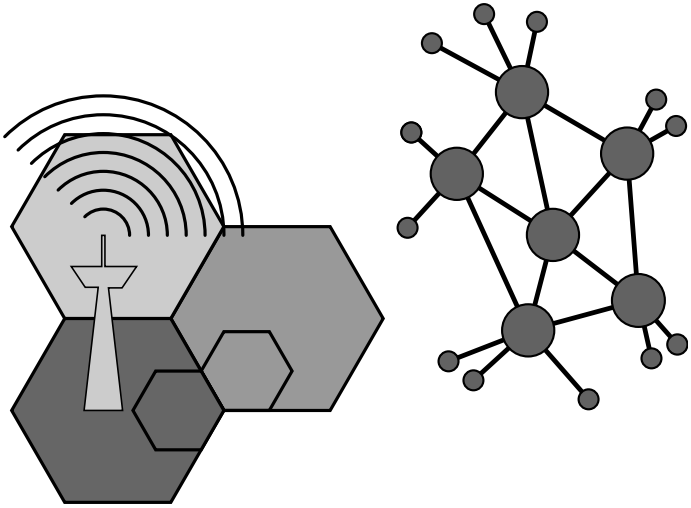
UNIVERSITÄT SIEGEN
Institut für Digitale Kommunikationssysteme

Forschungsberichte

Band 39 Herausgeber: Univ.-Prof. Dr. Christoph Ruland



Tao Wu

Authentication of Compressive Sensing based Image Content

2019

SHAKER VERLAG

Authentication of Compressive Sensing based Image Content

DISSERTATION

zur Erlangung des Grades eines Doktors

der Ingenieurwissenschaften

vorgelegt von

M.Sc. Tao Wu

geb. am 08.12.1988 in Hunan, China

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät

der Universität Siegen

Siegen 2018

1. Gutachter: Univ.-Prof. Dr. rer. nat. Christoph Ruland
2. Gutachter: Prof. Dr. Tiziano Bianchi
Vorsitzender: Prof. Dr. rer. nat. habil. Frank Gronwald

Tag der mündlichen Prüfung: 07.11.2018

UNIVERSITÄT SIEGEN

Institut für
Digitale Kommunikationssysteme

Forschungsberichte

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 39

Tao Wu

Authentication of Compressive Sensing based Image Content

SHAKER
VERLAG

Aachen 2019

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Siegen, Univ., Diss., 2018

Printed in Germany.

ISBN 978-3-8440-6517-6
ISSN 1614-0508

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

To my family

Acknowledgment

This work was created during my employment as a research assistant at the Chair for Data Communications Systems at the University of Siegen. It was funded by the German Research Foundation (DFG) as part of the research training group GRK 1564 “Imaging New Modalities”.

First of all, I would like to express my sincere gratitude to my supervisor Univ.-Prof. Dr. rer. nat. Karl Christoph Ruland, who provided me with the necessary means for my research, my work in the project, and my regular tasks at the chair.

Furthermore, I would like to thank Prof. Dr. Tiziano Bianchi, for agreeing without hesitation to act as the second reviewer for this thesis, Prof. Dr.-Ing. Otmar Loffeld for his participation in the examination commission, and Prof. Dr. rer. nat. habil. Frank Gronwald for chairing the commission.

I would also like to thank all my friends and colleagues from my chair and GRK 1564 project for all their valuable support. In particular, I would like to acknowledge Robin Fay, Romeo Ayemele Djeujo, Thomas Koller, Andreas Schantin, Matthias Schneider, Birgit Wichmann, Jochen Sassmannshausen, Jinse Shin, Donatus Weber, Obaid Ur-Rehman, Amir Tabatabaei, and Natasa Zivic.

Finally, I am grateful to my beloved family: both my parents and parents-in-law, who have always supported me with their endless love, and my sister who has always had faith in me. A special thanks is owed to Gudrun Lücke-Hogaust, who has guided and motived my life in Germany. Last but not least, I would like to thank my wife, Lili, for her patience, understanding, constant support, and faith in me, and my son, Tongshu, who has motivated and disturbed while I have finished this work; without him, this thesis could have been finished earlier, but without him, this work for me would be nothing.

Abstract

Compressive Sensing (CS), which is also called as Compressed Sensing or Compressive Sampling, has received much attention in recent years in the field of mathematics, computer science, and electronics. This novel strategy has redefined the sampling method by choosing an appropriate sensing domain, limiting the characteristics of source information, and performing recovery with a nonlinear solver. A well-configured CS-based sensing system may capture information below the Nyquist rate, so the imaging system can take full advantage of this theory. Therefore, CS-based Imaging (CSI) cameras can construct an N pixel image with only M measurements where $M \ll N$, and the sampling bandwidth of sensors is not limited when the target image can be k-sparse or "compressible" represented. Meanwhile, with the rapid development of the Internet and mobile personal devices, images have become increasingly important in people's lives. However, people cannot securely use the Internet, as information in cyberspace is digital data, which can easily be forged. Since the CSI technique may have a wide implementation in the Internet in the future, it is necessary for CS based images to be protected by an authentication mechanism that can provide the integrity and authenticity of the origin. Thus, this dissertation concentrates on this issue.

This thesis first reviews basic technical concepts of the CSI method and image authentication mechanisms. On the one hand, the security requirement of multimedia information is quite different from conventional data authentication. For the CSI system to provide the authentication of the image must be content-oriented. On the other hand, image recovery noise in the CSI-framework is unavoidable, so only the content or semantic meaning of the image shall be authenticated. Although many image authentication methods can successfully provide content authenticity, such mechanisms are only able to work with existing information, i.e. authentication after sensing process. The CSI system combines sensing and source coding in one step; therefore, integrating the authentication mechanism into the sensing step is the most secure way to authenticate

the sensed target information.

This dissertation subsequently proposes an authenticated CSI system that is based on the Compressive Sensing based Message Authentication Code (CSMAC) mechanism. This MAC method is embedded in the imaging process with a redundant secure matrix. Furthermore, the extraction mechanism may reduce the data size and support a restricted tolerance property. With the help of a pre-trained ϵ_{Vrfy} the verifier can tolerate an appropriate amount of recovery noise and detect the content modifications.

This study finally proposes an authenticated encrypted CSI mechanism, in order to support authentication, encryption, compression and sensing in one step. The mechanism is based on the data compression improvement for CS based images, which has an approximately 20% lower bit-rate for an acceptable image resolution compared to the naive CSI method. The simulated results illustrate that authenticated encrypted CSI is computationally secure for confidentiality and sensitive to a great amount of content-based tampering.

Zusammenfassung

Compressive Sensing (CS), auch als Compressed Sensing oder Compressive Sampling, ist in den vergangenen Jahren ein heißes Thema im Bereich der Mathematik, Informatik und Elektrotechnik, weil diese neuartige Strategie die Abtastung durch die Auswahl einer angemessenen Domäne, die Begrenzung der Quellinformationseigenschaft und die Rekonstruktion mit dem Nichtlinear-Problemlöser neu definiert. Ein gut konfiguriert CS basiertes System könnte Information unter der Nyquist-Rate erfassen, aus diesem Grund würde ein Bildgebungssystem von diesem Verfahren profitieren, d.h. ein Compressive Sensing basiertes Bildgebungssystem (CSI) könnte ein N Pixel Bild mit nur M Messungen für $M \ll N$ rekonstruieren, wenn das Zielbild k-sparse oder "compressible" repräsentiert werden kann. Dazu sind die Arbeitsbandbreite der Sensoren nicht begrenzt. Im Zuge der rapiden Entwicklung des Internets und der mobilen persönlichen Endgeräten erlangen Bilderinformation eine immer größere Bedeutung fürs Leben. Allerdings is die Informationssicherheit im Internet beschränkt, weil die digitalen Daten einfach gefälscht werden könnten. Das CSI Verfahren kann im zukünftigen Internet eingesetzt werden, wobei das CS basierte Bild von einem Authentifikationsmechanismus geschützt werden muss, d.h. die Integrität und die Authentität des Ursprungs der Daten muss sichergestellt werden. Die vorliegende Dissertation konzentriert sich auf dieses Thema.

Zunächst stellt diese Dissertation den technischen Hintergrund von CSI Verfahren und Bildauthentifizierungsmechanismen vor. Einerseits unterscheiden sich die Sicherheitsforderungen an Multimediainformation von der herkömmlichen Datenauthentifizierung, daher sollte das authentifizierte CSI System inhaltsorientiert sein. Anderseits ist das Wiederherstellungsrauschen unvermeidlich im einem CSI Bild, aus diesem Grund sollte nur der Inhalt, nämlich die Bildbedeutung, authentifiziert werden. Obwohl viele Bildauthentifizierungsmechanismen bereits die Authentität des Inhalts eines Bildes verifizieren können, können solche Methoden nur auf bereits existierende Informationen operieren, d.h. nach der Abtastung eines Bildes. CSI Systeme hingegen kombinieren Abtastungs- und Quell-

codierungsvorgang in einem Schritt, deswegen ist die Integration zwischen Abtastung und Authentifizierung eine der sichersten Vorgehensweisen, um die abgetastete Zielinformation zu authentifizieren.

Anschließend stellt diese Dissertation ein authentifiziertes CSI System vor, das auf Compressive Sensing based Message Authentiaction Code (CSMAC) basiert. Dieses MAC Verfahren wird in den Bildgebungsschritt mit Hilfe von einer redundanten sicheren Matrix integriert. Die eingesetzten Extractionsverfahren können die Datenlänge reduzieren und das eingeschränkte Rekonstruktionsrauschen tolerieren. Der zuvor trainierte Parameter ϵ_{Vrfy} hilft dem Prüfer, das Rauschen zu tolerieren und etwaige inhaltliche Fälschungen zu entdecken.

Anschließend wird ein praktisches authentifiziertes verschlüsseltes CSI Verfahren vorgestellt, das Authentifizierung, Verschlüsselung, Komprimierung und Abtastung in einem Schritt realisiert. CSI Methoden haben aber keine gute Datenkomprimierungsfähigkeit. Hier wird eine Verbesserung vorgeschlagen, auf der das authentifizierte verschlüsselte CSI basiert. Die simulierten Ergebnisse zeigen, dass dieses System rechnerische Sicherheit für Vertraulichkeit bietet, empfindlich gegen inhaltliche Fälschungen reagiert und bei der Bitrate einen Gewinn von fast 20% im Vergleich mit normalem Verfahren erreichen kann.

Contents