Av Helge Ridderstrøm (førsteamanuensis ved OsloMet – storbyuniversitetet)

Sist oppdatert 08.04.24

Om leksikonet: https://www.litteraturogmedieleksikon.no/gallery/om_leksikonet.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)

Grekeren Histaiaeus ønsket å oppfordre Aristagoras fra Milet til å gjøre opprør mot den persiske kongen. “Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to regrow. This was clearly a period of history that tolerated a certain lack of urgency. The messenger, apparently carrying nothing contentious, could travel without being harassed. Upon arriving at his destination he then shaved his head and pointed it at the intended recipient.” (Singh 1999 s. 5)

“Steganography also includes the practice of writing in invisible ink. As far back as the first century A.D., Pliny the Elder explained how the “milk” of the thithymallus plant could be used as an invisible ink. Although transparent after drying, gentle heating chars the ink and turns it brown.” (Singh 1999 s. 6)

“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).

“Named for its inventor, Girolamo Cardano (1501-1576), the Grille system works in the following way: Each recipient has a piece of paper or cardboard with holes cut in it (the grille). When the grille is placed over an innocent-looking message, the holes line up with specific letters in the message, revealing the hidden message within. Intercepting these messages becomes very difficult at this point because the larger message, which often takes up a page, completely blends the shorter, secret message into it. As with jargon code, this type of steganography requires imagination and good writing skills. Cardano's Grille is considered one of the safest ways to transmit a secret message." (Gregory Kipper i https://flylib.com/books/en/1.496.1.23/1/; lesedato 28.03.22)

"During World War I there were several instances where steganography was used with success. One method was called a Turning Grille, which enhanced Cardano's Grille. It looked like a normal grille, a square sheet of cardboard divided into cells with some of the cells punched out. To use the Turning Grille, the encoder would write the first sequence of letters, then rotate the grille 90 degrees and write the second sequence of letters, and so on, rotating the grille after each sequence. The Germans provided their troops with different grilles to be used for messages of different lengths and code-named them based on the number of letters in each grille. The French were able to devise an attack against this system, and the grilles lasted only four months." (Gregory Kipper i https://flylib.com/books/en/1.496.1.40/1/; lesedato 28.03.22)

"Another instance of steganography during World War I was when a woman suspected of working for the Germans was found with a blank piece of paper in the sole of her shoe. As it turned out, this "blank" piece of paper had a message written on it with invisible ink. The message was quickly revealed because it was written in a heat-based invisible ink. From that point on, the Germans quickly got much more clever and began hiding their messages in garments such as scarves and socks. Invisible ink subsections were created within the War Department, and a back-and-forth battle began between the Allies and the Germans. At one point in time, 2000 letters a month were being tested, 50 of which had invisible ink messages that proved useful. […] A British censor was responsible for discovering two German spies when he became suspicious of a large number of cigar orders. The cigar orders were the spies' covert communications, using the numbers and types of cigars to code ship movements. Because of the large volume of cigars that were supposedly being shipped, attention was drawn to their activities. The censor exposed the spies, who were later captured and executed." (Gregory Kipper i https://flylib.com/books/en/1.496.1.40/1/; lesedato 28.03.22)

"A form of steganography was used prior to the Civil War to help slaves escape to freedom. In their book *Hidden in Plain View: A Secret Story of Quilts and the Underground Railroad*, Tobin et al. tell about a code that has been passed down through the generations. In the 1800s, the Underground Railroad was one of the main escape routes used by slaves. Quilts, which were hung outside to dry, became an ideal way to display information inconspicuously. The quilts would have special patterns sewn into them, which would convey messages to prepare or provide direction to escaping slaves who knew what to look for. In this excerpt from *Hidden in Plain View*, you will see an example of this quilt coding. […]

Monkey wrench: This block told the slaves to gather their tools and belongings, and get mentally and physically ready for the journey ahead […]

Wagon wheel: This block was a symbol to begin the journey. Many of the slaves would hide in the bottom of wagons under straw or produce. Some wagons had false bottoms for concealing stowaways […]

Bear paw: This block told slaves to follow bear tracks over the mountain. Bears know the best way to get across a mountain, so following their tracks would lead the slaves safely through the passage […]

Crossroads: This block symbolized the halfway point of the journey […]

Log cabin: This block has a bit of story behind it. It was African tradition that when you passed a stranger you would take a stick and inscribe a symbol of your tribe in the dirt to let the other person know who you were. It acted as a greeting. So to "dig a log cabin on the ground" was a symbol used to communicate with other slaves […]

Bow ties: This block told escaping slaves that it was time for them to shed their old clothes and dress up to better fit into the climate of the city […]

Double wedding rings: This block did not exist until after the Civil War, but the Double Irish Chain quilt did. It symbolized to the slaves the chains that bound them to slavery […]

Flying geese: This block symbolized that it was time to head north. Many slaves, while working or traveling outside, would watch for flocks of geese. They knew when the geese were flying north it was time to follow them […]

Drunkard's path: This block told the slaves not to travel in a straight line because it would be easy for the bounty hunters to find them. Also, in African culture, evil travels in a straight line […]

Stars: This block symbolized the direction of freedom" (Gregory Kipper i https://flylib.com/books/en/1.496.1.39/1/; lesedato 28.03.22).

"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)

“A null cipher is an unencrypted message crafted in such a way that the real message is “camouflaged” in a larger, innocent-sounding message. A null cipher is also sometimes referred to as an open code. Null ciphers have one big drawback: They do not always “sound” quite right. The message may read clumsily, and suspected messages can be detected by mail filters. Although innocent sounding, messages often go undetected and are allowed to flow through. Following are some examples of messages containing null ciphers:

News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

By taking the first letter in each word, the following message can be derived: *Newt is upset because he thinks he is President.*

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank and overwhelming any day.

Taking the third letter in every word, the following message emerges: *Send lawyers guns and money*.” (Gregory Kipper i https://flylib.com/books/en/1.496.1.15/1/; lesedato 28.03.22)

“Although cryptography and steganography are independent, it is possible to both scramble and hide a message to maximize security. For example, the microdot is a form of steganography that became popular during the Second World War. German agents in Latin America would photographically shrink a page of text to a dot less than 1 millimeter in diameter, and then hide this microdot on top of a full stop in an apparently innocuous letter. The first microdot to be spotted by the FBI was in 1941, following a tip-off that the Americans should look for a tiny gleam from the surface of a letter, indicative of smooth film. Thereafter, the Americans could read the contents of most intercepted microdots, except when the German agents had taken the extra precaution of scrambling their message before reducing it. In such cases of cryptography combined with steganography, the Americans were sometimes able to intercept and block communications, but they were prevented from gaining any new information about German spying activity.” (Singh 1999 s. 6-7)

“Steganography and its prevention were also prevalent in World War II. After the attack on Pearl Harbor, the United States enacted a censorship organization. This organization worked to think of ways that coded messages could be passed in the open, and took steps to stop them and destroy the code. Chess games were banned by mail; crossword puzzles were examined or removed from correspondence, newspaper clippings, as well as students’ grades. At one point, knittings were closely monitored to prevent another Madame Defarge, who passed a number of secret messages during the French Revolution. Stamps were removed and replaced with ones of equal value but different denominations or numbers. Children's pictures were replaced, Xs and Os were removed from love letters, and, of course, blank paper was replaced and tested for invisible ink. Censor regulations also prohibited sending any text that was unclear, had personal notes not related to the message, or were in a language other than English, French, Spanish, or Portuguese. Censors would often paraphrase messages, and cables ordering flowers forbade any mention of a flower species. Mass media was also censored. Telephone and telegraph requests for special songs were not allowed, and mail-in song requests would be held for a random amount of time before being played. Personal ads were also censored, including ads for lost dogs. There were no more man-on-the-street interviews, as this could be something an agent could "accidentally" make happen. Children's Christmas lists were also censored." (Gregory Kipper i https://flylib.com/books/en/1.496.1.41/1/; lesedato 28.03.22)

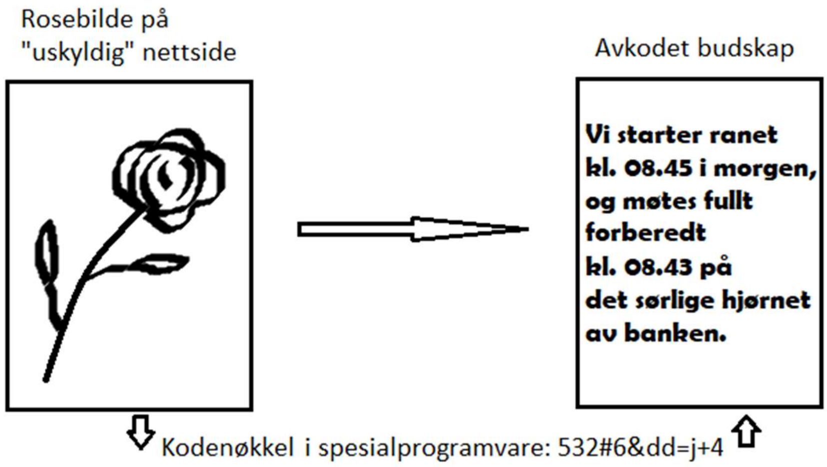
"American abstract expressionism, while perhaps macho, was not immune to attacks by conservatives. In the early 1950s, some right-wingers accused creators of these paintings of hiding information in them to pass on to U.S. enemies. William Hauptman, "The Suppression of Art in the McCarthy Decade," *Artforum* 12, no. 2 (October 1973)" (Staiger 2000 s. 158).

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)

"Margaret Thatcher, the former British Prime Minister, used a method of invisible watermarking in the 1980s. After several cabinet documents had been leaked to the press, Thatcher ordered that the word processors being used by government employees encode their identity in the word spacing of the document. This allowed for disloyal ministers to be quickly found out." (Gregory Kipper i https://flylib.com/books/en/1.496.1.45/1/; lesedato 28.03.22)

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:



Vi starter ranet
kl. 08.45 i morgen,
og møtes fullt
forberedt
kl. 08.43 på
det sørlige hjørnet
av banken.

“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)

Litteraturliste (for hele leksikonet): https://www.litteraturogmedieleksikon.no/gallery/litteraturliste.pdf

Alle artiklene i leksikonet er tilgjengelig på https://www.litteraturogmedieleksikon.no