Bibliotekarstudentens nettleksikon om litteratur og medier

Av Helge Ridderstrøm (førsteamanuensis ved OsloMet – storbyuniversitetet)

Sist oppdatert 10.01.19

Dette dokumentets nettadresse (URL) er:
https://www.litteraturogmedieleksikon.no/.cm4all/uproc.php/0/steganografi.pdf

Steganografi

Ordet kommer fra gresk for "skjult" og "skrift". Det betegner kommunikasjon som foregår på en slik måte at budskapet er skjult for de fleste, og at disse ikke engang oppdager at det blir kommunisert noe hemmelig. Kun den intenderte mottakeren skal oppdage et bestemt budskap. Steganografi kan oppfattes som en type kryptografi (som er alle teknikker for å skjule informasjon).

"Hvis man vil holde på en hemmelighed, skal man sørge for, at ingen kan se den. I 480 f.Kr. samlede den persiske kong Xerxes verdens hidtil største hær under sit imperiums langvarige konflikt med Grækenland. Den udvikling gik ikke hen over på hovedet på Demaratus, en græker, der levede i eksil i Persien. Han satte sig for at advare grækerne mod den kommende invasion. For ikke at blive afsløret skrabede han bivoksen af en skriveplade, skrev meddelelsen på træpladen og smurte voksen på igen. Ingen vagter på vejen til Grækenland lagde mærke til de tilsyneladende ubeskrevne plader. Da kureren nåede frem, bad han modtageren skrabe vokslaget af. Overraskelsesmomentet gik tabt, og den vældige persiske invasionsstyrke blev slået. Det er den første kendte brug af den teknik, der kaldes steganografi. Ordet stammer fra de græske ord for "dækkende" og "skrift". Det er muligt, at du ikke har kendt ordet, men hvis du som barn har skrevet beskeder med usynligt blæk, har også du beskæftiget dig med steganografi." (Rasmus Elm Rasmussen i https://www.altomdata.dk/gem-dine-hemmeligheder-i-fuld-offentlighed; lesedato 12.10.18)

"Steganografi er en flere tusinde år gammel teknik, brugt til at skjule hemmelige informationer. For eksempel beskrev Herodot (484 f.Kr. til ca. 420 f.Kr.) hvordan en vis Histaios lod sin budbringer kronrage, hvorpå der på hans hoved blev skrevet en besked. Budbringeren kunne derefter, da håret var groet ud igen, uhindret rejse til modtageren" (https://www.linuxin.dk/node/20779; lesedato 25.09.18).
"Steganography is an ancient practice. When spies in the Revolutionary War wrote in invisible ink or when Da Vinci embedded secret meaning in a painting that was steganography. […] the approach to steganography that ancient Greek leader Histiaeus used in 440 BCE: shaving a trusted slave's head, tattooing a secret message on his scalp, letting his hair grow in, and then sending him off to be

shaved again by the message's recipient." (Lily Hay Newman i https://www.wired.com/story/steganography-hacker-lexicon/; lesedato 12.07.18)

"By the 16-17th centuries, there had arisen a large literature on steganography and many of the methods depended on novel means of encoding information. In his four hundred page book *Schola Steganographica*, Gaspar Schott (1608-1666) explains how to hide messages in music scores: each note corresponds to a letter […]. Schott also expands the 'Ave Maria' code proposed by Johannes Trithemius (1462-1516) in *Steganographiæ*, one of the first known books in the field. The expanded code uses forty tables, each of which contains 24 entries (one for each letter of the alphabet of that time) in four languages: Latin, German, Italian and French. Each letter of the plain-text is replaced by the word or phrase that appears in the corresponding table entry and the stego-text ends up looking like a prayer or a magic spell. […] John Wilkins (1614-1672), Master of Trinity College, Cambridge […] explains how one can hide secretly a message into a geometric drawing using points, lines or triangles. […] A very widely used method is the acrostic. In his book, *The Codebreakers*, David Kahn explains how a monk wrote a book and put his lover's name in the first letters of successive chapters. He also tells of prisoners of war who hid messages in letters home using the dots and dashes on *i*, *j*, *t* and *f* to spell out a hidden text in Morse code. These 'semagrams' concealed messages but have an inherent problem, that the cover-text tends to be laborious to construct and often sounds odd enough to alert the censor. During both World Wars, censors intercepted many such messages. A famous one, from World War I, was a cablegram saying 'Father is dead' which the censor modified into 'Father is deceased'. The reply was a giveaway: 'Is Father dead or deceased?' " (Fabien Petitcolas, Ross Anderson og Markus Kuhn i http://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf; lesedato 31.08.18).

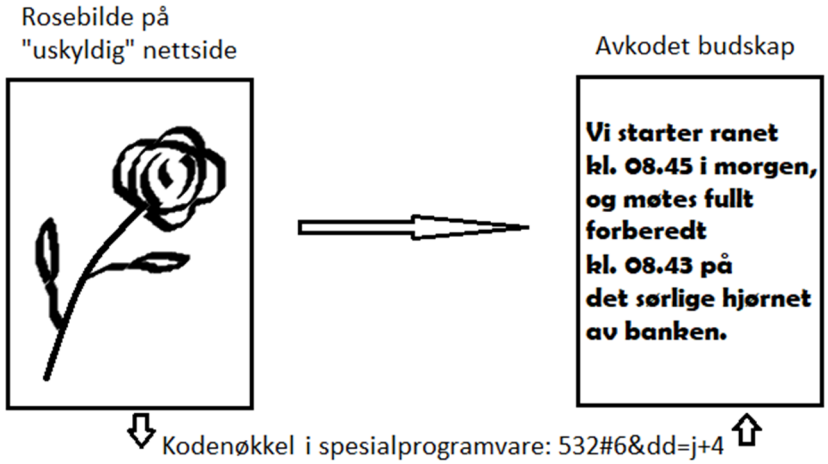
"Osynligt bläck användes så sent som under andra världskriget med framgång. För angripare som inte har tillgång till mer avancerad tekniskutrustning kan vi nå en acceptabel säkerhetsnivå genom att välja substanser som uppfyller dessa krav: Skriften syns inte alls med mikroskop förrän vi har framkallat den. Att framkalla skriften är svårt om man inte vet vilka substanser den har skrivits med." (Hans Husman i http://www.hanshusman.nu/kfbts/Kryptering%20Steganografi.htm; lesedato 10.11.02)

Det kan brukes svært enkle metoder i programvare for å skjule kommunikasjon, f.eks. slik: I et vanlig skriveprogram skrives det enkeltbokstaver mellom ordene, men disse enkeltbokstavene gjøres hvite og dermed usynlige. Til sammen utgjør enkeltbokstavene en tekst med et budskap. Fordi denne teksten er hvit, er den usynlig (en eventuell stavekontroll må være slått av), men mottakeren vet at den kan gjøres om til synlig tekst.

"Med steganografi er det ikke umiddelbart indlysende, at der ligger en meddelelse gemt i en fil, men hvis nogen opdager det, er det næppe umuligt at uddrage de

skjulte data. På den anden side er det indlysende, at en krypteret fil indeholder hemmeligheder, men det er mildt sagt problematisk at dechifrere informationen. Hvis man bruger både steganografi og kryptering, får man det bedste fra begge verdener." (Rasmus Elm Rasmussen i https://www.altomdata.dk/gem-dine-hemmeligheder-i-fuld-offentlighed; lesedato 12.10.18)

Informasjon kan gjemmes unna i lite påfallende bildedata på Internett (Münker og Roesler 1997 s. 208). Et verbalt budskap f.eks. være gjemt i et digitalt fotografi (SPoKK 1997 s. 343). Dette kan illustreres slik, der bare ranerne har tilgang til koden som trengs for å få fram budskapet:



"Med nya tjänster som utnyttjar så kallad steganografi kan man skicka dolda meddelanden gömda inuti andra helt alldagliga meddelanden – som i en rolig bild av en katt eller i en till synes helt normal Rick Astley-video som man postar på nätet. Steganografi är ett forskningsfält som använder sig av kryptering, men till skillnad från vanliga krypterade meddelanden är syftet med steganografi att dölja att det överhuvudtaget har skickats något meddelande. […] Tekniken är en ny möjlighet för exempelvis människor som lever i länder där internettrafiken censureras att kunna göra sig hörda. Om myndigheterna ifråga inte kan snappa upp att ett meddelande skickats kan de inte heller avlyssna det eller stoppa det. Dessutom är kryptering helt och hållet förbjudet för invånare i vissa länder, och det innebär att steganografin måste vara delikat utfört för att inte väcka misstankar. […] Den som känner till det hemliga lösenordet (en så kallad "hash") kan "avkoda" filen och får därmed fram ett krypterat meddelande. […] allt en mottagare behöver är nyckeln (som består av ett antal bokstäver eller siffror) och lösenordet. Filen kan denne ladda ner från en förutbestämd plats på nätet. Mottagaren av meddelandet behöver då inte känna till hur meddelandet har krypterats eller gömts inuti filen. Det finns inte heller någon särskilt "plats" i textfilen eller bildfilen där meddelandet göms – det är inbakat i filen som helhet." (Nanok Bie i https://www.svt.se/nyheter/utrikes/ny-teknik-gommer-hemligheter-rakt-framfor-ogonen-pa-dig; lesedato 10.09.18)

“Steganografi innebär att man gömmer en mängd information i en annan mängd information. Genom att kombinera steganografi och kryptering kan man uppnå högre säkerhet än om vi bara krypterar. Angriparen måste både upptäcka informationen, få fram den och dekryptera den. Informationen kan t.ex. gömmas i vanliga brev, bilder, musik m.m. eller på hemsidor.” (Hans Husman i http://www.hanshusman.nu/kfbts/Kryptering%20Steganografi.htm; lesedato 10.11.02)

“Steganography is the art of hiding information in plain sight […] Unlike encryption, where it’s obvious that a message is being hidden, steganography hides data in plain view, inside a file such as a picture. As far as images are concerned, to anyone who isn’t aware that it contains hidden data, it looks like just a normal, innocent picture. Steganography is useful in situations where sending encrypted messages might raise suspicion, such as in countries where free speech is suppressed. It’s also frequently used as a digital watermark to find when images or audio files are stolen.” (https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/; lesedato 03.04.18)

Steganografi kan brukes f.eks.:

“1. *För copyright-bevis*. Antag t.ex. att du skapar ett JavaScript program som du lägger ut på din hemsida. Du har förbehållit dig Copyright för programmet och vill inte att någon annan ska använda programmet utan att betala dig en summa pengar. Ingenting hindrar dock någon annan från att ta ditt program och hävda att han skrivit det. Genom steganografi kan du lägga dold information i programmet som bevisar att du är författaren. För ditt JavaScript måste du antagligen utveckla egna metoder, men när det gäller bilder och ljud finns färdiga program att ladda ner på Internet.

2. *För att tillföra information utan att förstöra det estetiska värdet*. Detta kan gälla t.ex. bilder, som man vill tillföra information om vad bilden föreställer. Att skriva det synligt på bilden förstör den. Genom att utnyttja steganografi kan man tillföra informationen utan att förstöra bilden.

3. *För att skydda mot olämplig spridning av information*. Antag, t.ex. att vi äger ett företag som forskar inom medicin. En del dokument som anställda har tillgång till är värda mycket stora summor, skulle en anställd via t.ex. email skicka dessa till fel person kan förlusten vara avsevärd. En metod för att skydda oss mot detta är att tillföra känsliga dokument en dold signatur. Mailservern får sedan kontrollera alla email och skulle ett mail innehålla den dolda signaturen så skickas det inte.

4. *För att lagra data*. Gömmer vi krypterad information måste angriparen inte bara lyckas dekryptera datat utan även hitta datat och utveckla en metod för att extrahera fram det. Detta ger utökad säkerhet.” (Hans Husman i http://www.hanshusman.nu/kfbts/Kryptering%20Steganografi.htm; lesedato 10.11.02)

“[S]ome malicious code can actually hide inside other, benign software – and be programmed to jump out when you aren’t expecting it. Hackers are increasingly using this technique, known as steganography, to trick internet users and smuggle malicious payloads past security scanners and firewalls. Unlike cryptography, which works to obscure content so it can’t be understood, steganography’s goal is to hide the fact that content exists at all by embedding it in something else. And since steganography is a concept, not a specific method of clandestine data delivery, it can be used in all sorts of ingenious (and worrying) attacks. […] Steganography is the practice of hiding secret messages in otherwise non-secret mediums.” (Lily Hay Newman i https://www.wired.com/story/steganography-hacker-lexicon/; lesedato 12.07.18)

“Steganografi skal lure nett-sensuren […] Demokrati-aktivister i sensur-hungrige land skal snart få hjelp. Hacktivismo-gruppen lanserer om få uker et Explorer-tillegg som gjemmer dine hemmeligheter og sletter dine spor. […] Det nettleser-baserte programmet Camera/Shy skal gjemme dine hemmeligheter ved hjelp av steganografi. Tanken er at demokratiforkjempere i Burma, Kina og andre utsatte steder skal kunne pakke inn informasjon de vil spre, på en enkel måte, og skjule den godt for myndighetenes overvåkere.” (http://www.digi.no/php/art.php?id=67293&utskrift=1; lesedato 24.10.06)

“There are several different techniques for concealing data inside of normal files. One of the most widely used and perhaps simplest to understand is the least significant bit technique, known commonly as LSB. This technique changes the last few bits in a byte to encode a message, which is especially useful in something like an image, where the red, green, and blue values of each pixel are represented by eight bits (one byte) ranging from 0 to 255 in decimal or 00000000 to 11111111 in binary. Changing the last two bits in a completely red pixel from 11111111 to 11111101 only changes the red value from 255 to 253, which to the naked eye creates a nearly imperceptible change in color but still allows us to encode data inside of the picture.” (https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/; lesedato 03.04.18)

“En af de mest populære former for digital steganografi består i, at man gemmer en meddelelse i en jpg-fil. Dette format koder hver pixel ved hjælp af 8 bits for hver af de tre primærfarver (rød, grøn og blå), hvilket giver mulighed for at vise 16,7 millioner forskellige farver. Der er flere muligheder, men lad os antage, at meddelelsen er blevet skjult ved hjælp af den mindst signifikante del af hver tiende pixel. Det betyder, at hver af disse pixels kun kan repræsentere 8,3 millioner. I mange tilfælde vil farven derfor være en anelse forkert. Man bemærker imidlertid næppe så små variationer – navnlig hvis man, som i vores tilfælde, kun ændrer nogle pixels, og de er spredt vidt omkring. Sammenlignet med det at skjule en meddelelse i en tekstfil er dette langt mere sikkert. Sikkerheden bliver også øget ved, at man vælger et billede, der ikke har store områder med nøjagtig samme farve. Ellers risikerer man, at pixels med andre farver springer i øjnene. Der er

grænser for, hvor megen information man kan gemme på denne måde, og en hovedregel inden for steganografi er, at jo større mængden af skjulte data er, desto større er sandsynligheden for afsløring. Hvis vi holder os til blot 1 ud af 10 pixels, kan vi dog gemme 800.000 bits i et fotografi på 8 megapixels. Det bliver til 100.000 tegn, 20.000 ord eller et dokument på 40 sider." (Rasmus Elm Rasmussen i https://www.altomdata.dk/gem-dine-hemmeligheder-i-fuld-offentlighed; lesedato 12.10.18)

"Grunden til, at meddelelser er så meget nemmere at gemme i et billede end i en tekstfil, er, at billeder indeholder information, der ikke påkalder sig opmærksomhed, hvis den bliver ændret en smule. Det samme gælder for andre former for mediefiler, og audiofiler er en anden udbredt transportform til steganografi." (Rasmus Elm Rasmussen i https://www.altomdata.dk/gem-dine-hemmeligheder-i-fuld-offentlighed; lesedato 12.10.18)

"Ved traditionel kryptering er det relativt nemt at se, at data er krypteret og dermed skjult for offentligheden. Når man befinder sig i lande, hvor dit privatliv og eller dine menneskerettigheder ikke respekteres, kan det være nødvendigt at skjule dine data, frem for blot at kryptere dem. I disse lande vil krypteringsteknologi med steganografi hjælpe. […] Indtil for nyligt har det kun været muligt at gemme relativt små mængder informationer. Typisk skjult i musik eller billedfiler. Dette har været glimrende til at gemme relativt små mængder informationer: Men skal man gemme større mængder, vækker det naturligvis mistanke, hvis man har voldsomt store musikfiler eller 700Mb store billeder." (Thomas Jensen i https://www.prosa.dk/artikel/steganografi/; lesedato 26.09.18)

"[A] file like an image can be stealthily encoded with information. For example, pixel values, brightness, and filter settings for an image are normally changed to affect the image's aesthetic look. But hackers can also manipulate them based on a secret code with no regard for how the inputs make the image look visually. This technique can be used for ethical reasons, such as to evade censorship or embed messages in Facebook photos. But these methods can also be used nefariously. For security defenders the question is how to tell the difference between an image that's been modified for legitimate reasons and one that's been changed to secretly contain malicious information. "Nothing is the same twice, there's no pattern to look for, and the steg[anography] itself is completely undetectable," says Simon Wiseman, the chief technology officer of the British network security firm Deep Secure, which is working on steganography defense. "With advanced statistics, if you're lucky, you might be able to get a hint that something's strange, but that's no good as a defense, because the false positive and false negative rate is still enormous. So detection does not work." […] financial institutions are increasingly dealing with unauthorized data exfiltration attempts in which a bad actor smuggles data like credit card numbers out past the organization's scanners by masking the information in unremarkable files. This strategy can also be used to facilitate insider trading. Possible mitigations all have to do with limiting network access,

monitoring who is interacting with the network, and restricting file adjustment, or sanitizing data before it leaves the network. These can be effective defense strategies, but none of them directly detects or addresses the steganographic techniques attackers are using." (Lily Hay Newman i https://www.wired.com/story/steganography-hacker-lexicon/; lesedato 12.07.18)

" "The cat-and-mouse game between malware developers and security vendors is always on," says Diwakar Dinkar, a research scientist at McAfee who contributed to the company's recent threat report. "Steganography in cyber attacks is easy to implement and enormously tough to detect, so cyber criminals are shifting towards this technique." This proliferation may partly be due to commoditization of steganographic attacks. If a particular technique is easy to carry out, its inventor can sell instructions to cybercriminals who might not have been able to think of it themselves. In this way, shrewd techniques trickle down. The spread of these methods may also come from necessity, as security defenses improve and there are fewer easy hacks available to cyber criminals. […] criminals using steganography to send commands to malware that is already running on a victim's computer." (Lily Hay Newman i https://www.wired.com/story/steganography-hacker-lexicon/; lesedato 12.07.18)

"[M]ottagaren behöver inte ladda ner något program i förväg. Istället kan man till exempel installera ett litet tillägg i sin webbläsare som automatiskt testar den egna nyckeln på allt webbmaterial man surfar igenom – och underrättar användaren när ett riktat meddelande påträffas. På så sätt behöver mottagaren av meddelandet inte ens veta exakt var på en sajt (eller exakt på vilken sajt av många) meddelandet finns – han eller hon surfar bara runt tills det "piper till". Fram till i dag har många steganografi-tekniker varit möjliga att upptäcka eftersom de oftast förlitat sig på att lägga till information i filen. Bram Cohens bidrag till fältet går ut på att skapa en ny implementering av tekniken som inte ska gå att upptäcka. Detta genom att istället mixa upp och ta bort data i filen. […] Med DissidentX ska flera olika meddelanden avsedda för olika mottagare ovetande om varandra kunna gömmas i samma fil. Varje enskilt meddelande i filen kan låsas upp med sitt eget lösenord och krypto-nyckel. Det här tricket är utmärkt för den som exempelvis genom tortyr eller på annat sätt hotas att uppge lösenordet. Då kan personen uppge ett alternativt lösenord som bara "låser upp" ett alternativt dolt meddelande. Koden till DissidentX är så kallad öppen källkod. Det innebär att vem-som-helst kan bygga tjänster och appar på systemet. Man kan alltså anta att det kommer flera olika varianter på tekniken. I kombination med nya implementeringar av Bitcoin-protokollet – som exemplet Dark Wallet – kan tekniken också användas för att gömma eller överföra stora summor pengar mellan parter utan att det ska kunna upptäckas av någon utomstående." (Nanok Bie i https://www.svt.se/nyheter/utrikes/ny-teknik-gommer-hemligheter-rakt-framfor-ogonen-pa-dig; lesedato 10.09.18)

"Amerikansk og fransk etterretningsvesen mener at Osama bin Laden trolig har brukt en teknikk kalt "steganografi" for å planlegge terroraksjonene i USA.

Teknikken lar deg gjemme informasjon i bilder uten av disse forandrer utseende." (https://www.digi.no/artikler/dagens-nettjuvel-gjem-beskjeder-i-bilder/307837; lesedato 27.09.18) "*USA Today* reported on Tuesday that bin Laden and others "are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other websites, U.S. and foreign officials say." The technique, known as steganography, is the practice of embedding secret messages in other messages – in a way that prevents an observer from learning that anything unusual is taking place." (https://www.wired.com/2001/02/bin-laden-steganography-master/; lesedato 20.11.18)

Alle artiklene og litteraturlista til hele leksikonet er tilgjengelig på https://www.litteraturogmedieleksikon.no