Datensicherheit, Zusammenfassung Vorlesung 14

Henry Haustein, Dennis Rössel

Was ist Multimedia-Sicherheit?

Forschungsgebiet, das sich mit der Durchsetzung von Schutzzielen an und mit digitalisierten Signalen als Abbild von Ausschnitten der Realität beschäftigt.

Welche Schutzziele sind für Multimedia-Sicherheit relevant, und was bedeuten sie in diesem Kontext?

Integrität, Zurechenbarkeit, Verdecktheit, Vertraulichkeit

Mit welchen Schutzmechanismen können diese Ziele durchgesetzt werden?

Multimedia-Forensik, digitale Wasserzeichen, Steganografie

Wie grenzt sich Steganographie von Kryptographie ab?

Steganographie verdeckt die Existenz von vertraulicher Kommunikation

Wie ist ein steganographisches System prinzipiell aufgebaut (Funktionen mit Ein- und Ausgabewerten)?

Einbetten der Nachricht in Coverdaten unter Verwendung eines Schlüssels

Extrahieren der Daten unter Verwendung des Schlüssels

Was sind relevante Anforderungen an steganographische Systeme?

Unentdeckbarkeit: Entdeckung nicht besser als Raten

Hohe Einbettungsrate

Welche Möglichkeiten für die Verwendung von Schlüsseln in der Steganographie gibt es?

Schlüssel kann Abstände zwischen Einbettungen oder Schlüssel ist Startwert für Zufallszahlengenerator

Welche Klassen von Einbettungstechniken gibt es?

LSB-Ersetzung, Inkrementieren und Dekrementieren

Wie funktionieren LSB-Ersetzung, Inkrementieren und Dekrementieren?

LSB-Ersetzung: letztes Bit jedes Pixels mit Nachricht ersetzen

Inkrementieren: Wenn $cover \mod 2 \neq emb$, dann $stego = cover + 1$

Dekrementieren: Wenn $cover \mod 2 \neq emb$, dann $stego = cover - 1$

Wie ist die Sicherheit der LSB-Ersetzung zu bewerten?

unsicher, da gut untersucht, verschiedene Ansätze zur Analyse: visueller Angriff, Histogrammangriff, Analyse der Bildstruktur