skalierung zumindest

die Beschreibungsdaten im Klartext erhalten werden müssen, kann damit im Netzwerk keine Skalierung vorgenommen werden. Eine Variante die in diesem Fall üblicherweise Anwendung findet, lautet selektive Verschlüsselung. Dabei wird nicht der gesamte Datenstrom verschlüsselt sondern nur ausgewählte Teile. Üblicherweise werden Beschreibungsdaten im Klartext belassen und nur die Bilddaten verschlüsselt. Allerdings haben sich in diesem Zusammenhang und im Kontext von "digital rights management" (DRM) noch andere Arten der selektiven Verschlüsselung etabliert. Man unterscheidet grob nach dem Anwendungsfall von DRM folgende Methoden:

Strenge Sicherheit wird oft auch als "message privacy" Sicherheit (MP security) bezeichnet. Formell heißt MP-Sicherheit, dass aus dem verschlüsselten Strom keine Rückschlüsse auf den Klartext gezogen werden können [BRRS09]. Im Falle von MC-EZBC-Daten konnten wir zeigen [HU10a], dass bereits die Beschreibungsdaten ausreichen, um Rückschlüsse zu ziehen. Es kann hier also nur mit traditioneller Verschlüsselung eine strenge Sicherheit gewährleistet werden.

Inhaltssicherheit ist eine Aufweichung der strengen Sicherheit. Es wird erlaubt, dass Beschreibungsdaten rekonstruiert werden dürfen. Allerdings dürfen bei der Inhaltssicherheit die Inhaltsdaten, also bei Video etwa das Bildmaterial, nicht in einer Art und Weise rekonstruierbar sein die eine Erkennung der Inhalte erlaubt [SU12].

Hinreichende Sicherheit bezeichnet eine Art der Verschlüsselung, die es durchaus erlaubt, Inhaltsdaten teilweise zu rekonstruieren. Allerdings wird gefordert, dass ein Missbrauch der Daten verhindert wird. Dies geschieht üblicherweise dadurch, dass die Inhaltsdaten nur auf eine Art rekonstruiert werden können welche die Qualität der Daten extrem verringert [SU10]. Im Falle von Videos reicht es üblicherweise, die Qualität soweit zu mindern dass ein Konsum der Daten schlecht bis gar nicht möglich ist.

Transparente Sicherheit ist eine Art von hinreichender Verschlüsselung bei der allerdings eine Mindestqualität gefordert wird. Anders als bei hinreichender Sicherheit, wo es nur darum geht, die Qualität hinreichen zu verringern, will man bei transparenter Sicherheit die Qualität nur in einem bestimmen Maß vermindern. Das Ziel der transparenten Sicherheit ist es üblicherweise eine Vorschau mit niederer Qualität zu geben, die mit dem korrekten Schlüssel auf eine hohe Qualität zurückgeführt werden kann [LC07].

Bezüglich der Sicherheit dieser selektiven Verschlüsselungsverfahren, speziell im Zusammenhang mit Shannons Arbeit, hat Lookabaugh et al. [LS04] gezeigt, dass die Sicherheit gewährleistet ist.

In [HU09b] haben wir für MC-EZBC-basierte Videos ein Verschlüsselungsverfahren entwickelt, welches die Bilddaten verschlüsselt und damit für hinreichende und transparente Sicherheit geeignet ist. In [HU10a] haben wir untersucht, ob es sich auch für Inhaltssicherheit eignet und feststellen müssen, dass temporale Information die Sicherheit in dieser Hinsicht kompromittiert. Wir haben eine Erweiterung für das Verschlüsselungsverfahren aus [HU09b] entwickelt, welches Inhaltssicherheit erlaubt. Zudem haben wir zeigen können dass keine Form der selektiven Verschlüsselung für MC-EZBC-basierte Videos eine strenge Sicherheit gewährleisten kann.

3.2 Kanalverschlüsselung

Eine andere Form der sicheren Ende-zu-Ende Verbindung kann erreicht werden, indem man unverschlüsselte Daten über einen sicheren Kanal versendet. Dafür gibt es einen auf RTP basierenden Standard namens "Secure Real-time Transport Protocol", der in [BMN+04] definiert ist. Dabei wird ein sicherer Kanal aufgebaut und die Daten werden darüber versendet. Das zieht nach sich, dass an jeder Stelle im Netzwerk, die auf die Daten zugreift, der Schlüssel bekannt sein muss. Das heißt nicht nur, dass das Schlüsselmanagement zu einem Problem wird, sondern auch, dass jede Stelle im Netzwerk, die auf den Datenstrom zugreift, ein potentielles Angriffsziel ist.
Im Gegensatz zur selektiven Verschlüsselung der Daten muss außerdem der Datenstrom komplett entschlüsselt und wieder verschlüsselt werden, wenn auf die Daten zugegriffen wird. Dadurch entstehen einerseits zeitliche Verzögerungen bei der Auslieferung der Daten und andererseits steigen die Hardwareanforderungen an die MANEs, die die Last der Ent- und Verschlüsselung tragen. In [HHK+11] haben wir Messungen angestellt, die sowohl Latenz als auch Hardwareanforderungen von Kanal- und Datenverschlüsselung vergleichen. Die Messungen haben klar ergeben, dass auf Basis der Effizienz die Kanalverschlüsselung der Datenverschlüsselung unterlegen ist.

4 Visuelle Evaluierung und Sicherheit

Bei der visuellen Evaluierung von Bildinhalten geht es darum, die Qualität zu bestimmen, in der ein Konsument das Bildmaterial wahr nimmt. Das ist einerseits bei der Kompression wichtig, spielt aber auch bei der selektiven Verschlüsselung, bei Inhalts-, hinreichender und transparenter Verschlüsselung eine Rolle. Optimalerweise wird die Qualität direkt durch Befragung von Menschen ermittelt. Es gibt dafür Standards, wie das zu geschehen hat. Die wichtigsten sind die Empfehlungen der ITU, speziell die "Methodology for the subjective assessment of the quality of television pictures" [ITU02] und "Audiovisual quality in multimedia services" [ITU96]. Dabei werden Laborbedingen spezifiziert, etwas Bildschirmauflösung, der Abstand zum Bild, die Dauer der Anzeige und Beleuchtung. Zusätzlich wird die Anzahl der Testsubjekte auf mindestens fünfzehn festgelegt. Der dadurch entstehende Zeit- und Kostenaufwand ist schon für kleine Testreihen recht hoch.
Üblicherweise wird anstelle der Testreihen mit menschlichen Betrachtern dazu übergegangen, Bildmetriken zu verwenden. Diese bilden das menschliche Sehvermögen ab und werden auch als objektive Metriken bezeichnet. Entwickelt werden diese Bildmetriken mit der Hilfe von Datenbanken, die eine Vielzahl von Bildern mit unterschiedlichen Veränderungen und Verzerrungen enthalten, zusammen mit Messwerten durch menschliche Betrachter laut ITU-Empfehlung. Die Veränderungen der Bilder unterscheiden sich von Datenbank zu Datenbank, enthalten aber üblicherweise typische Arten der Kompression, z.B. JPEG oder JPEG2000, und häufig auftretende Veränderungen wie Rauschen, Unschärfe oder Kontraständerungen. Typische Vertreter solcher Datenbanken sind die "LIVE Image Quality Assessment Database" [SWCB] und "Tampere Image Database" [PBE+08, PLZ+09].

Typischerweise werden Bildmetriken verwendet, die sowohl eine schnell Evaluierung er-

lauben als auch annähernd dem menschlichen Sehen entsprechen. Die am weitesten verwendet Bildmetrik ist immer noch der Signal-Rausch-Abstand [Lia09], da diese Metrik einfach zu implementierten und schnell anzuwenden ist. Allerdings ist von dieser Metrik auch bekannt, dass sie das menschliche Sehen nur schlecht abbildet [HTG08, HU10b]. Daher werden in letzter Zeit immer öfter Metriken verwendet, die besser dem menschlichen Sehen entsprechen, aber immer noch schnell anwendbar sind. Typische Vertreter dieser Kategorie sind SSIM [WBSS04] und NICE [DR09]. Obwohl es bessere Bildmetriken gibt, etwa VIF [SB06] oder CPA1 [CPA10], werden diese vergleichsweise selten verwendet, weil sie kompliziert und sehr langsam sind. Um die Evaluierung weiter zu optimieren, haben wir in [HU11] eine Bildmetrik entwickelt die besser dem menschlichen Sehen entspricht als SSIM und NICE. Die Leistung ist am ehesten mit der CPA1 vergleichbar. Dabei ist die Metrik allerdings schneller als SSIM und NICE.
Diese Bildmetriken sind generell gut geeignet, wenn es um hohe Qualität geht, die hauptsächlich bei Kompression oder Bildbearbeitung interessant ist. Allerdings eignen sie sich weniger, wenn die Qualität merklich nachlässt, wie es etwa bei hinreichender oder transparenter Verschlüsselung der Fall sein kann. Wir haben in [HU10b] gezeigt, dass die normale Leistung einer Metrik nicht für niederqualitatives Bildmaterial gilt. In [HU13] haben wir eine Methodologie für die Evaluierung von Sicherheitsmetriken vorgestellt und herkömmliche Metriken evaluiert. Dabei hat sich herausgestellt, dass nur die VIF annähernd die Leistung bringt, die man von einer Sicherheitsmetrik erwarten würde.

5 Zusammenfassung

Wir haben die Fragestellung behandelt in welchen Gebieten Probleme bei Video-on-Demand Systemen auftreten die auf Wavelet-basierte Videokompression aufbauen. Zu den gefundenen Themengebieten haben wir ein Übersicht über derzeitige Standards gegeben und Lösungen für die gefundenen Probleme präsentiert.

Literatur

[Apo06] J. Apostolopoulos. Architectural Principles for Secure Streaming & Secure Adaptation in the Developing Scalable Video Coding (SVC) Standard. In *Proceedings of the IEEE International Conference on Image Processing, ICIP '06*, Seiten 729–732, Oktober 2006.

[BMN+04] M. Baugher, D. McGrew, M. Naslund, E. Carrara und K. Norrman. The Secure Real-time Transport Protocol (SRTP). RFC 3711 (Proposed Standard), Marz 2004.

[BRRS09] M. Bellare, T. Ristenpart, P. Rogaway und T. Stegers. Format-preserving encryption. In *Proceedings of Selected Areas in Cryptography, SAC '09*, Jgg. 5867, Seiten 295–312, August 2009.

[CPA10] Maurizio Carosi, Vinod Pankajakshan und Florent Autrusseau. Towards a simplified perceptual quality metric for watermarking applications. In *Proceedings of SPIE, Multimedia on Mobile Devices*, Jgg. 7542, Januar 2010.

[CW04] Peisong Chen und John W. Woods. Bidirectional MC-EZBC With Lifting Implementation. *IEEE Transactions on Circ. and Systems for Video Technology*, 14(10):1183–1194, 2004.

[DR09] S. S. Hemami D. Rouse. Natural Image Utility Assessment Using Image Contours. In *IEEE International Conference on Image Processing (ICIP'09)*, Seiten 2217–2220, November 2009.

[HHK+11] Hermann Hellwagner, Heinz Hofbauer, Robert Kuschnig, Thomas Stütz und Andreas Uhl. Secure Transport and Adaptation of MC-EZBC Video Utilizing H.264-based Transport Protocols. *Elsevier Journal on Signal Processing: Image Communication*, 27(2):192–207, 2011.

[Hof13] Heinz Hofbauer. *Visual Evaluation, Scaling and Transport of Secure Videos*. Dissertation, University of Salzburg, Department of Computer Sciences, April 2013.

[HSU09] H. Hofbauer, T. Stütz und A. Uhl. Secure Scalable Video Compression for GVid. In *Proceedings of the 3rd Austrian Grid Symposium*, Jgg. 269 of *books@ocg.at*, Seiten 88–102, 2009.

[HTG08] Q. Huynh-Thu und M. Ghanbari. Scope of validity of PSNR in image/video quality assessment. *Electronics Letters*, 44(13):800–801, Juni 2008.

[HU09a] Heinz Hofbauer und Andreas Uhl. The Cost of In-Network Adaption of the MC-EZBC for Universal Multimedia Access. In *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis (ISPA '09)*, September 2009.

[HU09b] Heinz Hofbauer und Andreas Uhl. Selective Encryption of the MC EZBC Bitstream for DRM Scenarios. In *Proceedings of the 11th ACM Workshop on Multimedia and Security*, Seiten 161–170, September 2009.

[HU10a] Heinz Hofbauer und Andreas Uhl. Selective Encryption of the MC-EZBC Bitstream and Residual Information. In *18th European Signal Processing Conference, 2010 (EUSIPCO-2010)*, Seiten 2101–2105, August 2010.

[HU10b] Heinz Hofbauer und Andreas Uhl. Visual Quality Indices and Low Quality Images. In *IEEE 2nd European Workshop on Visual Information Processing*, Seiten 171–176, Juli 2010.

[HU11] Heinz Hofbauer und Andreas Uhl. An Effective and Efficient Visual Quality Index based on Local Edge Gradients. In *IEEE 3rd European Workshop on Visual Information Processing*, Seite 6pp., Juli 2011.

[HU13] Heinz Hofbauer und Andreas Uhl. An Evaluation of Visual Security Metrics. *IEEE Transactions on Multimedia*, Seite 15 pages, 2013. submitted.

[ISO05] ISO/IEC 14496-10. Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding, 2005.

[ISO07] ISO/IEC 21000-7:2007. Information technology – Multimedia framework (MPEG-21) – Part 7: Digital Item Adaptation, November 2007.

[ITU96] ITU-T REC P.910. SERIES P: TELEPHONE TRANSMISSION QUALITY Audiovisual quality in multimedia services, 1996.

[ITU02] ITU-R BT.500-11. Methodology for the subjective assesment of the quality of television pictures, 2002.

[ITU07] ITU-T H.264. Advanced video coding for generic audiovisual services, November 2007.

[ITU12] ITU-T REC H.264. SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS Infrastructure of audiovisual services Coding of moving video, Januar 2012.

[KKH10] R. Kuschnig, I. Kofler und H. Hellwagner. Improving Internet Video Streaming Performance by Parallel TCP-based Request-Response Streams. In *Proceedings of the 7th Annual IEEE Consumer Communications and Networking Conference (IEEE CCNC 2010)*, Januar 2010.

[KKRH08] R. Kuschnig, I. Kofler, M. Ransburg und H. Hellwagner. Design options and comparison of in-network H.264/SVC adaptation. *Journal of Visual Communication and Image Representation*, 19(8):529–542, September 2008.

[LC07] Q. Li und I. J. Cox. Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking. *IEEE Transactions on Information Forensics and Security*, 2(2):127–139, Juni 2007.

[Lia09] Shiguo Lian. Efficient image or video encryption based on spatiotemporal chaos system. *Chaos, Solitons & Fractals*, 40(5):2509 – 2519, 2009.

[LMA+07] L. Lima, F. Manerba, N. Adami, A. Signoroni und R. Leonardi. Wavelet-Based Encoding for HD Applications. In *2007 IEEE International Conference on Multimedia and Expo*, Seiten 1351–1354, Juli 2007.

[LS04] T. D. Lookabaugh und D. C. Sicker. Selective Encryption for consumer applications. *IEEE Communications Magazine*, 42(5):124–129, 2004.

[PBE+08] N. Ponomarenko, F. Battisti, K. Egizarian, J. Astola und V. Lukin. Color Image Database for Evaluation of Image Quality Metrics. In *Proceedings of International Workshop on Multimedia Signal Processing*, Seiten 403–408, Oktober 2008.

[PHH+03] Gabriel Panis, Andreas Hutter, Jörg Heuer, Herman Hellwagner, Harald Kosch, Christian Timmerer, Sylvain Devillers und Myriam Amielh. Bitstream syntax description: a tool for multimedia resource adaptation within MPEG-21. In *Special Issue on Multimedia Adaptation*, Jgg. 18 of *Signal Processing: Image Communication*, Seiten 721–747, Sept. 2003.

[PLZ+09] N. Ponomarenko, V. Lukin, A. Zelensky, K. Egiazarian, M. Carli und F. Battisti. TID2008 - A Database for Evaluation of Full-Reference Visual Quality Assessment Metrics. In *Advances of Modern Radioelectronics*, Jgg. 10, Seiten 30–45, 2009.

[SB06] H. R. Sheikh und A. C. Bovik. Image information and visual quality. *IEEE Transactions on Image Processing*, 15(2):430–444, Mai 2006.

[SCFJ03] H. Schulzrinne, S. Casner, R. Frederick und V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. RFC 3550, Juli 2003.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, Oktober 1949.

[SMW07] H. Schwarz, D. Marpe und T. Wiegand. Overview of the Scalable Video Coding Extension of the H.264/AVC Standard. *IEEE Transactions on Circuits and Systems for Video Technology*, 17(9):1103–1120, 2007.

[SRL98] H. Schulzrinne, A. Rao und R. Lanphier. Real Time Streaming Protocol (RTSP). RFC 2326, April 1998.

[SU10] Thomas Stütz und Andreas Uhl. Efficient Format-Compliant Encryption of Regular Languages: Block-Based Cycle-Walking. In *Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security, CMS '10*, Jgg. 6109, Seiten 81–92, Mai 2010.

[SU12] Thomas Stütz und Andreas Uhl. A Survey of H.264 AVC/SVC Encryption. *IEEE Transactions on Circuits and Systems for Video Technology*, 22(3):325–339, 2012.

[SWCB] H. R. Sheikh, Z. Wang, L. Cormack und A. C. Bovik. LIVE Image Quality Assessment Database Release 2.

[TPP08] Nicolas Tizon und Beatrice Pesquet-Popescu. Scalable and Media Aware Adaptive Video Streaming over Wireless Networks. *EURASIP Journal on Advances in Signal Processing*, Volume 2008(Article ID 218046):11 pages, 2008.

[VCE03] A. Vetro, C. Christopoulos und T. Ebrahimi. From the guest editors - Universal multimedia access. *IEEE Signal Processing Magazine*, 20(2):16 – 16, 2003.

[WBSS04] Z. Wang, A.C. Bovik, H.R. Sheikh und E.P. Simoncelli. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4):600–612, April 2004.

[WGW04] Y. Wu, A. Golwelkar und J. W. Woods. MC-EZBC video proposal from Rensselaer Polytechnic Institute. *ISO/IEC JTC1/SC29/WG11, MPEG2004/M10569/S15*, Marz 2004.

[WHP+07] Y. Wang, M. Hannuksela, S. Pateux, A. Eleftheriadis und S. Wenger. System and Transport Interface of SVC. *IEEE Transactions on Circuits and Systems for Video Technology*, 17(9):1149–1163, September 2007.

[WHS+05] S. Wenger, M.M. Hannuksela, T. Stockhammer, M. Westerlund und D. Singer. RTP Payload Format for H.264 Video. RFC 3984, Februar 2005.

Heinz Hofbauer, geboren am 15.12.1977, erlangte seine Hochschulreife an der Höheren Technische Bundeslehranstalt für Elektrotechnik in Salzburg. Anschließend absolvierte er sein Studium an der Universität Salzburg im Bereich Angewandte Informatik. Er schrieb seine Diplomarbeit über die Nutzung von Quasi-Monte-Carlo-Methoden für die parallele Integration von uneigentlichen Integralen und erlangte seinen Abschluss als Diplom-Ingenieur. Danach widmete er sich dem Studium der Bild- und Videoverschlüsselung und der Bestimmung der Qualität von Bild- und Videokompression. Zudem kam das Studium von Videokompression und Übertragung von skalierbarem Videomaterial. Das Studium und die Forschung kulminierte 2013 in der Dissertation mit dem Titel "Visual Evaluation, Scaling and Transport of Secure Videos" und erlangte den Abschluss als Doctor technicæ. Seine Forschungsschwerpunkte liegen derzeit in der visuellen Evaluierung selektiver Verschlüsselungsverfahren, Watermarking und Verschlüsselung von Bild und Video sowie der Biometrie.