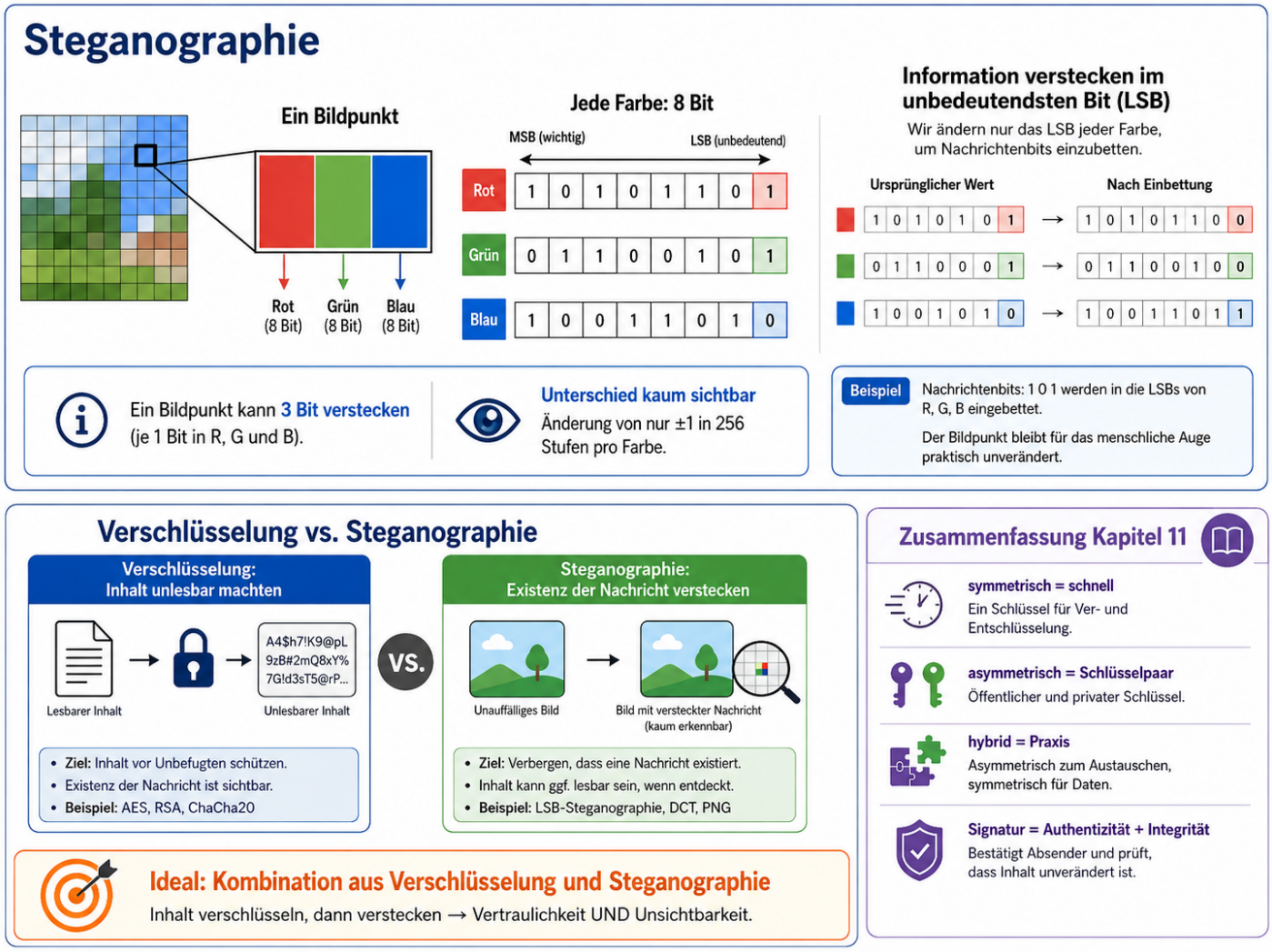
13.8 Steganographie



Kurzüberblick

Steganographie bedeutet:

Informationen werden in unauffälligen Daten versteckt.

Das Ziel ist nicht nur, den Inhalt zu schützen, sondern vor allem zu verbergen, dass überhaupt eine geheime Nachricht vorhanden ist.

> **IHK-Merksatz:**
> Verschlüsselung macht den Inhalt unlesbar.
> Steganographie versteckt die Existenz der Nachricht.

Quelle 11.6 – Steganographie

In der Quelle wird Steganographie als das Verstecken von Informationen in alltäglichen, unauffälligen Daten beschrieben.

Als Beispiel wird ein Bild verwendet.

Ein Bild besteht aus vielen Bildpunkten.

Jeder Bildpunkt kann Farbinformationen enthalten, zum Beispiel:

- Rot
- Grün
- Blau

Bei einem RGB-Bild besteht ein Bildpunkt also aus drei Farbanteilen.

Jeder Farbanteil hat typischerweise 8 Bit.

Grundidee

Ein Bildpunkt kann vereinfacht so aufgebaut sein:

Farbanteil	Größe
Rot	8 Bit
Grün	8 Bit
Blau	8 Bit

Zusammen ergibt das:

Bestandteil	Rechnung
Rot	8 Bit
Grün	8 Bit
Blau	8 Bit
Gesamt pro Bildpunkt	24 Bit

Das bedeutet:

Ein Bildpunkt enthält viele kleine Binärinformationen.

Wenn man nur sehr kleine Teile davon verändert, sieht das menschliche Auge oft kaum einen Unterschied.

Least Significant Bit

Das unbedeutendste Bit nennt man:

Least Significant Bit

Abkürzung:

LSB

Dieses Bit hat den kleinsten Einfluss auf den Zahlenwert.

Wenn man nur dieses letzte Bit ändert, verändert sich die Farbe nur minimal.

Beispiel:

Wert vorher	Wert nachher	Änderung
10101100	10101101	nur das letzte Bit geändert
01100101	01100100	nur das letzte Bit geändert
10011010	10011011	nur das letzte Bit geändert

Der Farbwert ändert sich dadurch nur sehr wenig.

> **Kurz gesagt:**
> Beim LSB-Verfahren wird Information in den kleinsten, kaum sichtbaren Änderungen versteckt.

Beispiel mit einem RGB-Bildpunkt

Ein RGB-Bildpunkt besteht aus:

Farbe	Beispielwert
Rot	10101101
Grün	01100101
Blau	10011010

In jedem dieser drei Farbwerte kann man das letzte Bit verändern.

Dadurch kann ein einzelner Bildpunkt ungefähr 3 Bit verstecken:

Farbe	versteckbares Bit
Rot	1 Bit

Farbe	versteckbares Bit
Grün	1 Bit
Blau	1 Bit
Gesamt	3 Bit pro Bildpunkt

> **Merksatz:**
> Ein RGB-Bildpunkt kann bei einfacher LSB-Steganographie ungefähr 3 Bit verstecken.

Warum sieht man die Veränderung kaum?

Wenn nur das letzte Bit eines Farbwertes verändert wird, ändert sich der Farbwert nur um 1.

Bei 8 Bit gibt es 256 mögliche Werte.

Das heißt:

Eine Änderung um 1 ist sehr klein.

Beispiel	Bedeutung
Farbwert 120	ursprünglicher Farbwert
Farbwert 121	nach Änderung des letzten Bits
Unterschied	kaum sichtbar

Für das menschliche Auge ist so eine minimale Änderung meistens nicht erkennbar.

Steganographie ist nicht dasselbe wie Verschlüsselung

Steganographie und Verschlüsselung werden oft verwechselt.

Sie haben aber unterschiedliche Ziele.

Technik	Ziel
Verschlüsselung	Inhalt unlesbar machen
Steganographie	Existenz der Nachricht verstecken

Beispiel:

Situation	Bedeutung

verschlüsselte Datei	Jeder sieht, dass etwas Verschlüsseltes vorhanden ist
steganographisches Bild	Es sieht wie ein normales Bild aus
verschlüsselte Nachricht im Bild	Inhalt ist geschützt und zusätzlich versteckt

> **Achtung Prüfungsfalle:**
> Steganographie macht den Inhalt nicht automatisch sicher.
> Sie versteckt zunächst nur, dass eine Nachricht vorhanden ist.

Vergleich: Verschlüsselung und Steganographie

Merkmal	Verschlüsselung	Steganographie
Hauptziel	Inhalt schützen	Nachricht verstecken
Sichtbarkeit	Geheimtext ist sichtbar	Nachricht soll unauffällig bleiben
Wenn entdeckt	Inhalt ist hoffentlich noch unlesbar	Inhalt könnte lesbar sein
Typisches Beispiel	AES, RSA, ChaCha20	Nachricht in Bild verstecken
Sicherheitsziel	Vertraulichkeit	Verbergen der Existenz
Ideale Nutzung	allein möglich	besser mit Verschlüsselung kombinieren

---

Ideale Kombination

Die beste Vorgehensweise ist oft:

1. Nachricht zuerst verschlüsseln.
2. Verschlüsselte Nachricht anschließend verstecken.

Warum?

Wenn die versteckte Nachricht entdeckt wird, ist sie immer noch verschlüsselt.

Schritt	Wirkung
Verschlüsseln	Inhalt wird unlesbar
Verstecken	Existenz der Nachricht wird verborgen
Kombination	Inhalt ist geschützt und schwerer zu finden

> **IHK-Merksatz:**
> Erst verschlüsseln, dann verstecken.
> So erhält man Vertraulichkeit und Unauffälligkeit.

Einfaches Beispiel

Alice möchte Bob eine geheime Nachricht schicken.

Die Nachricht lautet:

```
Treffen um 18 Uhr
```

Alice verschlüsselt die Nachricht zuerst.

Daraus wird zum Beispiel:

```
A7x!9LmQ2#
```

Danach versteckt Alice diesen Geheimtext in einem Bild.

Bob erhält ein scheinbar normales Bild.

Mit dem passenden Verfahren kann Bob die versteckte Nachricht auslesen und danach entschlüsseln.

Was sieht Eve?

Wenn Eve das Bild sieht, erkennt sie im besten Fall nicht, dass darin eine Nachricht versteckt ist.

Fall	Was passiert?
Eve erkennt nichts	Nachricht bleibt unentdeckt
Eve findet versteckte Daten	ohne Verschlüsselung könnte der Inhalt lesbar sein
Eve findet verschlüsselte versteckte Daten	Inhalt bleibt trotzdem geschützt

Darum ist die Kombination aus Verschlüsselung und Steganographie sinnvoll.

Typische Trägerdaten

Steganographie kann Informationen in verschiedenen Dateitypen verstecken.

Beispiele:

Trägerdatei	Möglichkeit
Bilddatei	Bits in Farbwerten verstecken
Audiodatei	kleine Änderungen im Audiosignal
Videodatei	Bild- und Audiodaten nutzen
Textdatei	Leerzeichen, Formatierung oder Zeichenmuster
Netzwerkverkehr	versteckte Informationen in Protokollfeldern

Für die IHK ist meistens die Grundidee wichtiger als ein spezielles Werkzeug.

Vorteile der Steganographie

Vorteil	Erklärung
unauffällig	Nachricht soll nicht erkennbar sein
kombinierbar	kann mit Verschlüsselung kombiniert werden
viele Träger möglich	Bilder, Audio, Video oder andere Daten
zusätzlicher Schutz	Angreifer muss zuerst erkennen, dass etwas versteckt ist

---

Nachteile und Risiken

Nachteil	Erklärung
nicht automatisch verschlüsselt	Inhalt kann lesbar sein, wenn entdeckt
Datei kann verändert werden	Kompression oder Bearbeitung kann versteckte Daten zerstören
begrenzter Speicherplatz	nicht beliebig viel Information passt unauffällig hinein
Analyse möglich	Spezialwerkzeuge können Auffälligkeiten erkennen
falsche Nutzung	kann auch für schädliche Zwecke missbraucht werden

---

Problem: Bildkompression

Ein wichtiges Problem ist Kompression.

Wenn ein Bild nachträglich verändert oder stark komprimiert wird, können versteckte Informationen beschädigt oder zerstört werden.

Beispiel:

Aktion	Risiko
Bild verkleinern	versteckte Bits können verloren gehen
Bild stark komprimieren	Farbwerte ändern sich
Bildformat wechseln	versteckte Daten können zerstört werden
Bild bearbeiten	versteckte Nachricht kann beschädigt werden

> **Kurz gesagt:**
> Steganographie ist empfindlich gegenüber Veränderungen an der Trägerdatei.

Steganographie und Sicherheit

Steganographie allein ist keine vollständige Sicherheitslösung.

Sie schützt vor allem gegen Aufmerksamkeit.

Das heißt:

Eve soll möglichst gar nicht merken, dass eine geheime Nachricht existiert.

Aber wenn Eve die versteckte Nachricht findet, braucht man zusätzlich Verschlüsselung.

Ziel	Technik
Inhalt unlesbar machen	Verschlüsselung
Existenz verbergen	Steganographie
Absender prüfen	digitale Signatur
Veränderung erkennen	Hash / Signatur

Typische IHK-Fragen zur Steganographie

Was ist Steganographie?

Steganographie ist das Verstecken von Informationen in unauffälligen Daten.

Was ist das Ziel der Steganographie?

Das Ziel ist, die Existenz einer Nachricht zu verbergen.

Was ist der Unterschied zur Verschlüsselung?

Verschlüsselung macht den Inhalt unlesbar.
Steganographie versteckt, dass eine Nachricht vorhanden ist.

Warum sollte man Steganographie mit Verschlüsselung kombinieren?

Wenn die versteckte Nachricht entdeckt wird, bleibt der Inhalt trotzdem geschützt.

Was bedeutet LSB?

LSB bedeutet Least Significant Bit, also das unbedeutendste Bit.

Warum eignet sich das LSB für Steganographie?

Weil eine Änderung am letzten Bit den Farbwert nur minimal verändert und oft kaum sichtbar ist.

Wie viele Bit kann ein RGB-Bildpunkt bei einfacher LSB-Steganographie ungefähr verstecken?

Ungefähr 3 Bit, also je 1 Bit in Rot, Grün und Blau.

Prüfungsfalle: Steganographie schützt nicht automatisch den Inhalt

Wenn eine Nachricht nur versteckt, aber nicht verschlüsselt wurde, kann sie bei Entdeckung lesbar sein.

Darum gilt:

Aussage	Bewertung
Steganographie versteckt die Nachricht.	richtig
Steganographie verschlüsselt automatisch den Inhalt.	falsch
Verschlüsselung macht den Inhalt unlesbar.	richtig
Kombination aus beidem ist sinnvoll.	richtig

> **Achtung:**
> Versteckt ist nicht automatisch verschlüsselt.

Prüfungsfalle: Steganographie ist kein Ersatz für Verschlüsselung

Steganographie und Verschlüsselung haben unterschiedliche Aufgaben.

Aufgabe	Besser passende Technik

Inhalt geheim halten	Verschlüsselung
Nachricht unauffällig verstecken	Steganographie
Absender prüfen	digitale Signatur
Dateiänderung erkennen	Hashfunktion

> **Merksatz:**
> Steganographie ersetzt keine Verschlüsselung.
> Sie ergänzt Verschlüsselung.

Zusammenfassung

Steganographie bedeutet, Informationen in unauffälligen Daten zu verstecken.

Ein typisches Beispiel ist das Verstecken von Daten in Bildpunkten.

Bei RGB-Bildern bestehen Bildpunkte aus Rot, Grün und Blau.

Wenn jeweils das letzte Bit verändert wird, kann man Informationen verstecken, ohne dass das Bild sichtbar stark verändert wirkt.

Steganographie versteckt aber nur die Existenz der Nachricht.

Für echten Schutz des Inhalts sollte die Nachricht vorher verschlüsselt werden.

> **IHK-Spickzettel:**
> Steganographie = Nachricht verstecken
> Verschlüsselung = Inhalt unlesbar machen
> LSB = Least Significant Bit
> RGB-Bildpunkt = Rot + Grün + Blau
> ungefähr 3 Bit pro Bildpunkt versteckbar
> beste Kombination = erst verschlüsseln, dann verstecken
> Prüfungsfalle = versteckt ist nicht automatisch verschlüsselt

---

Revision #2
Created 2 June 2026 23:58:57 by Admin
Updated 3 June 2026 06:18:12 by Admin