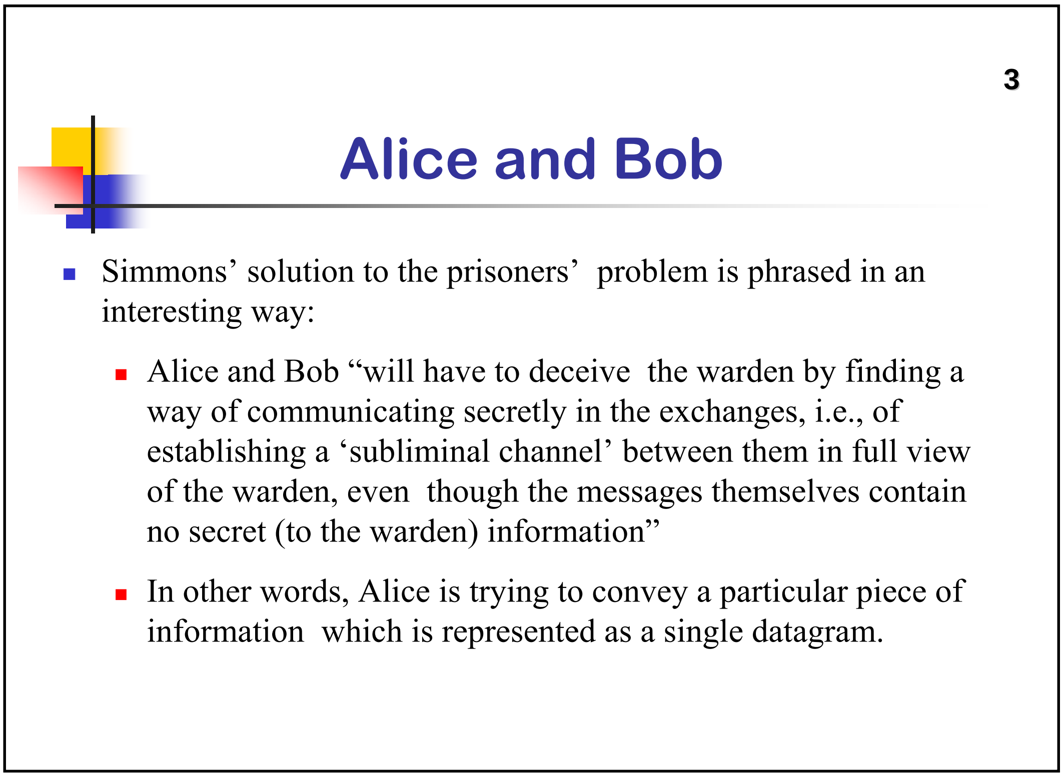
Steganography

Dr.Talal Alkharobi

2

Alice and Bob

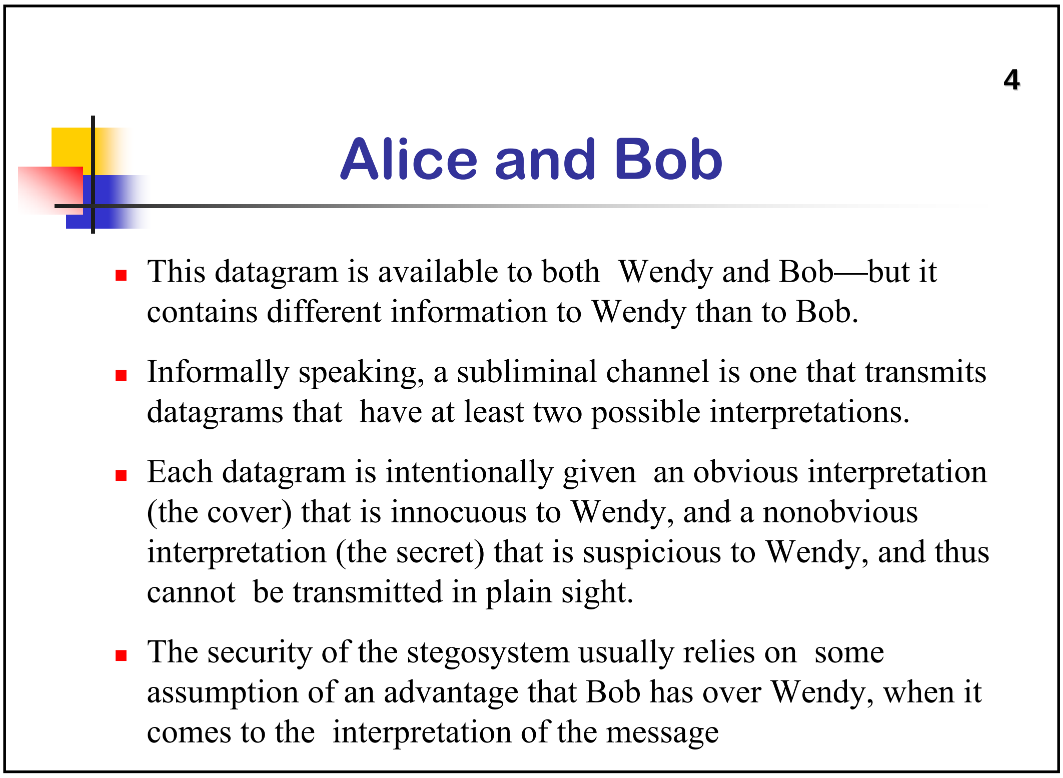
- In 1984, Gustavus Simmons illustrated what is now widely known as the prisoners' problem:
  - Two accomplices in a crime, Alice and Bob, are arrested in separate cells.
  - They want to coordinate an escape plan, but their only means of communication is by way of messages conveyed for them by Wendy the warden.
  - Should Alice and Bob try to exchange messages that are not completely open to Wendy, or ones that seem suspicious to her, they will be put into a high security prison



3

Alice and Bob

- Simmons' solution to the prisoners' problem is phrased in an interesting way:
  - Alice and Bob "will have to deceive the warden by finding a way of communicating secretly in the exchanges, i.e., of establishing a 'subliminal channel' between them in full view of the warden, even though the messages themselves contain no secret (to the warden) information"
  - In other words, Alice is trying to convey a particular piece of information which is represented as a single datagram.



4

Alice and Bob

- This datagram is available to both Wendy and Bob—but it contains different information to Wendy than to Bob.
- Informally speaking, a subliminal channel is one that transmits datagrams that have at least two possible interpretations.
- Each datagram is intentionally given an obvious interpretation (the cover) that is innocuous to Wendy, and a nonobvious interpretation (the secret) that is suspicious to Wendy, and thus cannot be transmitted in plain sight.
- The security of the stegosystem usually relies on some assumption of an advantage that Bob has over Wendy, when it comes to the interpretation of the message

5

Alice and Bob

- Bob can interpret the message with regard to its secret meaning, while Wendy can only interpret the message as the cover.

6

Steganography

- The art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message;
- In contrast to cryptography, the existence of the message itself is not disguised, but the content is obscured.
- The word "Steganography" is of Greek origin and means "covered, or hidden writing".

7

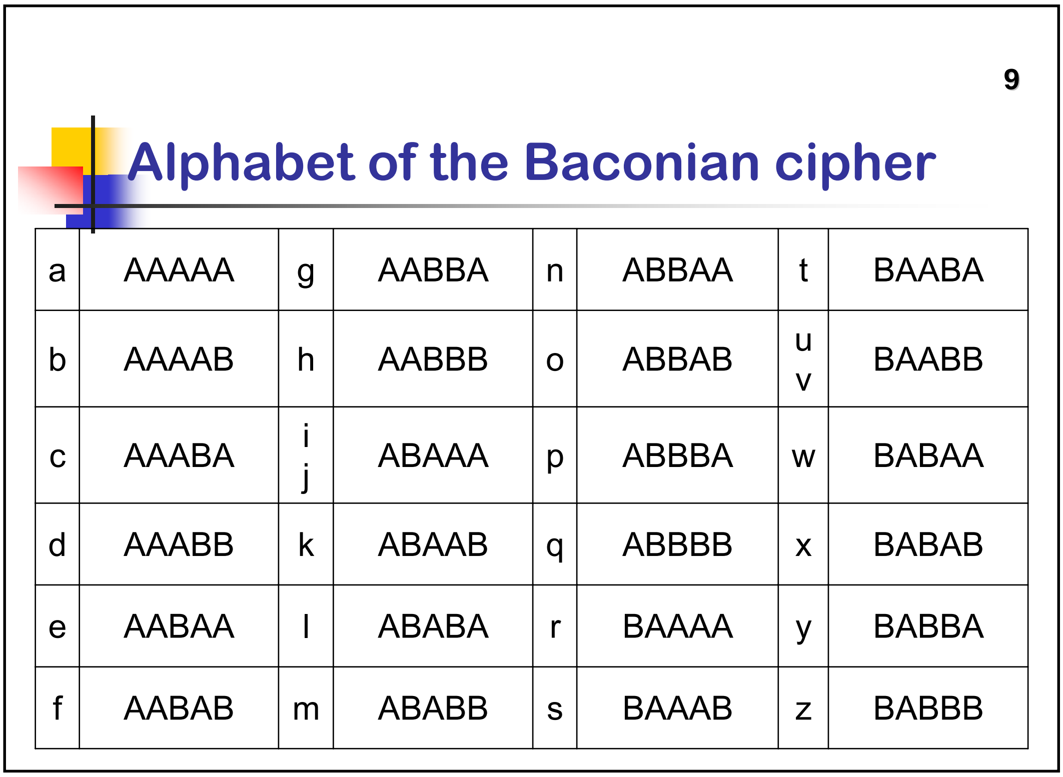
Steganography very old

- Its ancient origins can be traced back to 440 BC. Herodotus mentions two examples of Steganography in The Histories of Herodotus
  - Demeratus sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax. Wax tablets were in common use then as re-usable writing surface, sometimes used for shorthand.
  - Another ancient example is that of Histiaeus, who shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden.

8

Bacon's (Baconian) cipher

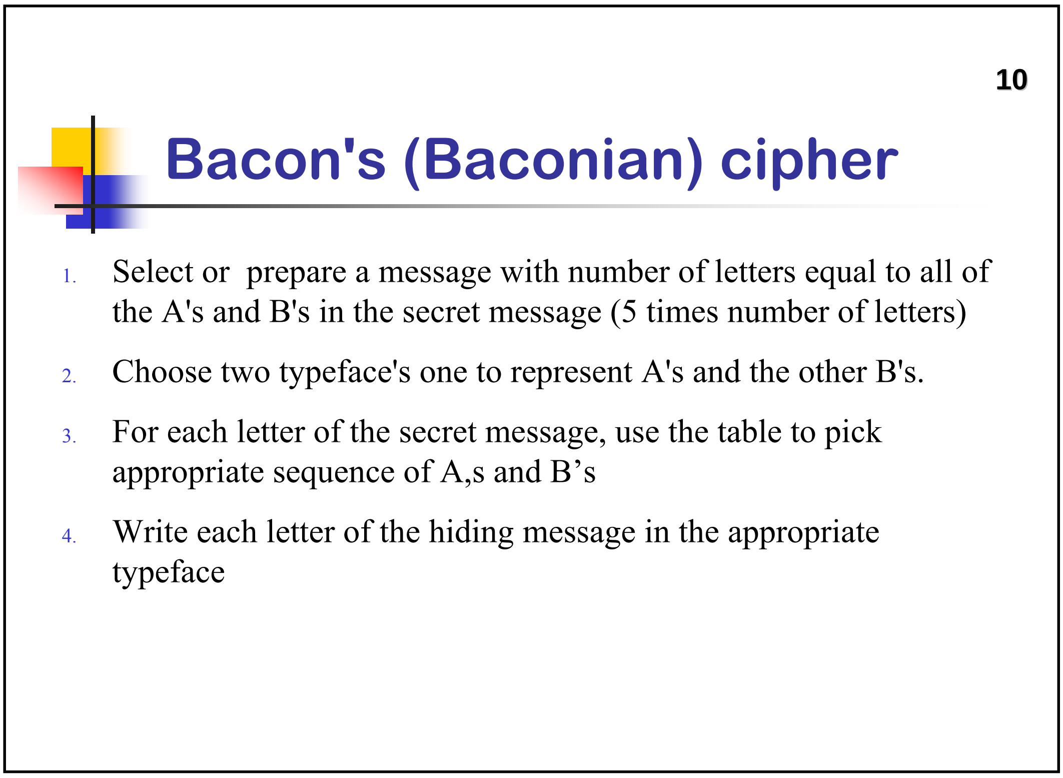
- A method of hiding a secret message as opposed to a true cipher) devised by Francis Bacon (1561-1626).
- A message is concealed in the presentation of text, rather than its content.
- To encode a message, each letter of the plain text is replaced by a group of five of the letters 'A' or 'B'.
- This replacement is done according to the alphabet of the Baconian cipher
- The writer must make use of two different typefaces for this cipher.



9

Alphabet of the Baconian cipher

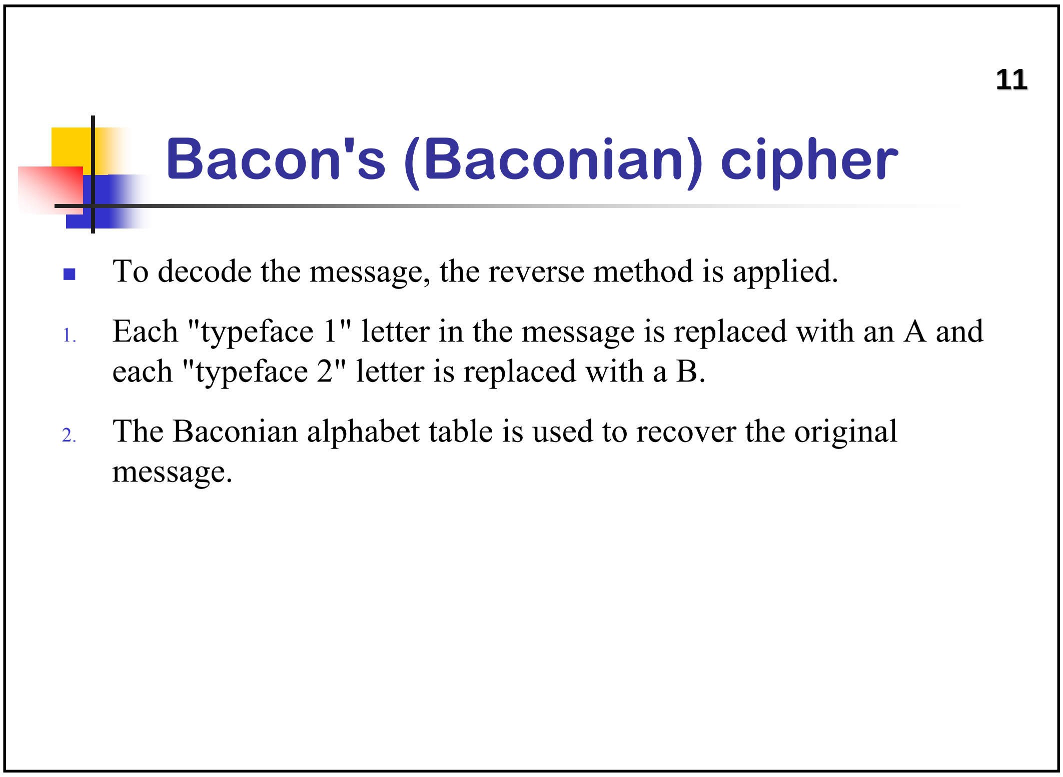
a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u v	BAABB
c	AAABA	i j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB



10

Bacon's (Baconian) cipher

1. Select or prepare a message with number of letters equal to all of the A's and B's in the secret message (5 times number of letters)
2. Choose two typeface's one to represent A's and the other B's.
3. For each letter of the secret message, use the table to pick appropriate sequence of A,s and B’s
4. Write each letter of the hiding message in the appropriate typeface

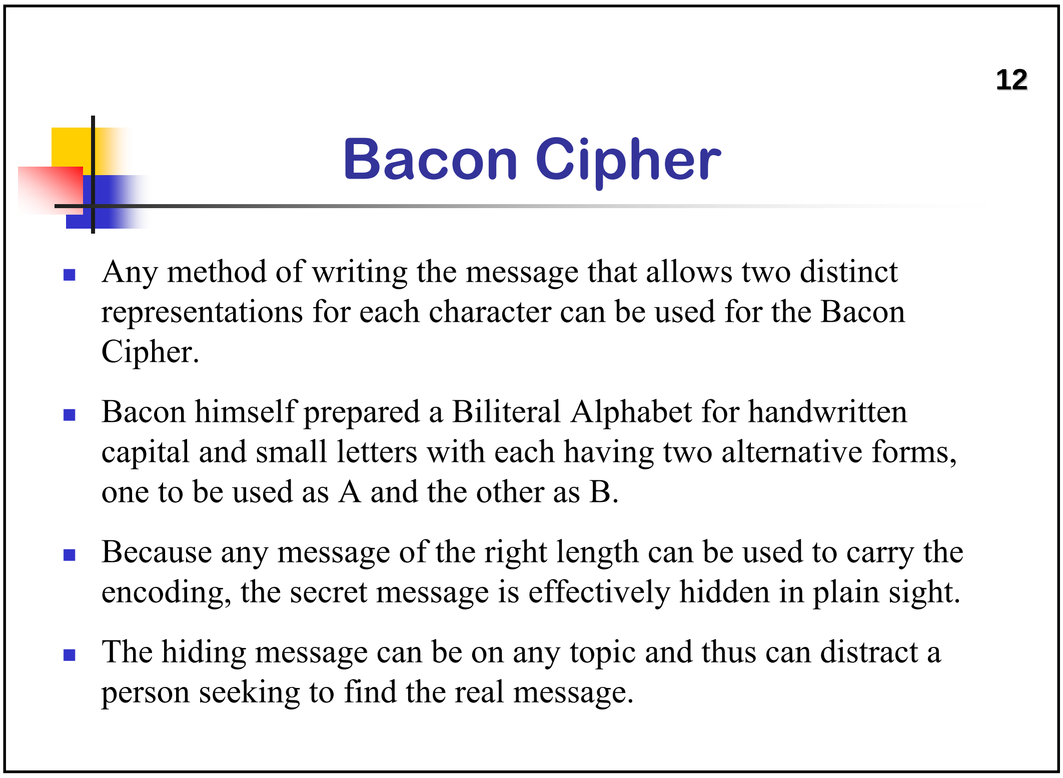


11

Bacon's (Baconian) cipher

- To decode the message, the reverse method is applied.

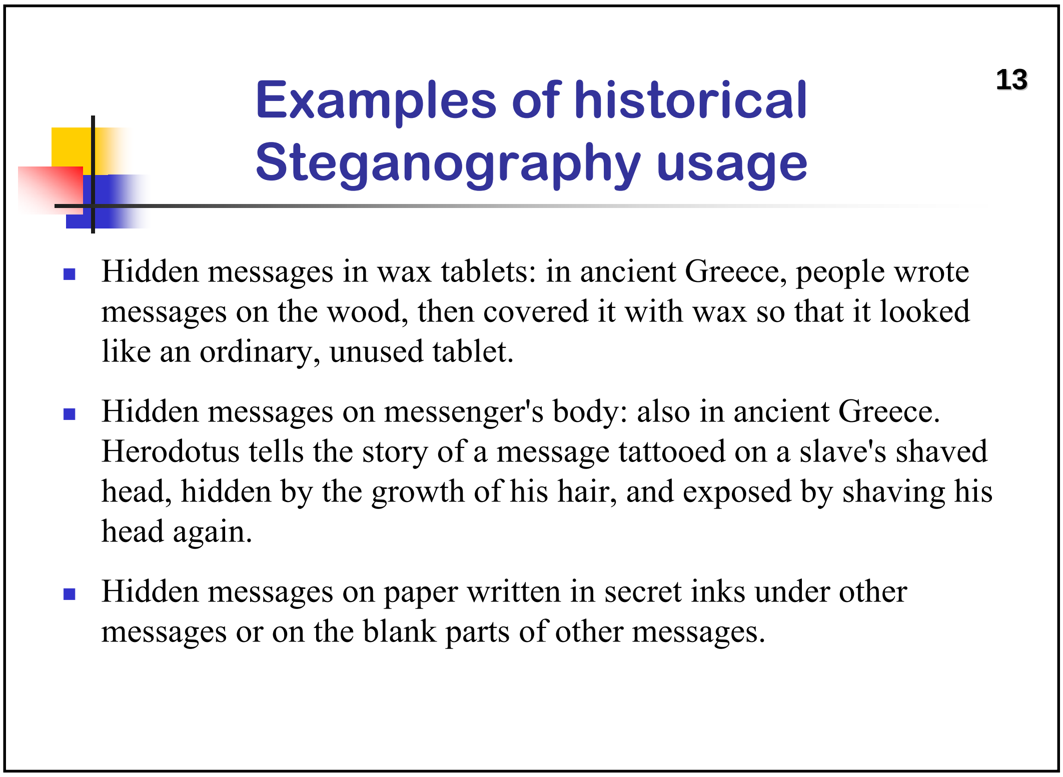
1. Each "typeface 1" letter in the message is replaced with an A and each "typeface 2" letter is replaced with a B.
2. The Baconian alphabet table is used to recover the original message.



12

Bacon Cipher

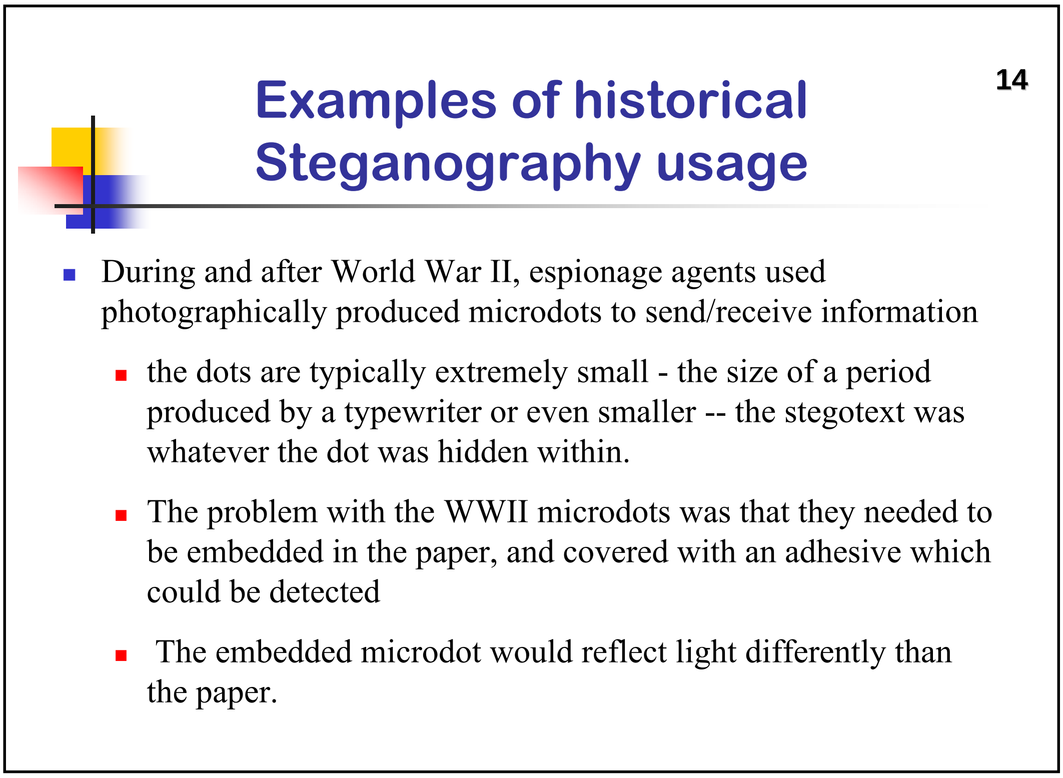
- Any method of writing the message that allows two distinct representations for each character can be used for the Bacon Cipher.
- Bacon himself prepared a Biliteral Alphabet for handwritten capital and small letters with each having two alternative forms, one to be used as A and the other as B.
- Because any message of the right length can be used to carry the encoding, the secret message is effectively hidden in plain sight.
- The hiding message can be on any topic and thus can distract a person seeking to find the real message.



13

Examples of historical Steganography usage

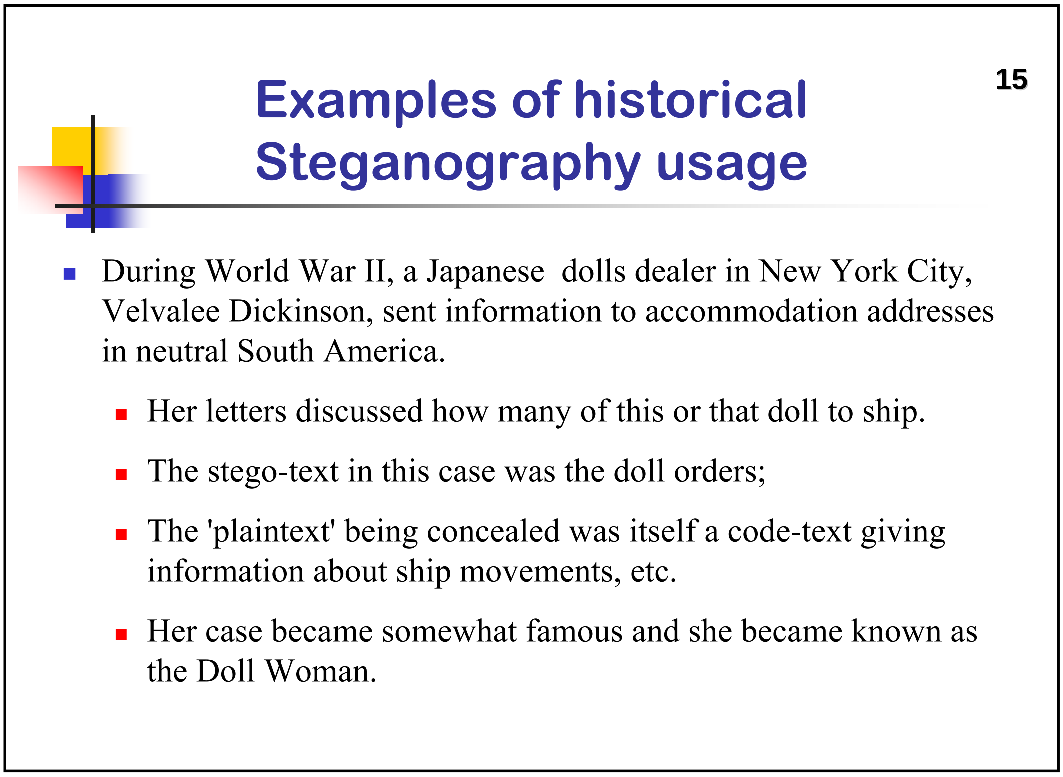
- Hidden messages in wax tablets: in ancient Greece, people wrote messages on the wood, then covered it with wax so that it looked like an ordinary, unused tablet.
- Hidden messages on messenger's body: also in ancient Greece. Herodotus tells the story of a message tattooed on a slave's shaved head, hidden by the growth of his hair, and exposed by shaving his head again.
- Hidden messages on paper written in secret inks under other messages or on the blank parts of other messages.



14

Examples of historical Steganography usage

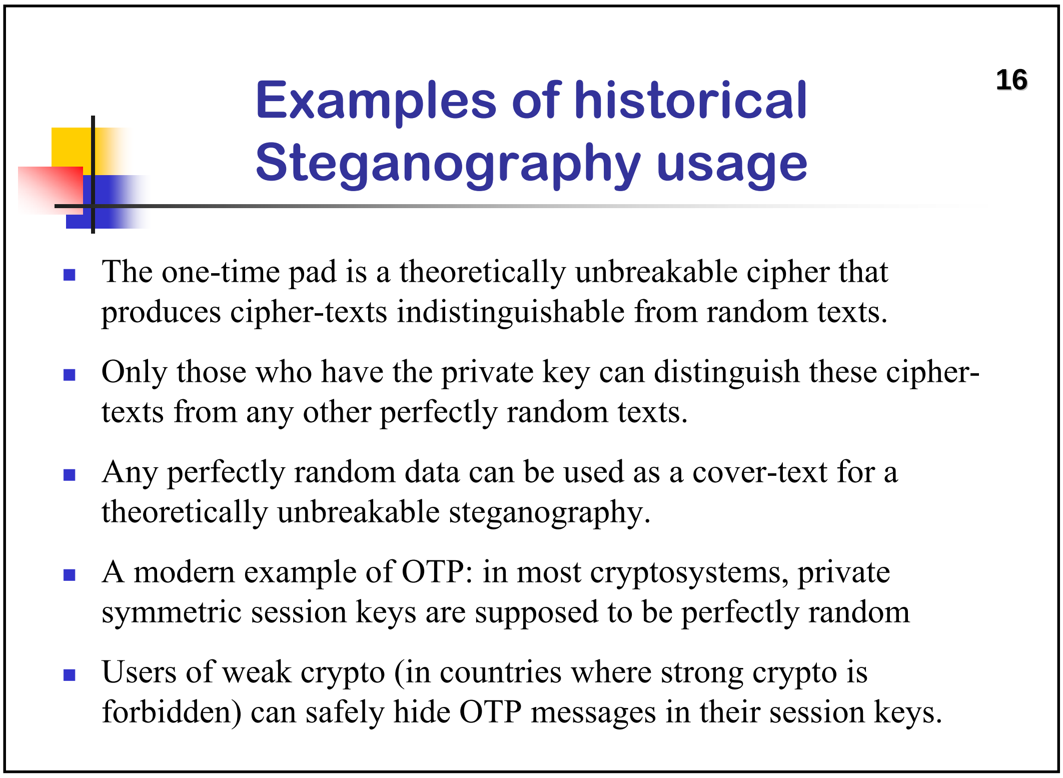
- During and after World War II, espionage agents used photographically produced microdots to send/receive information
  - the dots are typically extremely small - the size of a period produced by a typewriter or even smaller -- the stegotext was whatever the dot was hidden within.
  - The problem with the WWII microdots was that they needed to be embedded in the paper, and covered with an adhesive which could be detected
  - The embedded microdot would reflect light differently than the paper.



15

Examples of historical Steganography usage

- During World War II, a Japanese dolls dealer in New York City, Velvalee Dickinson, sent information to accommodation addresses in neutral South America.
  - Her letters discussed how many of this or that doll to ship.
  - The stego-text in this case was the doll orders;
  - The 'plaintext' being concealed was itself a code-text giving information about ship movements, etc.
  - Her case became somewhat famous and she became known as the Doll Woman.



16

Examples of historical Steganography usage

- The one-time pad is a theoretically unbreakable cipher that produces cipher-texts indistinguishable from random texts.
- Only those who have the private key can distinguish these cipher-texts from any other perfectly random texts.
- Any perfectly random data can be used as a cover-text for a theoretically unbreakable steganography.
- A modern example of OTP: in most cryptosystems, private symmetric session keys are supposed to be perfectly random
- Users of weak crypto (in countries where strong crypto is forbidden) can safely hide OTP messages in their session keys.

17

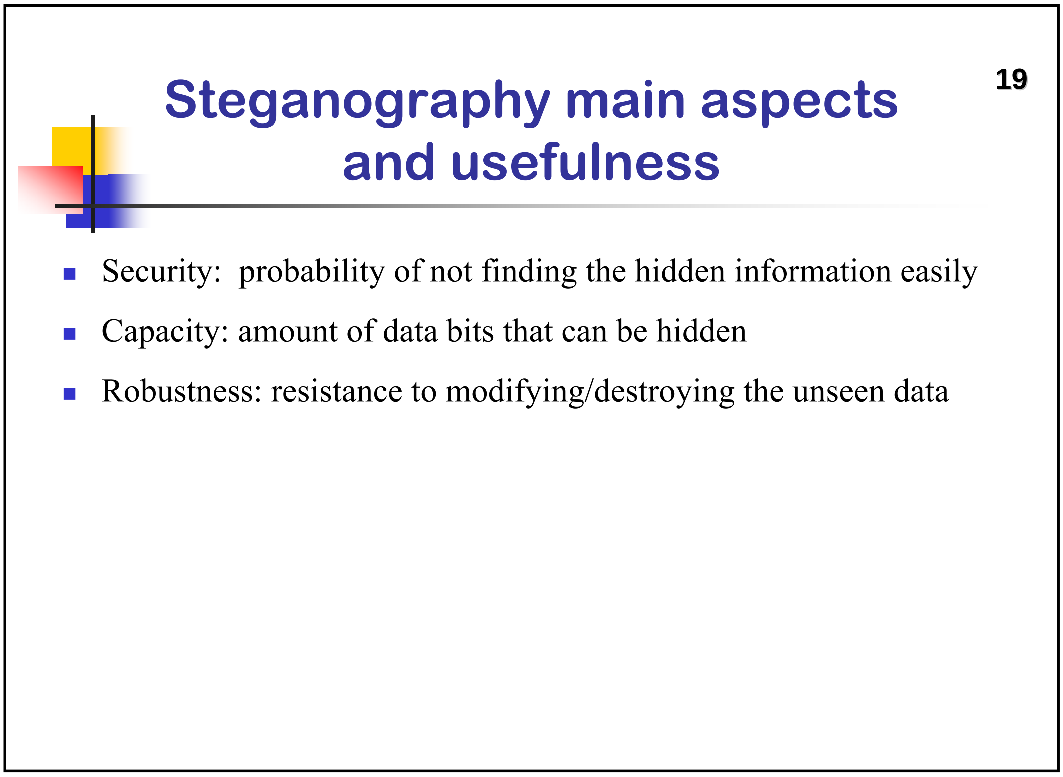
Steganography

- A steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message.
- This apparent message is the cover-text. A message may be hidden by using invisible ink between the visible lines of a documents.
- The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.
- An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal

18

Steganography

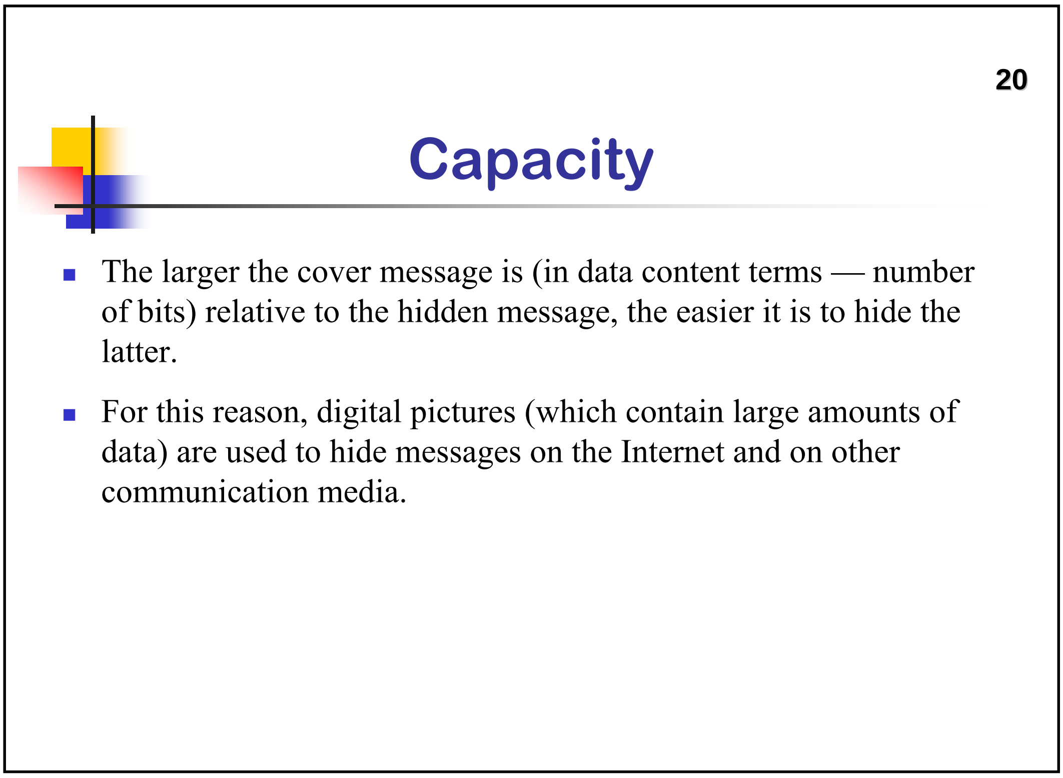
- A steganographic message (the plaintext) is often first encrypted by some traditional means, and then a cover-text is modified in some way to contain the encrypted message (cipher-text), resulting in stego-text.
- For example, the letter size, spacing, typeface, or other characteristics of a cover-text can be manipulated to carry the hidden message; only the recipient (who must know the technique used) can recover the message and then decrypt it.



19

Steganography main aspects and usefulness

- Security: probability of not finding the hidden information easily
- Capacity: amount of data bits that can be hidden
- Robustness: resistance to modifying/destroying the unseen data



20

Capacity

- The larger the cover message is (in data content terms — number of bits) relative to the hidden message, the easier it is to hide the latter.
- For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media.

21

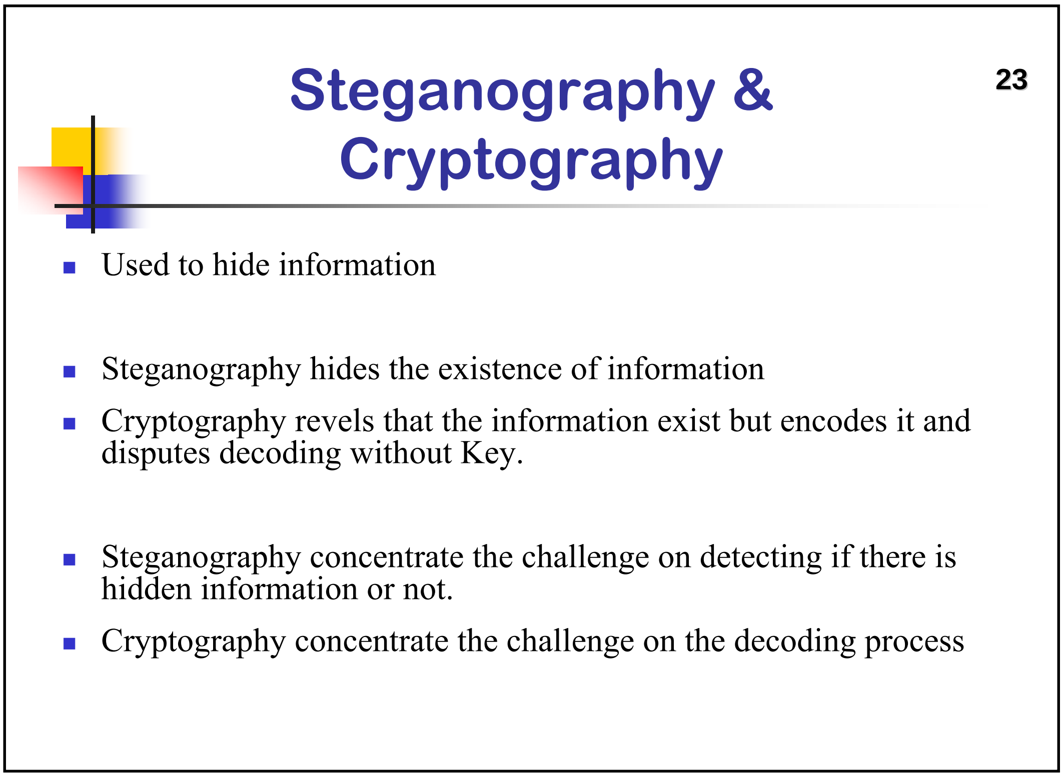
Security

- The objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the injection of the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible;
- That is to say, the changes are indistinguishable from the noise floor of the carrier.
- From an information theoretical point of view, this means that the channel must have more capacity than the 'surface' signal requires, that is, there must be redundancy.

22

Security

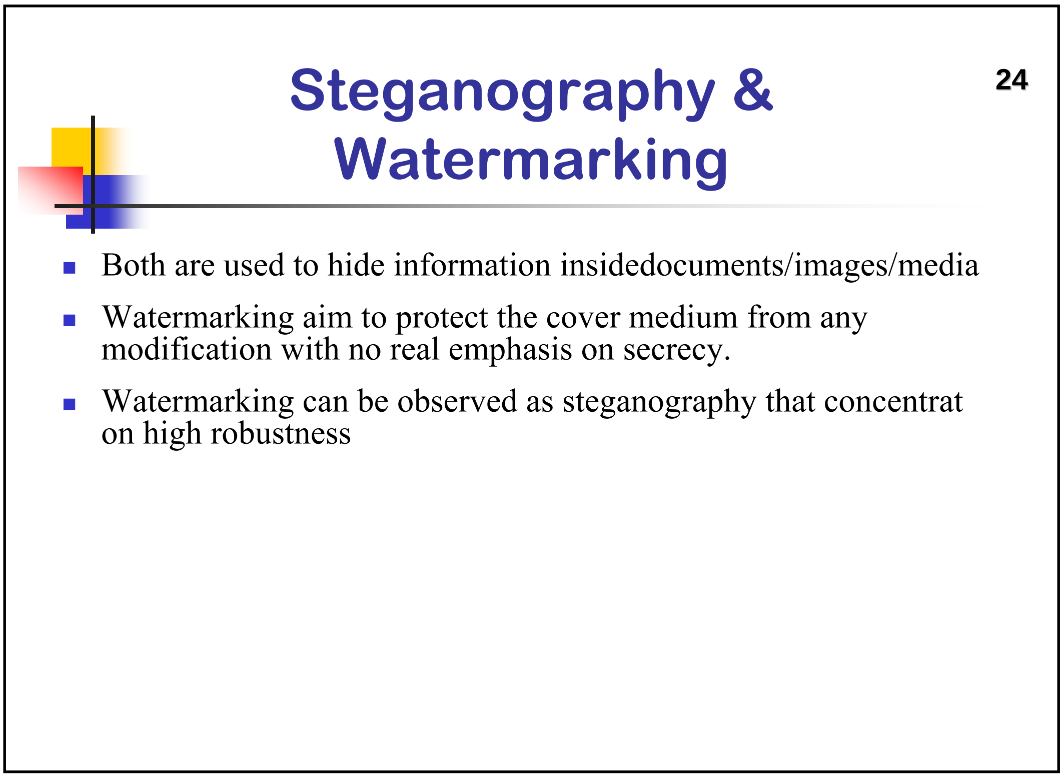
- In digital image, there is noise from the imaging element;
- In digital audio, there is noise from recording techniques or amplification equipment.
- In general, electronics that digitize an analog signal suffer from several noise sources such as thermal noise, flicker noise, and shot noise.
- This noise provides enough variation in the captured digital information that it can be exploited as a noise cover for hidden data.



Steganography & Cryptography

23

- Used to hide information
- Steganography hides the existence of information
- Cryptography revels that the information exist but encodes it and disputes decoding without Key.
- Steganography concentrate the challenge on detecting if there is hidden information or not.
- Cryptography concentrate the challenge on the decoding process



Steganography & Watermarking

24

- Both are used to hide information insidedocuments/images/media
- Watermarking aim to protect the cover medium from any modification with no real emphasis on secrecy.
- Watermarking can be observed as steganography that concentrat on high robustness

25

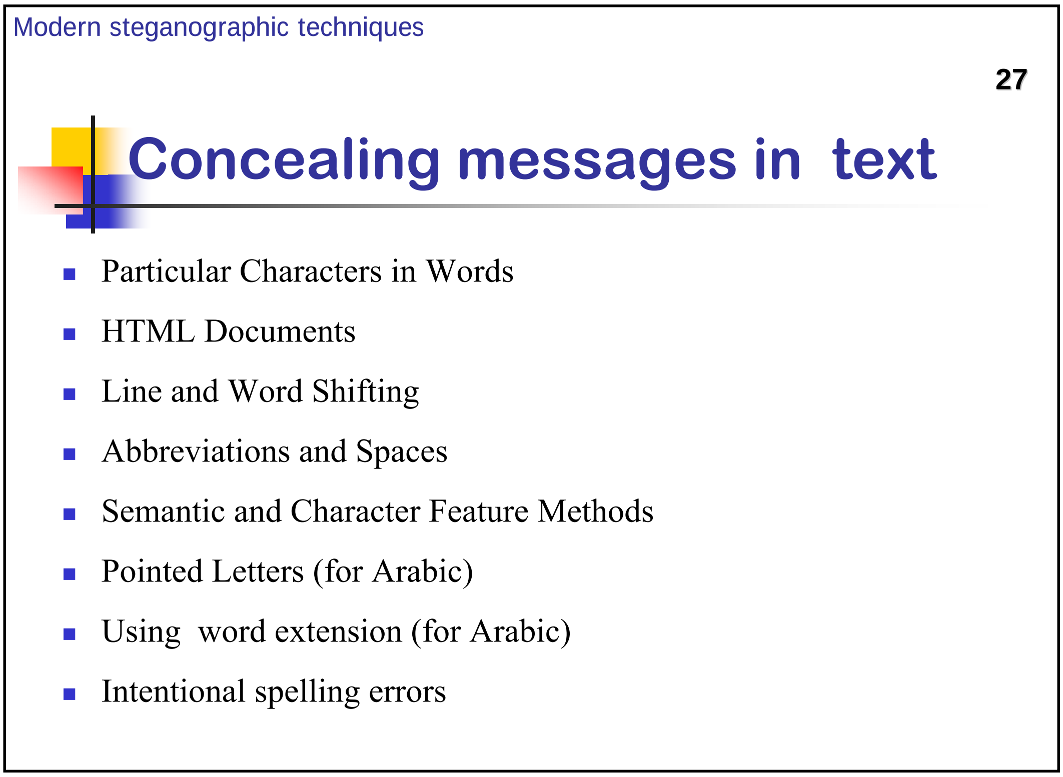
Steganographic techniques

- Concealing messages in text, images, sound or video
- Concealing data within encrypted data.
- Chaffing and winnowing
- Invisible ink
- Null ciphers
- Concealed messages in tampered executable files,
- Injecting imperceptible delays
- Content-Aware Steganography

26

Steganography

- Another digital carrier can be the network protocols: Covert Transmission Control Protocol by Craig Rowland, for example, forms covert communications channels using the Identification field in Internet Protocol packets or the sequence number field in Transmission Control Protocol segments

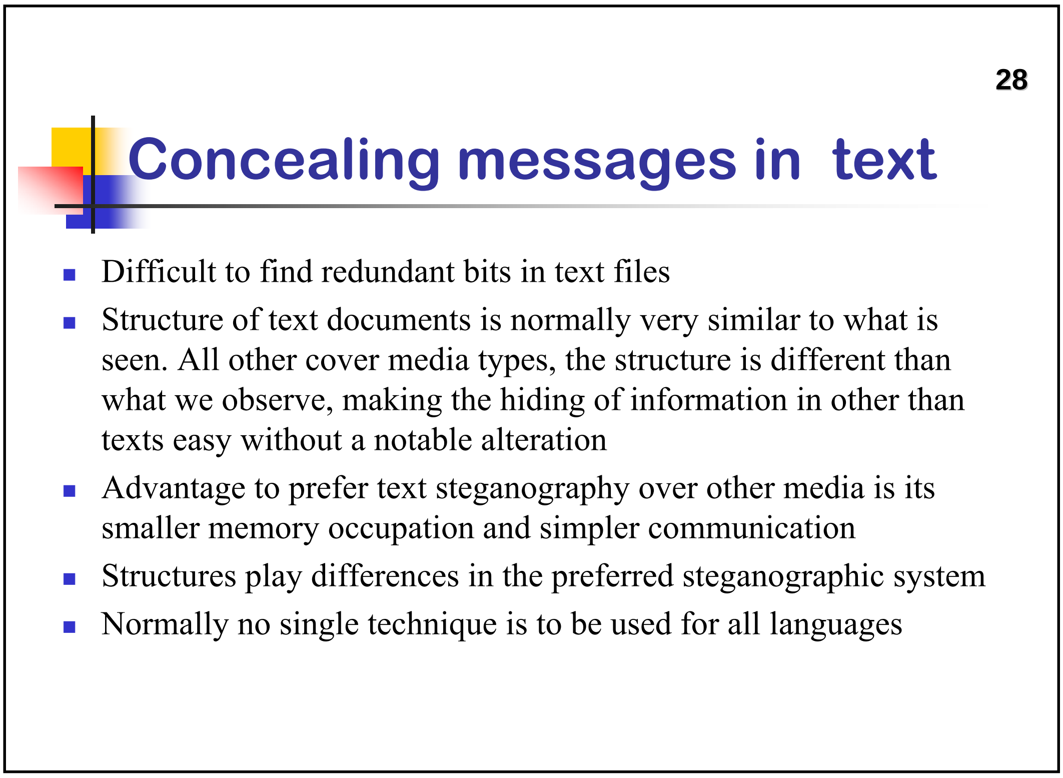


Modern steganographic techniques

27

Concealing messages in text

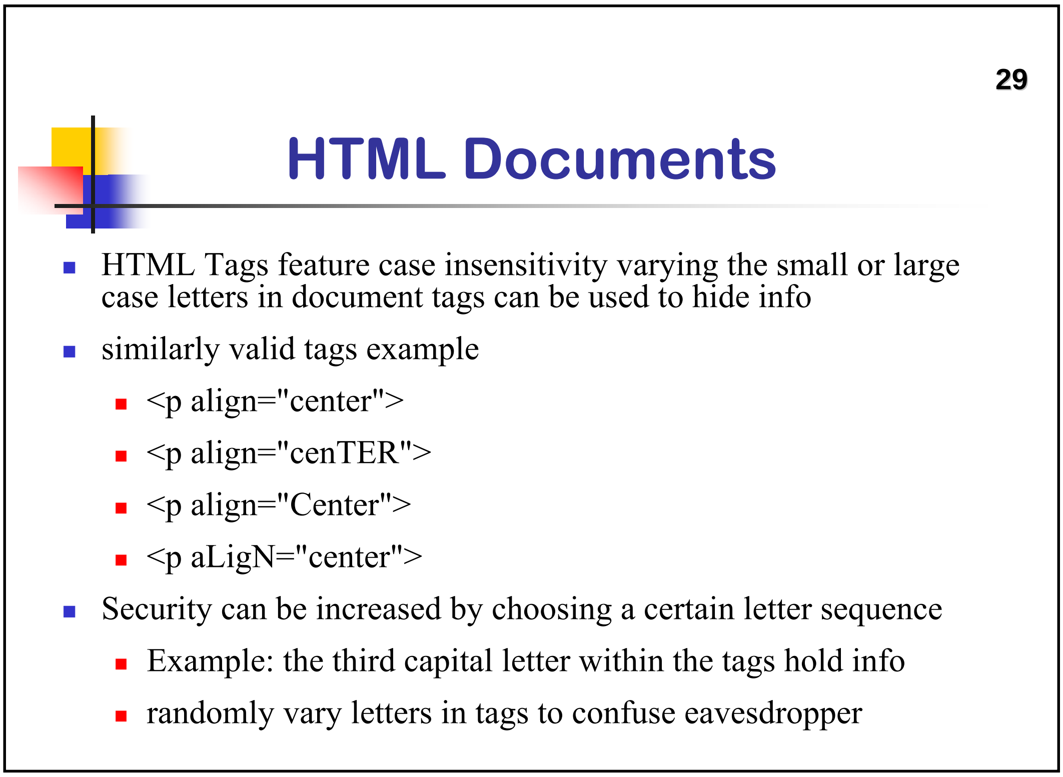
- Particular Characters in Words
- HTML Documents
- Line and Word Shifting
- Abbreviations and Spaces
- Semantic and Character Feature Methods
- Pointed Letters (for Arabic)
- Using word extension (for Arabic)
- Intentional spelling errors



28

Concealing messages in text

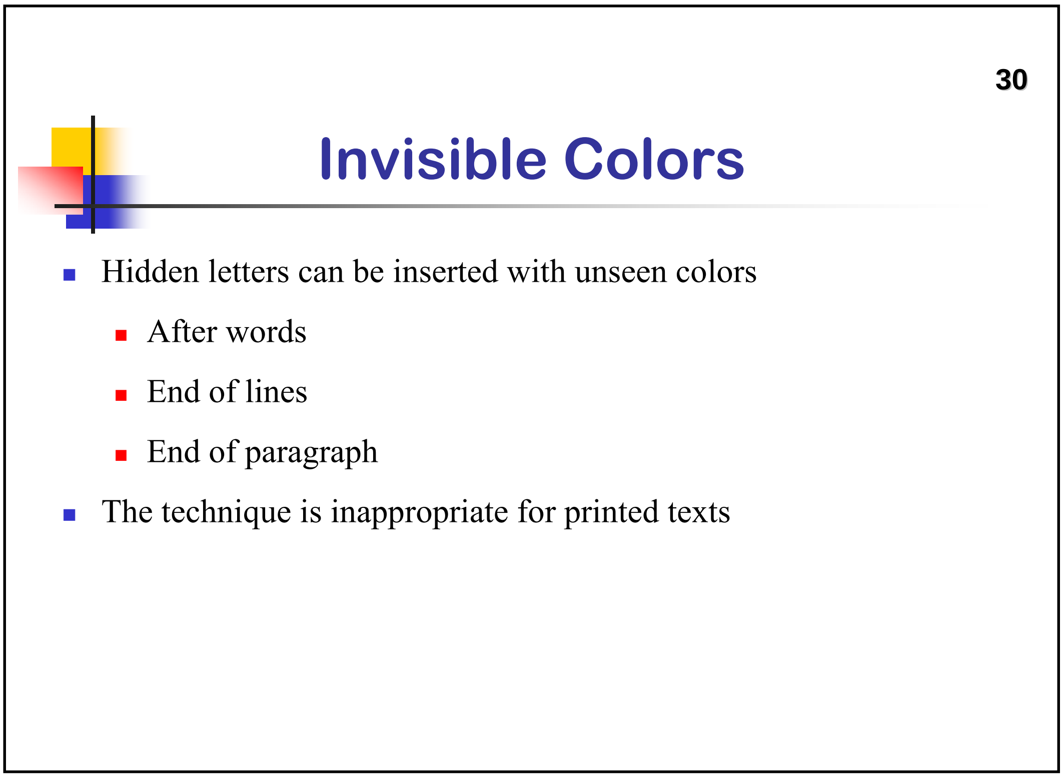
- Difficult to find redundant bits in text files
- Structure of text documents is normally very similar to what is seen. All other cover media types, the structure is different than what we observe, making the hiding of information in other than texts easy without a notable alteration
- Advantage to prefer text steganography over other media is its smaller memory occupation and simpler communication
- Structures play differences in the preferred steganographic system
- Normally no single technique is to be used for all languages



29

HTML Documents

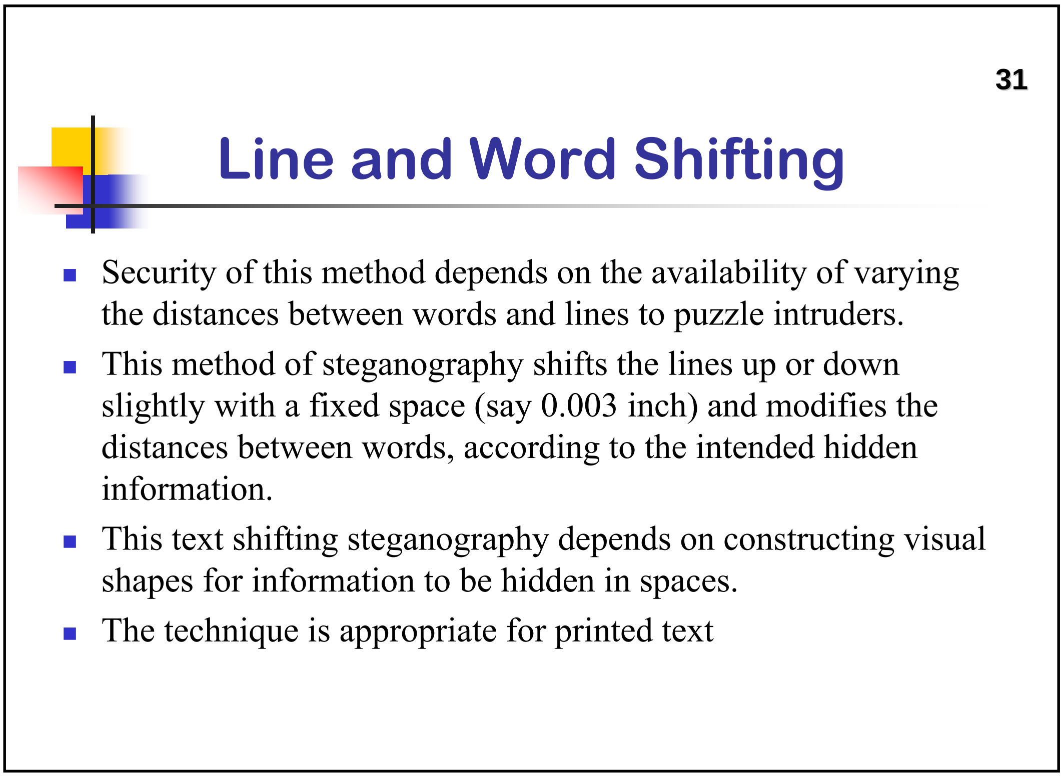
- HTML Tags feature case insensitivity varying the small or large case letters in document tags can be used to hide info
- similarly valid tags example
  - <p align="center">
  - <p align="cenTER">
  - <p align="Center">
  - <p aLigN="center">
- Security can be increased by choosing a certain letter sequence
  - Example: the third capital letter within the tags hold info
  - randomly vary letters in tags to confuse eavesdropper



30

Invisible Colors

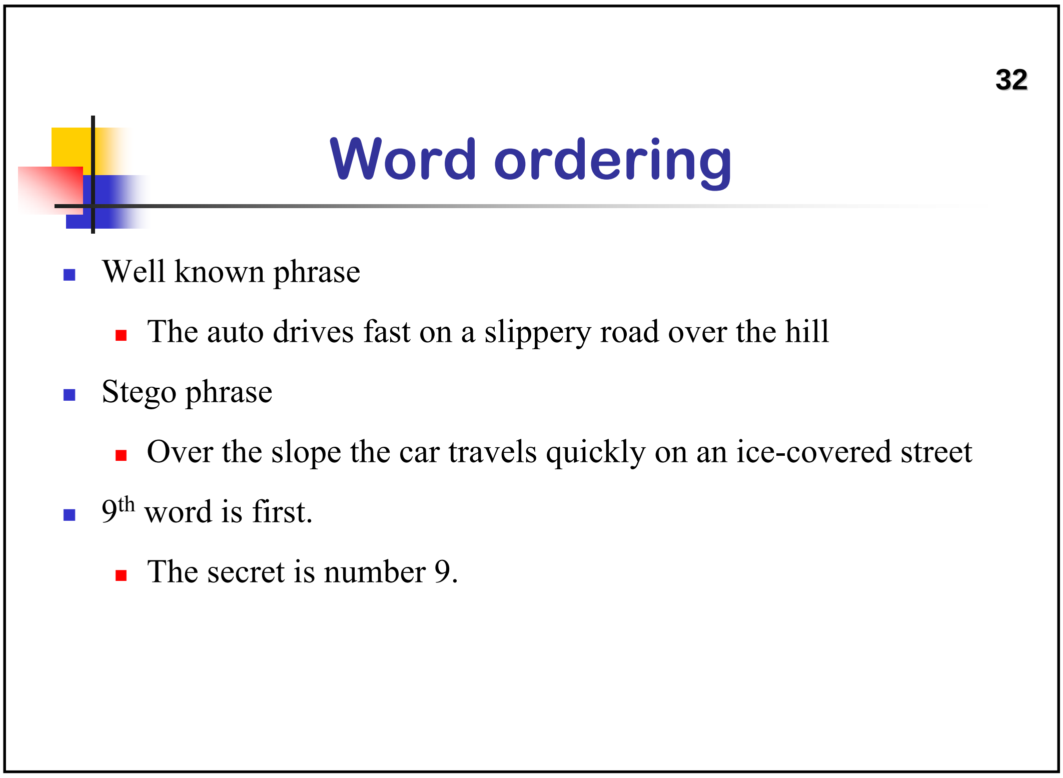
- Hidden letters can be inserted with unseen colors
  - After words
  - End of lines
  - End of paragraph
- The technique is inappropriate for printed texts



31

Line and Word Shifting

- Security of this method depends on the availability of varying the distances between words and lines to puzzle intruders.
- This method of steganography shifts the lines up or down slightly with a fixed space (say 0.003 inch) and modifies the distances between words, according to the intended hidden information.
- This text shifting steganography depends on constructing visual shapes for information to be hidden in spaces.
- The technique is appropriate for printed text



32

Word ordering

- Well known phrase
  - The auto drives fast on a slippery road over the hill
- Stego phrase
  - Over the slope the car travels quickly on an ice-covered street
- 9th word is first.
  - The secret is number 9.

33

Spaces

- By adding extra white-spaces between words, or at end of lines or paragraph of the text
- Does not reveal secrecy to the normal reader → high security
- Cannot hide too much information → low capacity
- Electronic text editors automatically remove extra white-spaces → low robustness

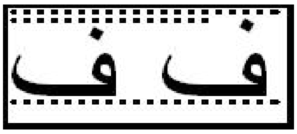
34

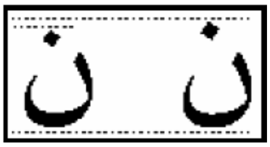
Character Feature Steganography

- Changes some of the features of the text characters.
- Example, the most significant bits of some characters are extended to hold bits of the hidden information.
- Character steganography can hold a large quantity of secret information without making normal readers aware of the existence of such information in the text.

35

Pointed Letters

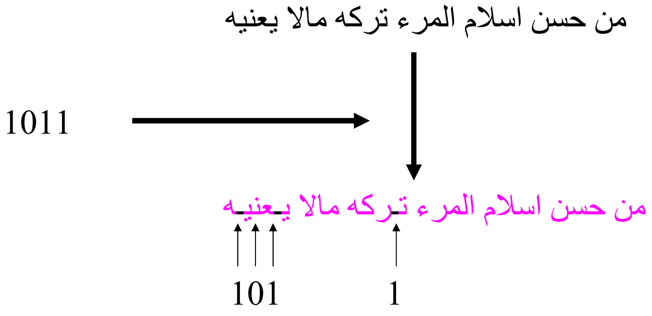




un-pointed letters	pointed letters
ا ح د ر س ص ط ع ك ل م هـ و	ب ت ث ج خ ذ ز ش ض ظ غ ف ق ن ي

36

Pointed Letters & Extensions



من حسن اسلام المرء تركه مالا يعنيه

1011

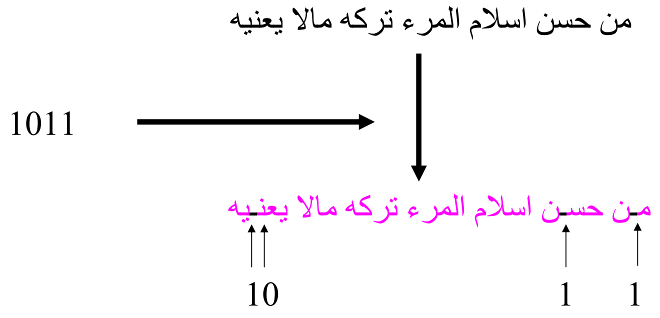
من حسن اسلام المرء تـركه مالا يـعنيـه

101 1

37

Pointed Letters & Extensions (Special for Arabic)

- Steganography example adding extensions before pointed letters.



من حسن اسلام المرء تركه مالا يعنيه

1011

مـن حسـن اسلام المرء تركه مالا يعنـيه

10 1 1

Modern steganographic techniques

38

Concealing messages in images, sound or video

- Cover data should not be significantly modified (not noticable by human)
- Distortion cannot be eliminated so error-correcting codes need to be included whenever required
- Optionally played at slower or faster speed is possible with video
- Video Encoded Invisible Light

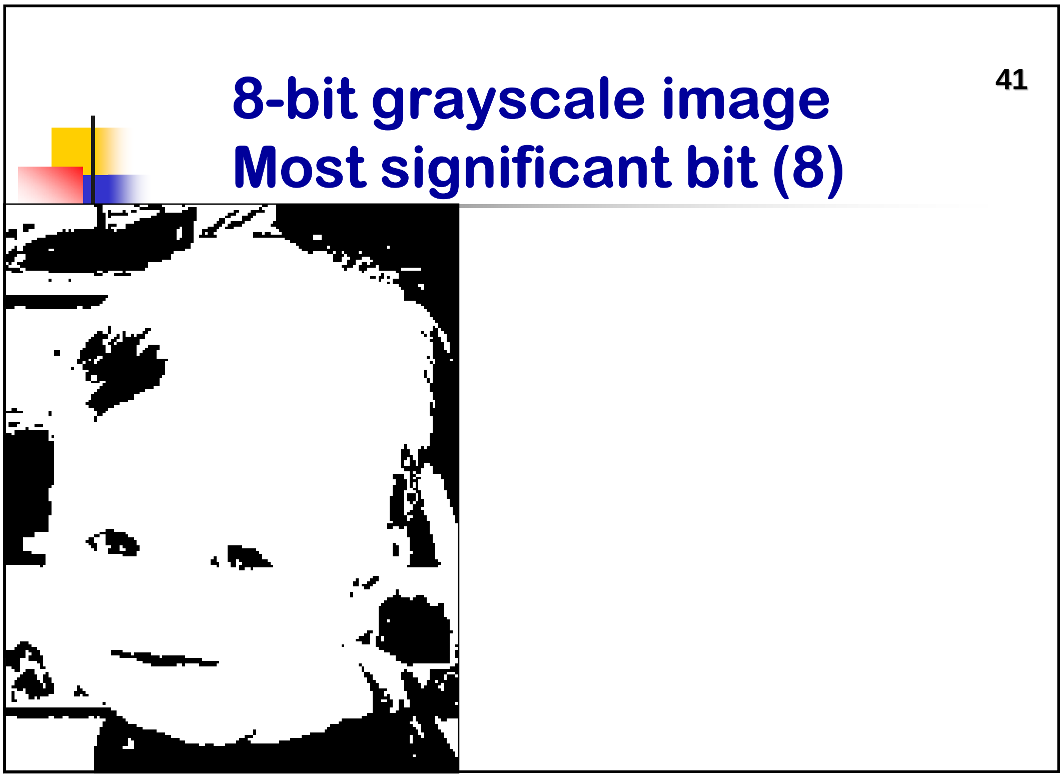
39

Concealing messages in images, sound or video

- Ways to hide information in images
  - Least significant bit(s) (BMP)
  - Palette Shifts (GIF)
  - Discrete Cosine Transforms (JPG)

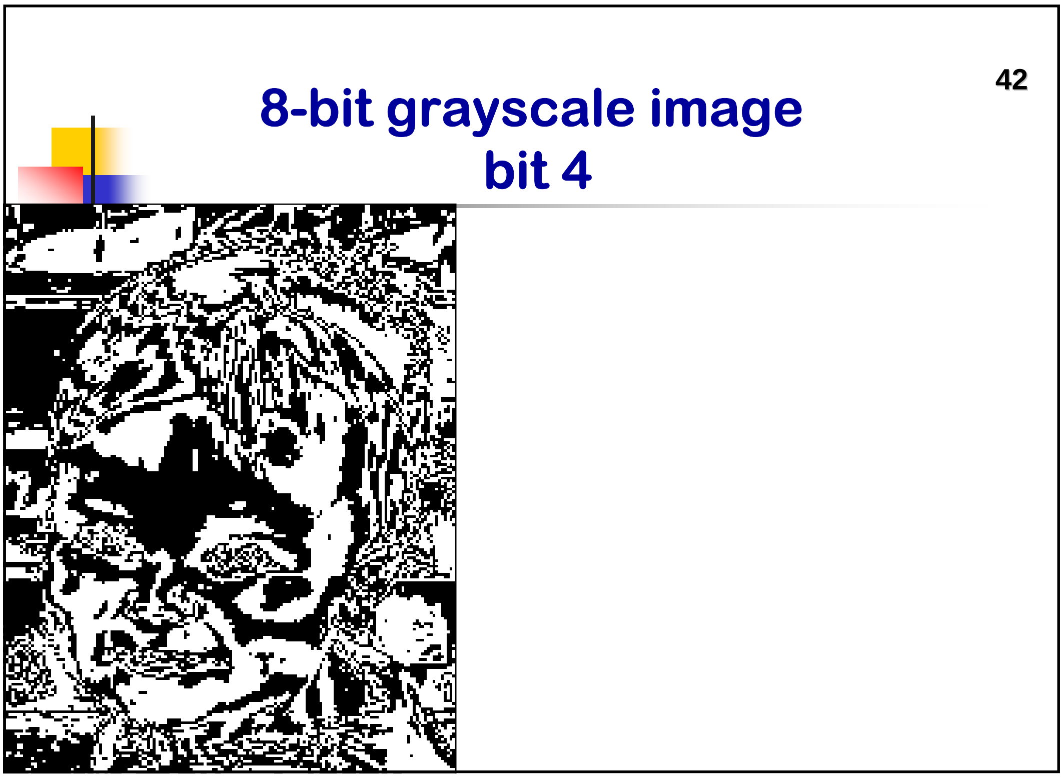
40

8-bit grayscale source image



41

8-bit grayscale image Most significant bit (8)

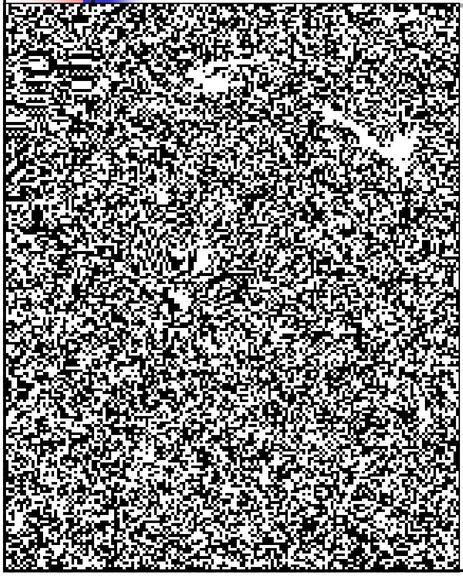


42

8-bit grayscale image bit 4

43

8-bit grayscale image Least significant bit (0)

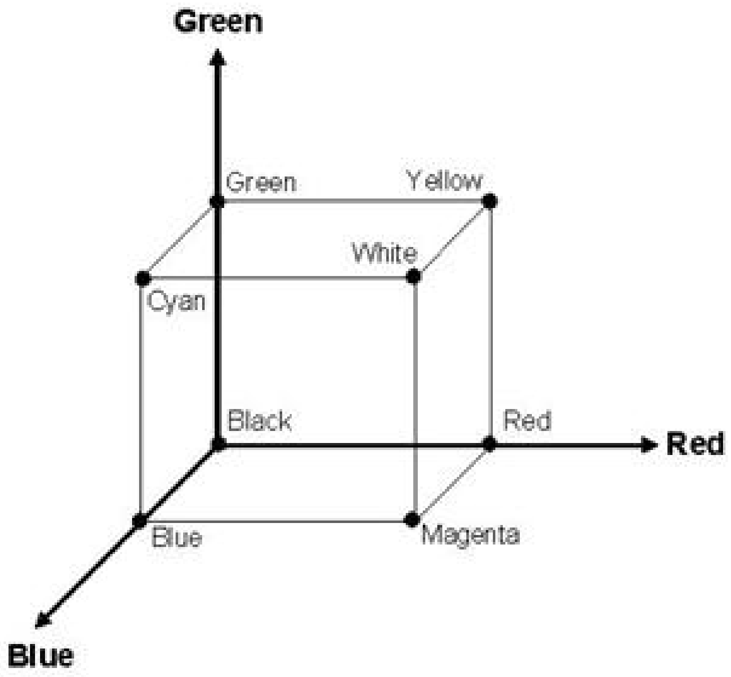


44

RGB

- A 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel.
- If we consider just the blue there will be 256 different values
- The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye.
- Therefore, the least significant bit can be used (more or less undetectably) for something else other than color information.
- If we do it with the green and the red as well we can get one letter of ASCII text for every three pixels.

45



46

Discrete Cosine Transform (DCT) Wavelet transform

- Message is embedded into cover image by modulating the original coefficients in transform domain
- To encode:
  - Take the DCT or wavelet transform of the cover image
  - Find the coefficients below a certain threshold
  - Replace these bits with bits to be hidden (can use LSB insertion)
  - Take the inverse transform
  - Store as regular image.

47

Discrete Cosine Transform (DCT) Wavelet transform

- To decode this image to get the message:
  - Find the coefficients below a certain threshold
  - Extract bits of data from these coefficients
  - Combine bits into actual message

48

Audio Stegrnography

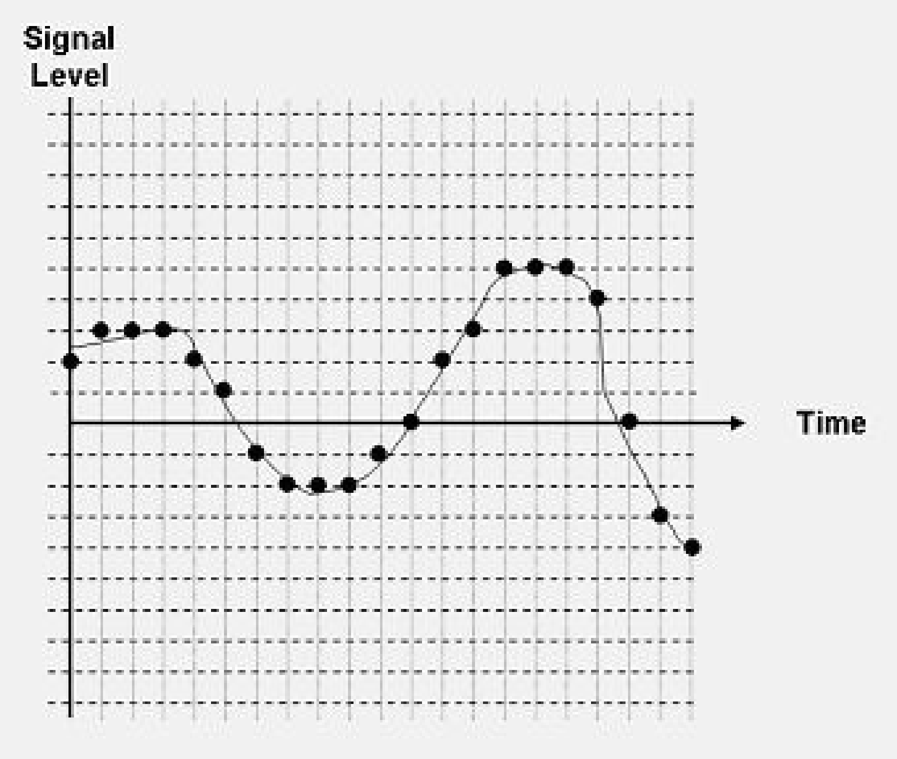
- Audio encoding involves converting an analog signal to a bit stream.
- Analog sound-voice and music-is represented by sine waves of different frequencies.
- The human ear can hear frequencies nominally in the range of 20-20,000 cycles/second (Hertz or Hz).
- Sound is analog, meaning that it is a continuous signal.
- Storing the sound digitally requires that the continuous sound wave be converted to a set of samples that can be represented by a sequence of zeros and ones.

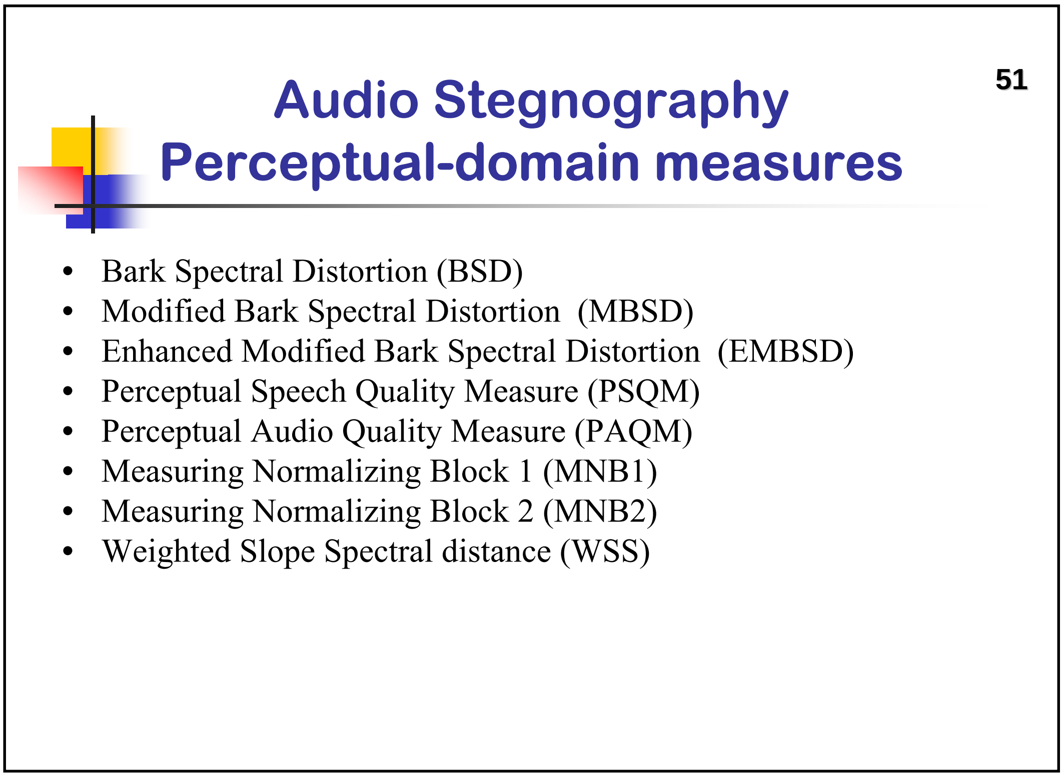
49

Audio Stegrnography

- Analog-to-digital conversion is accomplished by sampling the analog signal (with a microphone or other audio detector) and converting those samples to voltage levels.
- The voltage or signal level is then converted to a numeric value using a scheme called pulse code modulation.
- The device that performs this conversion is called a coder-decoder or codec.
  Pulse code modulation provides only an approximation of the original analog signal,

50

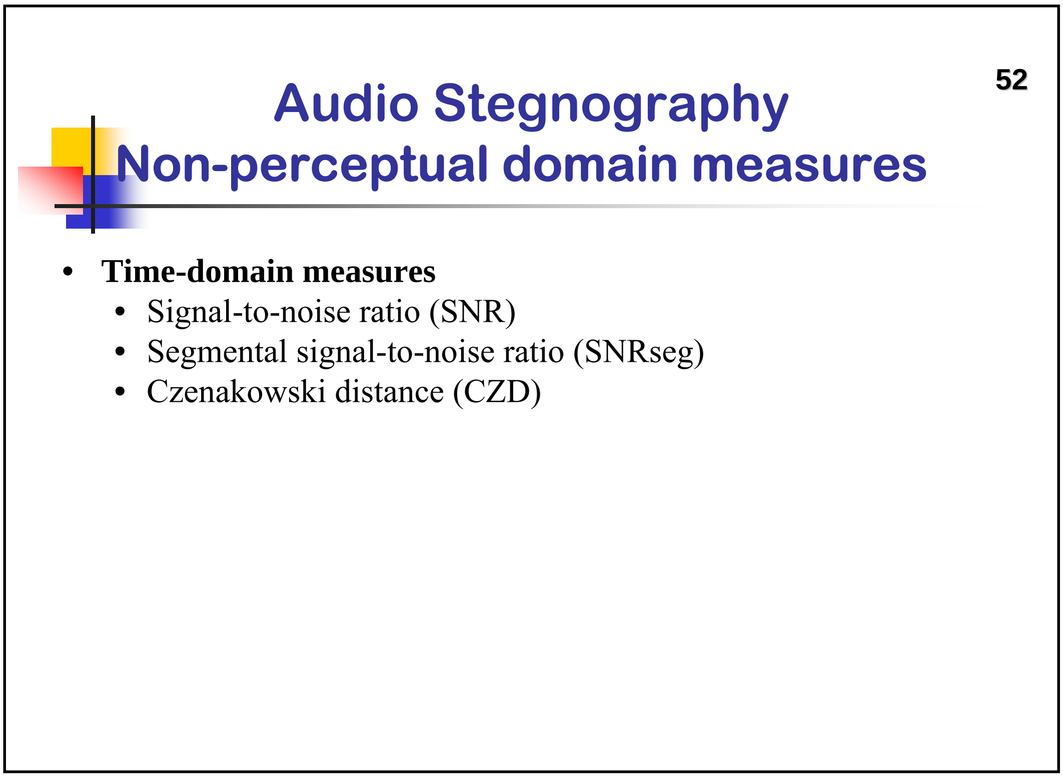




51

Audio Stegnography
Perceptual-domain measures

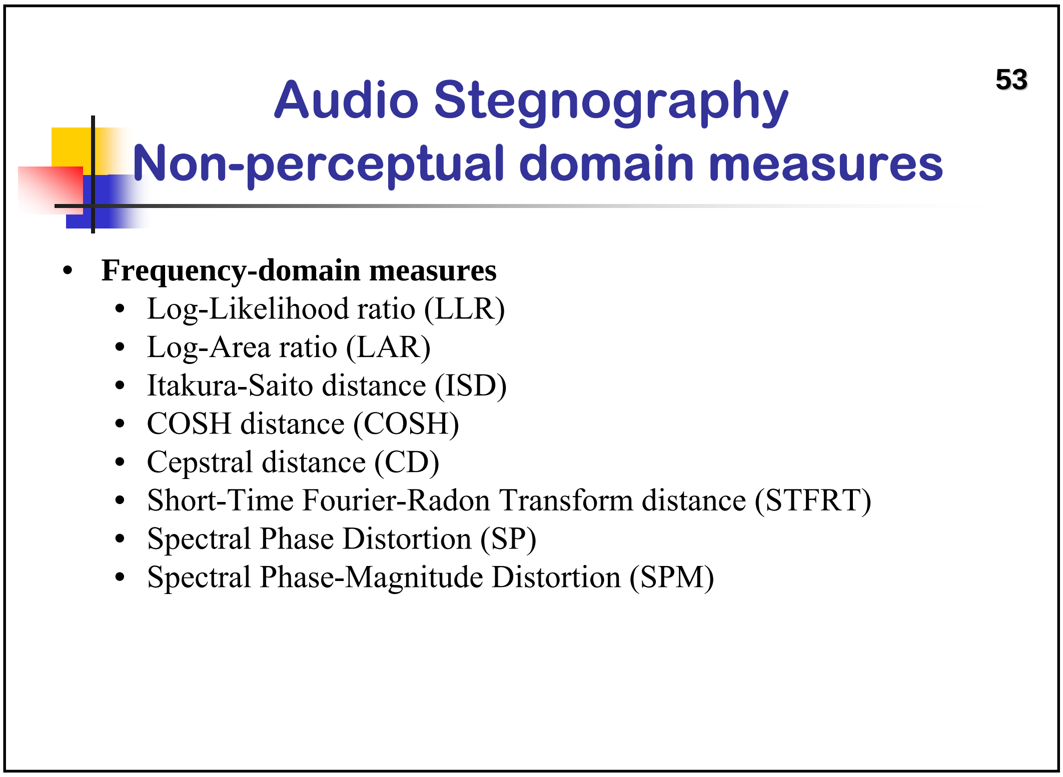
- Bark Spectral Distortion (BSD)
- Modified Bark Spectral Distortion (MBSD)
- Enhanced Modified Bark Spectral Distortion (EMBSD)
- Perceptual Speech Quality Measure (PSQM)
- Perceptual Audio Quality Measure (PAQM)
- Measuring Normalizing Block 1 (MNB1)
- Measuring Normalizing Block 2 (MNB2)
- Weighted Slope Spectral distance (WSS)



52

Audio Stegnography
Non-perceptual domain measures

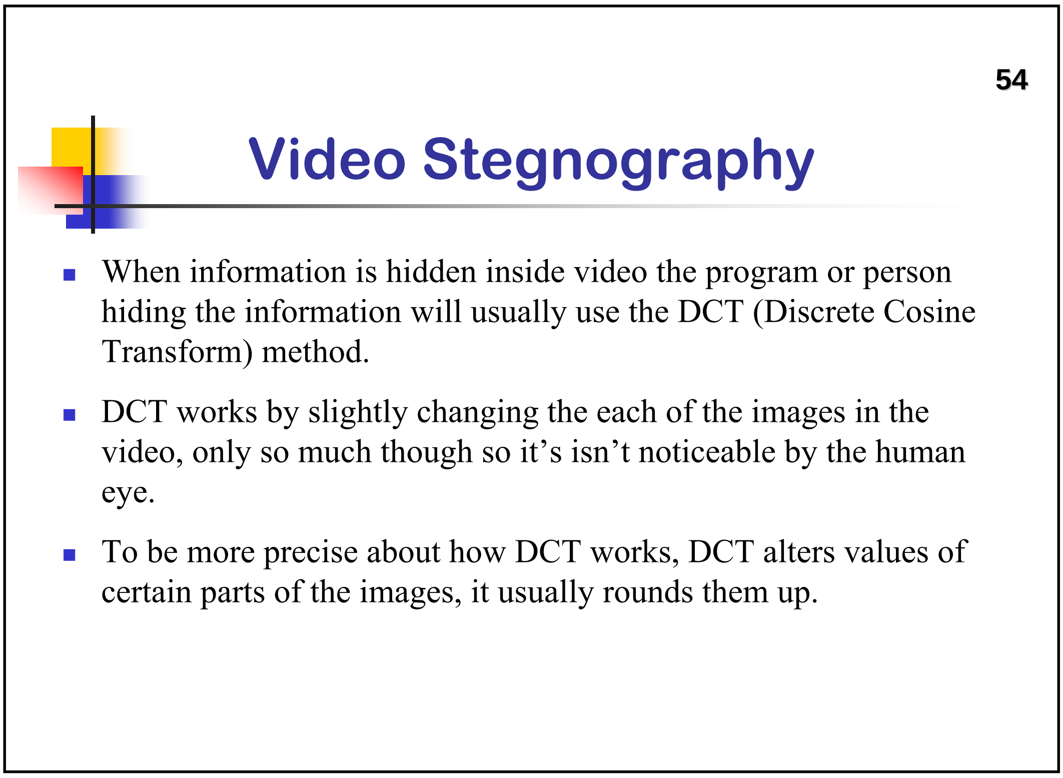
- **Time-domain measures**
  - Signal-to-noise ratio (SNR)
  - Segmental signal-to-noise ratio (SNRseg)
  - Czenakowski distance (CZD)



53

Audio Stegnography Non-perceptual domain measures

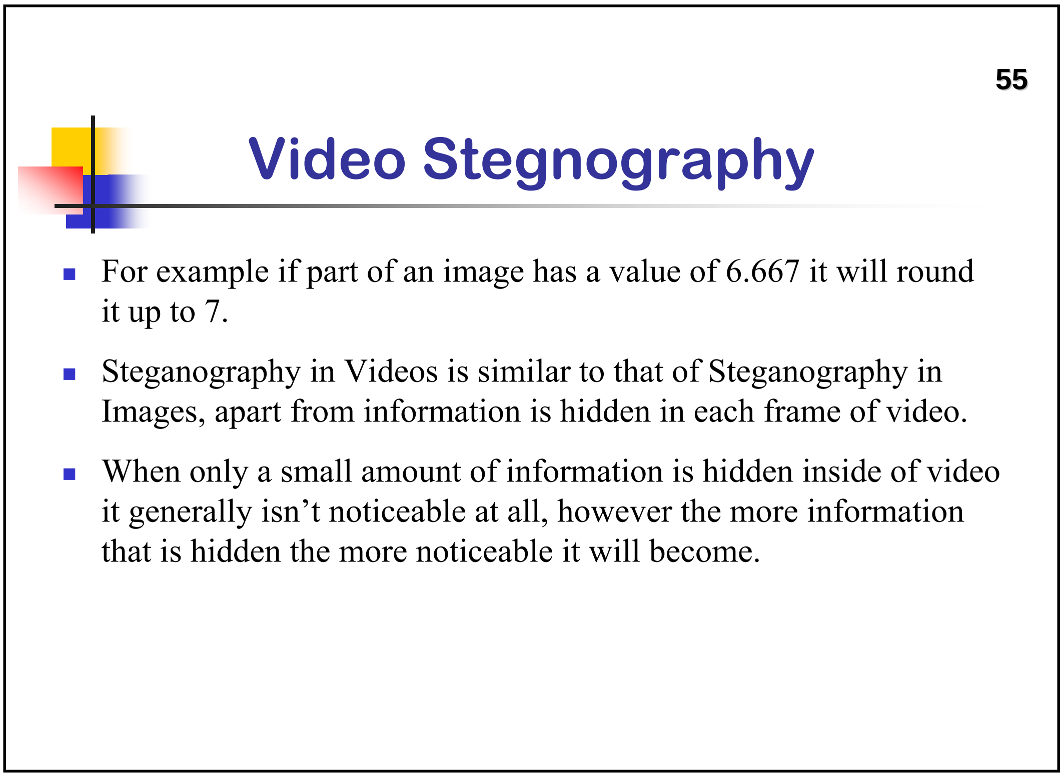
- **Frequency-domain measures**
  - Log-Likelihood ratio (LLR)
  - Log-Area ratio (LAR)
  - Itakura-Saito distance (ISD)
  - COSH distance (COSH)
  - Cepstral distance (CD)
  - Short-Time Fourier-Radon Transform distance (STFRT)
  - Spectral Phase Distortion (SP)
  - Spectral Phase-Magnitude Distortion (SPM)



54

Video Stegnography

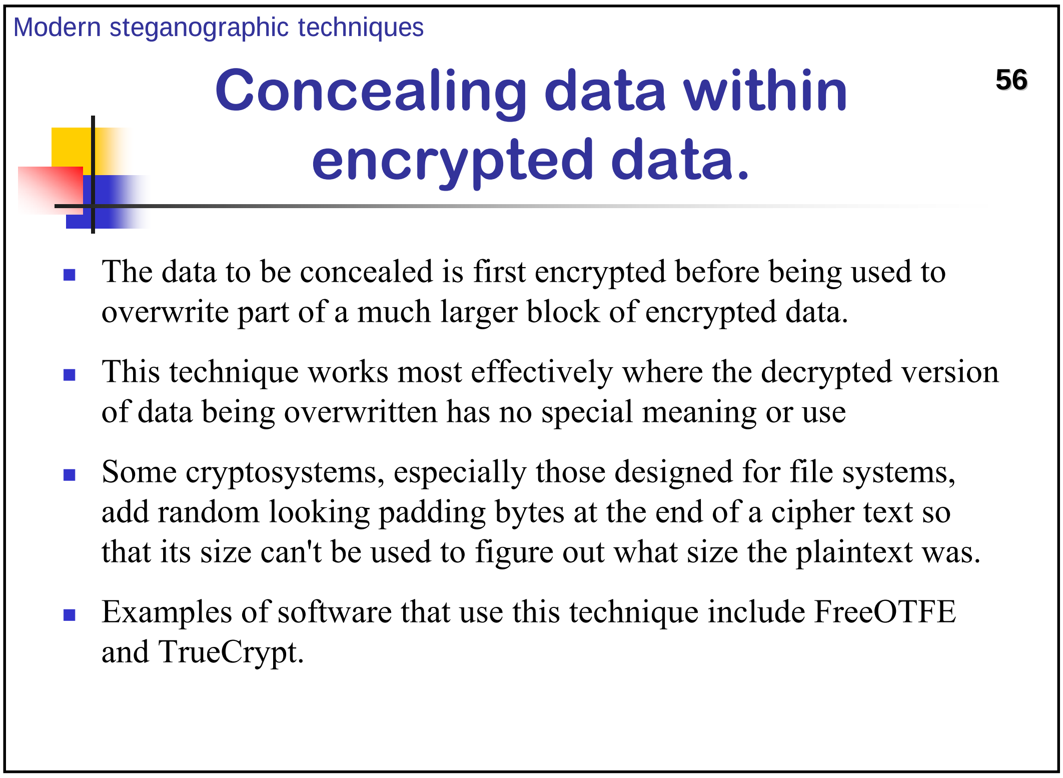
- When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method.
- DCT works by slightly changing the each of the images in the video, only so much though so it’s isn’t noticeable by the human eye.
- To be more precise about how DCT works, DCT alters values of certain parts of the images, it usually rounds them up.



55

Video Stegnography

- For example if part of an image has a value of 6.667 it will round it up to 7.
- Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video.
- When only a small amount of information is hidden inside of video it generally isn’t noticeable at all, however the more information that is hidden the more noticeable it will become.

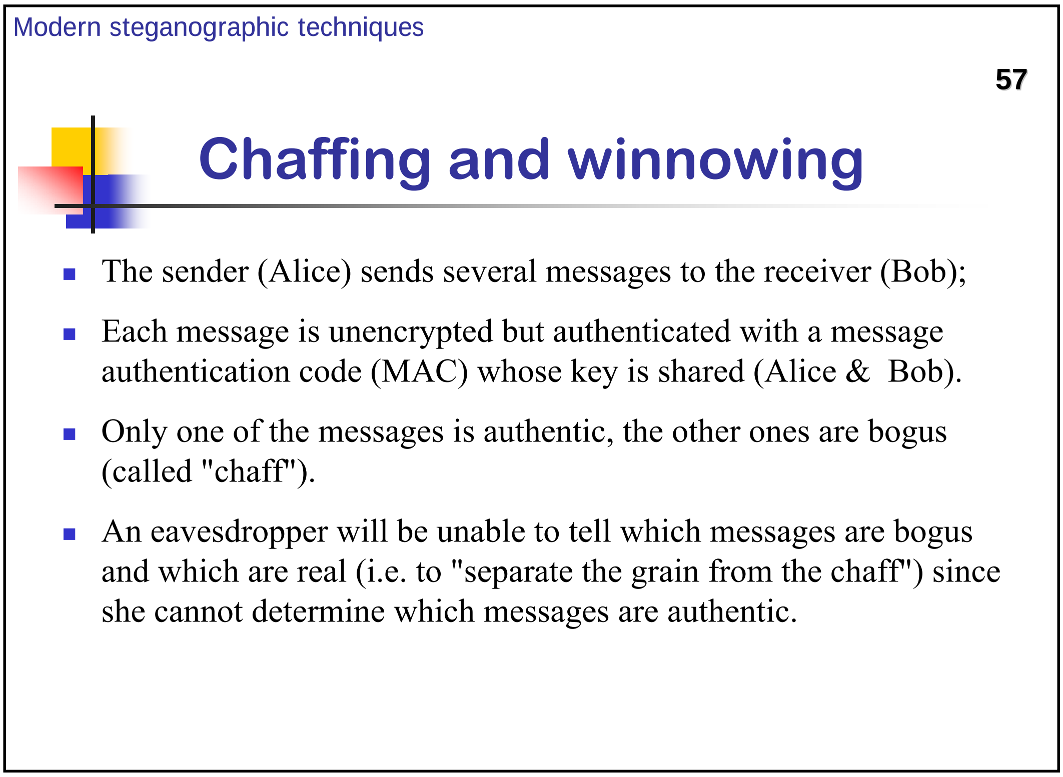


Modern steganographic techniques

56

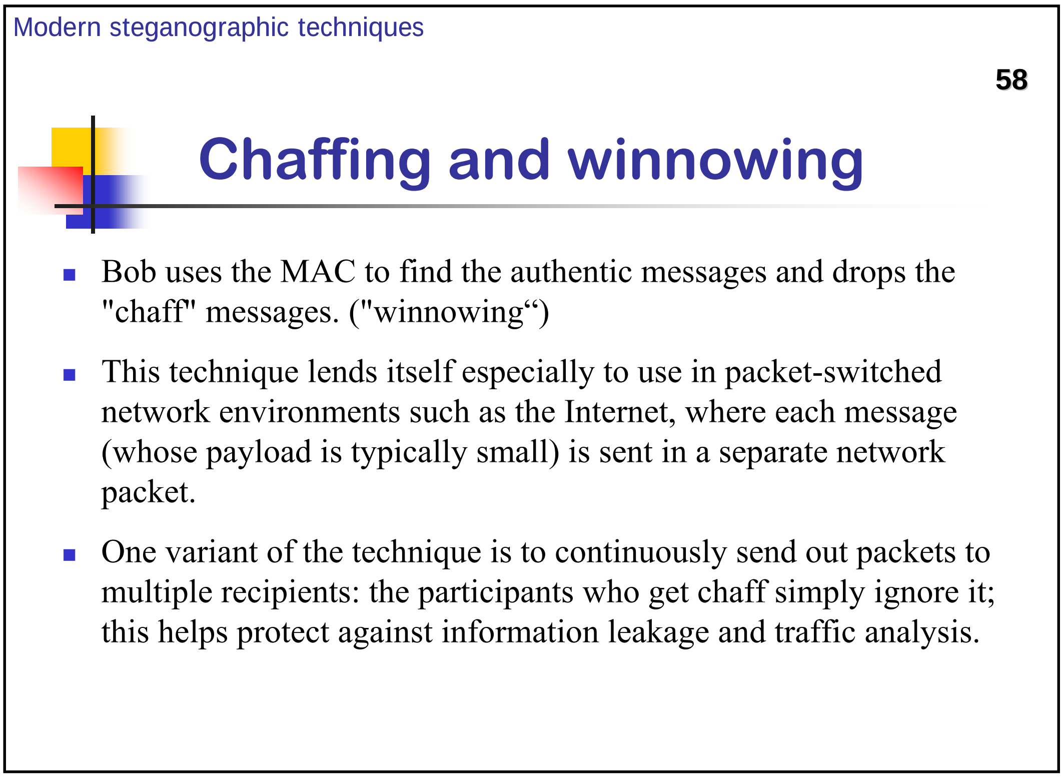
Concealing data within encrypted data.

- The data to be concealed is first encrypted before being used to overwrite part of a much larger block of encrypted data.
- This technique works most effectively where the decrypted version of data being overwritten has no special meaning or use
- Some cryptosystems, especially those designed for file systems, add random looking padding bytes at the end of a cipher text so that its size can't be used to figure out what size the plaintext was.
- Examples of software that use this technique include FreeOTFE and TrueCrypt.



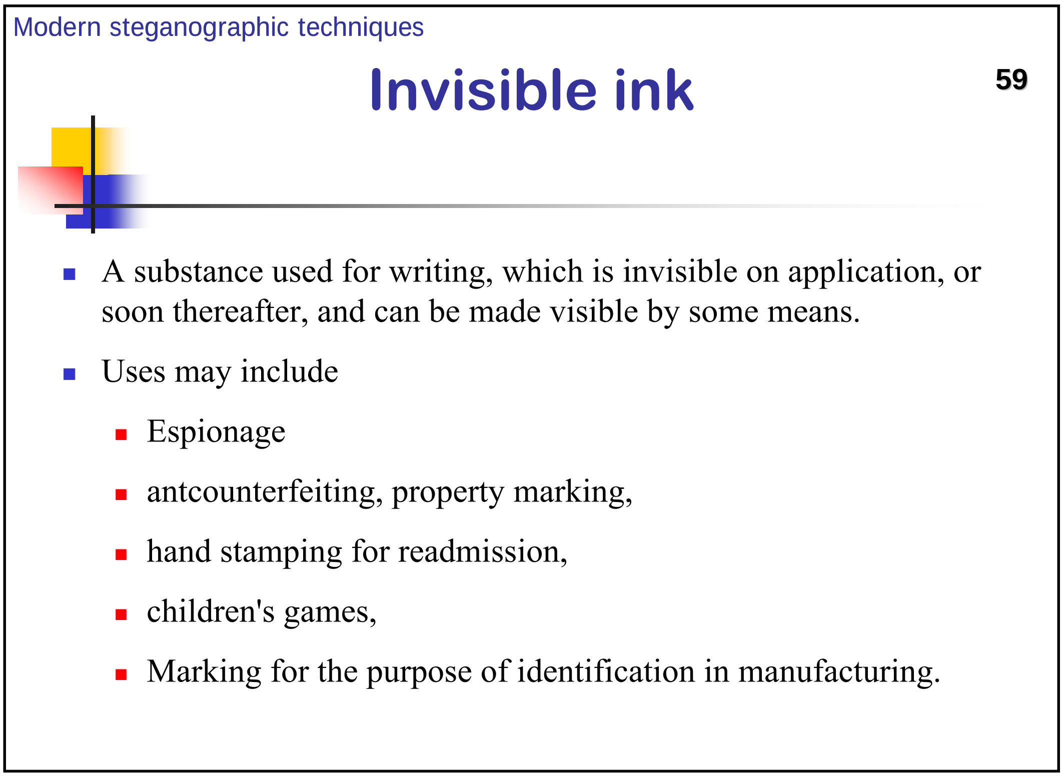
Chaffing and winnowing

- The sender (Alice) sends several messages to the receiver (Bob);
- Each message is unencrypted but authenticated with a message authentication code (MAC) whose key is shared (Alice & Bob).
- Only one of the messages is authentic, the other ones are bogus (called "chaff").
- An eavesdropper will be unable to tell which messages are bogus and which are real (i.e. to "separate the grain from the chaff") since she cannot determine which messages are authentic.



Chaffing and winnowing

- Bob uses the MAC to find the authentic messages and drops the "chaff" messages. ("winnowing“)
- This technique lends itself especially to use in packet-switched network environments such as the Internet, where each message (whose payload is typically small) is sent in a separate network packet.
- One variant of the technique is to continuously send out packets to multiple recipients: the participants who get chaff simply ignore it; this helps protect against information leakage and traffic analysis.

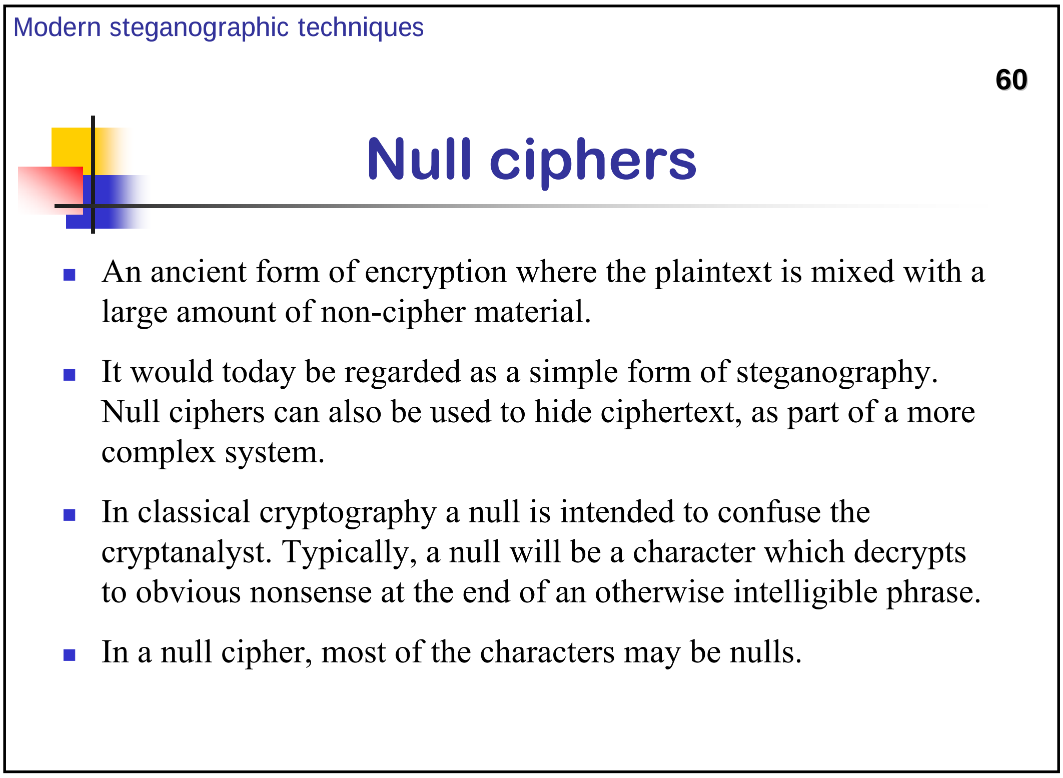


Modern steganographic techniques

59

Invisible ink

- A substance used for writing, which is invisible on application, or soon thereafter, and can be made visible by some means.
- Uses may include
  - Espionage
  - antcounterfeiting, property marking,
  - hand stamping for readmission,
  - children's games,
  - Marking for the purpose of identification in manufacturing.

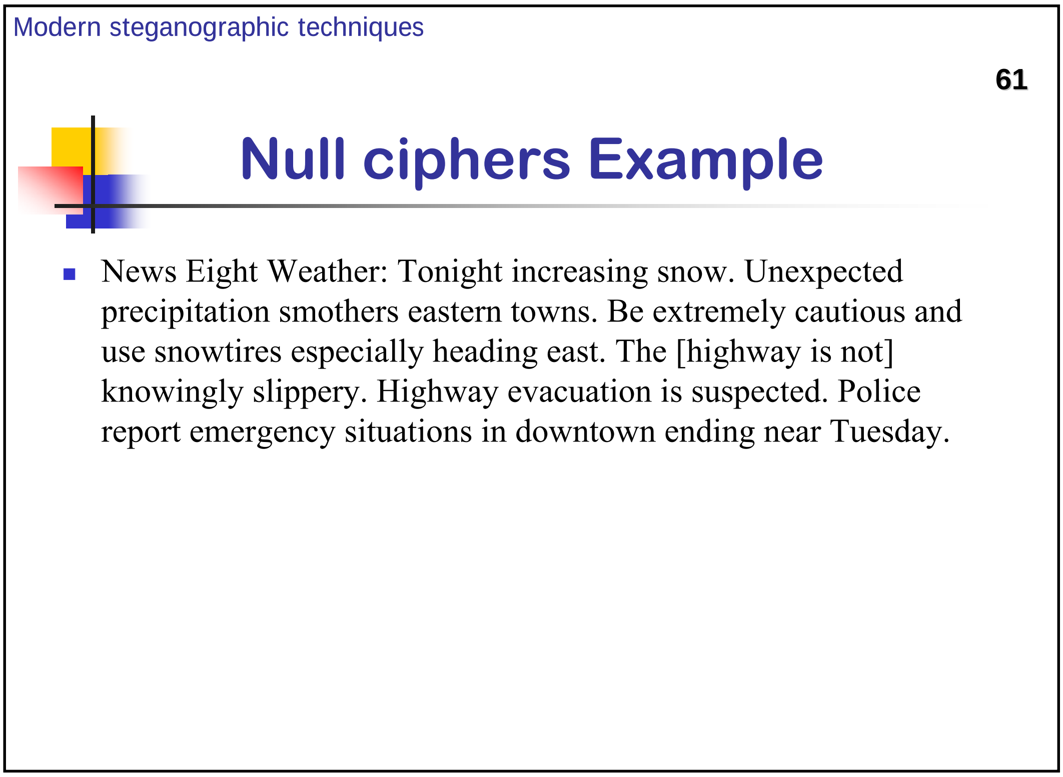


Modern steganographic techniques

60

Null ciphers

- An ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material.
- It would today be regarded as a simple form of steganography. Null ciphers can also be used to hide ciphertext, as part of a more complex system.
- In classical cryptography a null is intended to confuse the cryptanalyst. Typically, a null will be a character which decrypts to obvious nonsense at the end of an otherwise intelligible phrase.
- In a null cipher, most of the characters may be nulls.

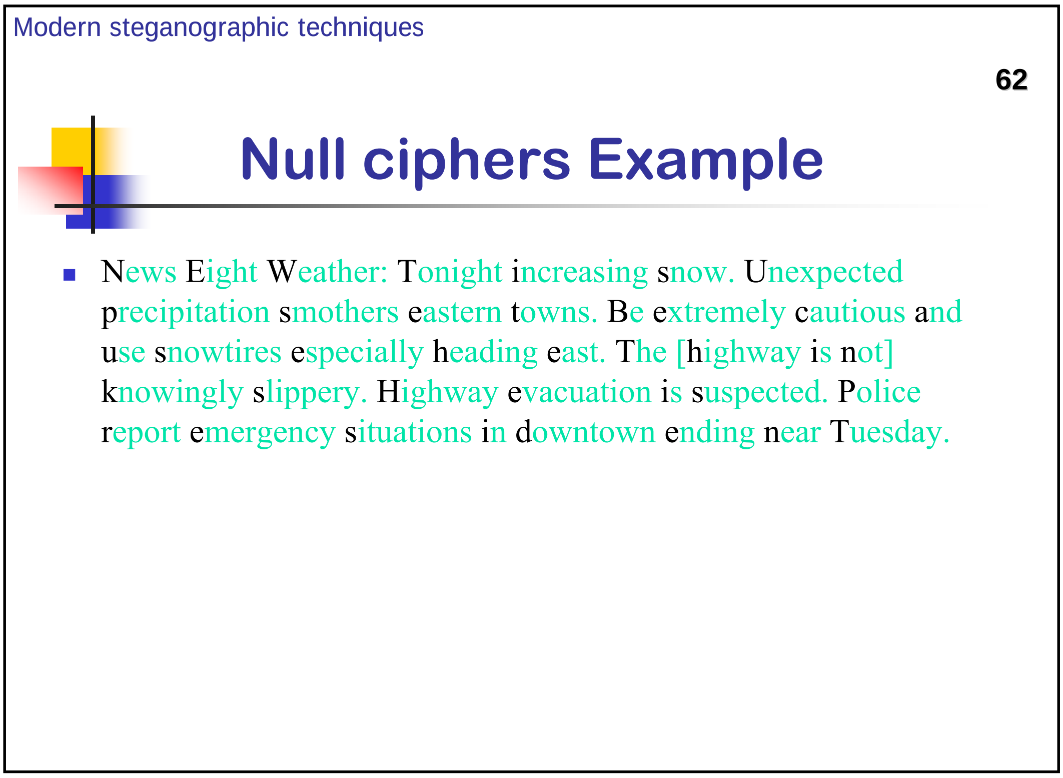


Modern steganographic techniques

61

Null ciphers Example

- News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.



Modern steganographic techniques

62

Null ciphers Example

- News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Modern steganographic techniques

63

Null ciphers Example

- News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Newt is upset because he thinks he is President

Modern steganographic techniques

64

Null ciphers

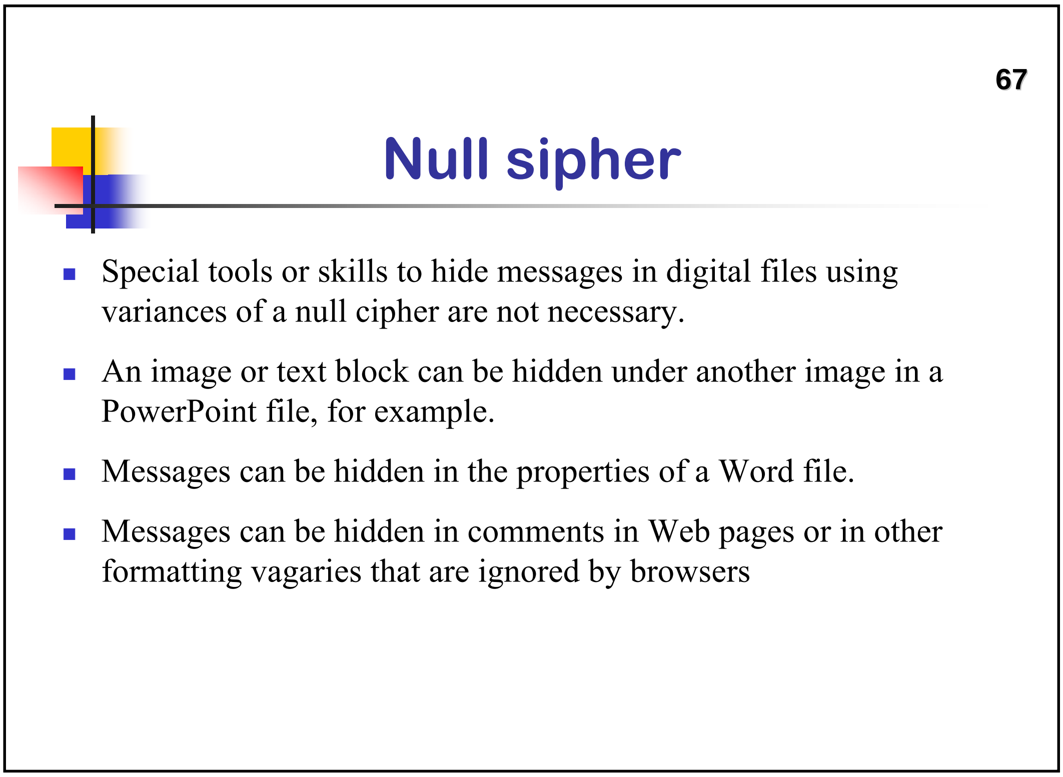
- Make it harder, select the first letter from the first word, second letter from the second word, third from the third, and so on, to hide the information in.
- The term null cipher is used to mean choosing not to use encryption at all in a system where various encryption options are offered, an option some software offers for testing/debugging.

Spam

Dear Friend , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1621 ; Title 5 ; Section 303 ! Do NOT confuse us with Internet scam artists . Why work for somebody else when you can become rich within 38 days ! Have you ever noticed the baby boomers are more demanding than their parents & more people than ever are surfing the web ! Well, now is your chance to capitalize on this ! WE will help YOU sell more & SELL MORE . You can begin at absolutely no cost to you ! But don't believe us ! Ms Anderson who resides in Missouri tried us and says "My only problem now is where to park all my cars" . This offer is 100% legal . You will blame yourself forever if you don't order now ! Sign up a friend and your friend will be rich too . Cheers ! Dear Salaryman , Especially for you - this amazing news . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 2116 , Title 3 ; Section 306 ! This is a ligitimate business proposal ! Why work for somebody else when you can become rich within 68 months ! Have you ever noticed more people than ever are surfing the web and nobody is getting any younger ! Well, now is your chance to capitalize on this . We will help you decrease perceived waiting time by 180% and SELL MORE . The best thing about our system is that it is absolutely risk free for you ! But don't believe us ! Mrs Ames of Alabama tried us and says "My only problem now is where to park all my cars" . We are licensed to operate in all states ! You will blame yourself forever if you don't order now ! Sign up a friend and you'll get a discount of 20% ! Thanks ! Dear Salaryman , Your email address has been submitted to us indicating your interest in our briefing ! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our mailing list . This mail is being sent in compliance with Senate bill 1618 , Title 6 , Section 307 . THIS IS NOT A GET RICH SCHEME . Why work for somebody else when you can become rich within 17 DAYS ! Have you ever noticed more people than ever are surfing the web and more people than ever are surfing the web ! Well, now is your chance to capitalize on this ! WE will help YOU turn your business into an E-BUSINESS and deliver goods right to the customer's doorstep ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Ms Simpson of Wyoming tried us and says "Now I'm rich, Rich, RICH" ! We assure you that we operate within all applicable laws . We implore you - act now ! Sign up a friend and you'll get a discount of 50% . Thank-you for your serious consideration of our offer .

Spam

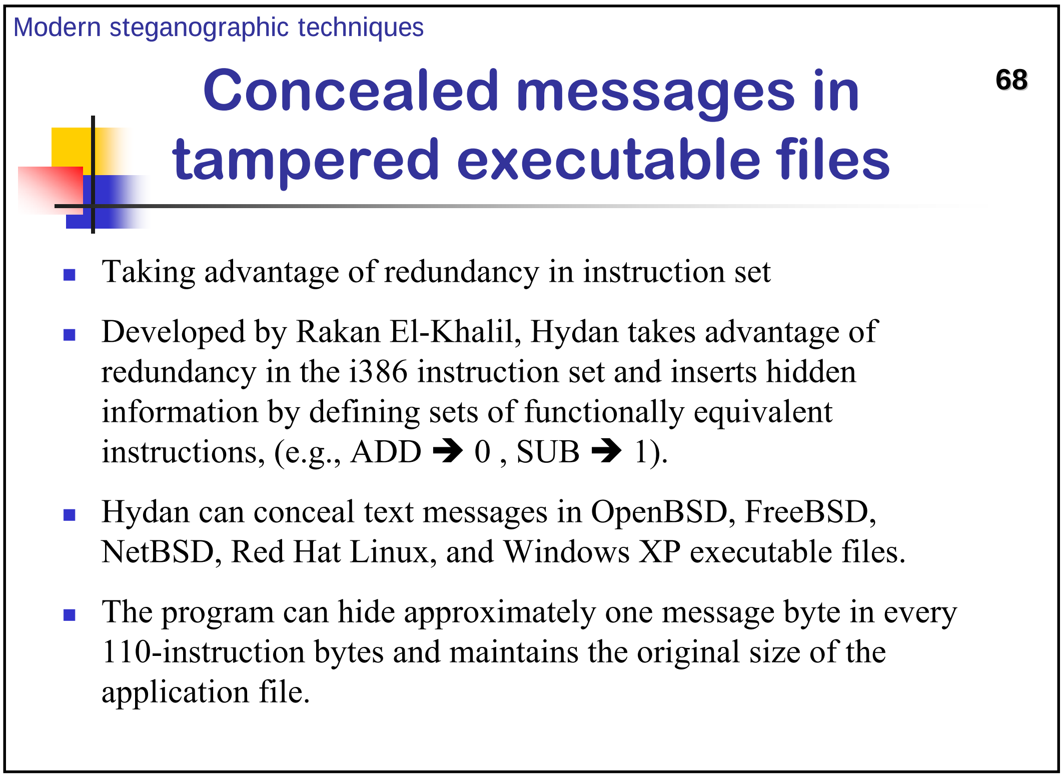
- This message looks like typical spam, which is generally ignored and discarded.
- This message was created at spam mimic, a Website that converts a short text message into a text block that looks like spam using a grammar-based mimicry idea first proposed by Peter Wayner
- The reader will learn nothing by looking at the word spacing or misspellings in the message; the zeros and ones are encoded by the choice of the words.
- The hidden message in the spam carrier above is:
  - Meet at Main and Willard at 8:30



67

Null sipher

- Special tools or skills to hide messages in digital files using variances of a null cipher are not necessary.
- An image or text block can be hidden under another image in a PowerPoint file, for example.
- Messages can be hidden in the properties of a Word file.
- Messages can be hidden in comments in Web pages or in other formatting vagaries that are ignored by browsers



Modern steganographic techniques

68

Concealed messages in tampered executable files

- Taking advantage of redundancy in instruction set
- Developed by Rakan El-Khalil, Hydan takes advantage of redundancy in the i386 instruction set and inserts hidden information by defining sets of functionally equivalent instructions, (e.g., ADD ➔ 0 , SUB ➔ 1).
- Hydan can conceal text messages in OpenBSD, FreeBSD, NetBSD, Red Hat Linux, and Windows XP executable files.
- The program can hide approximately one message byte in every 110-instruction bytes and maintains the original size of the application file.

Modern steganographic techniques

69

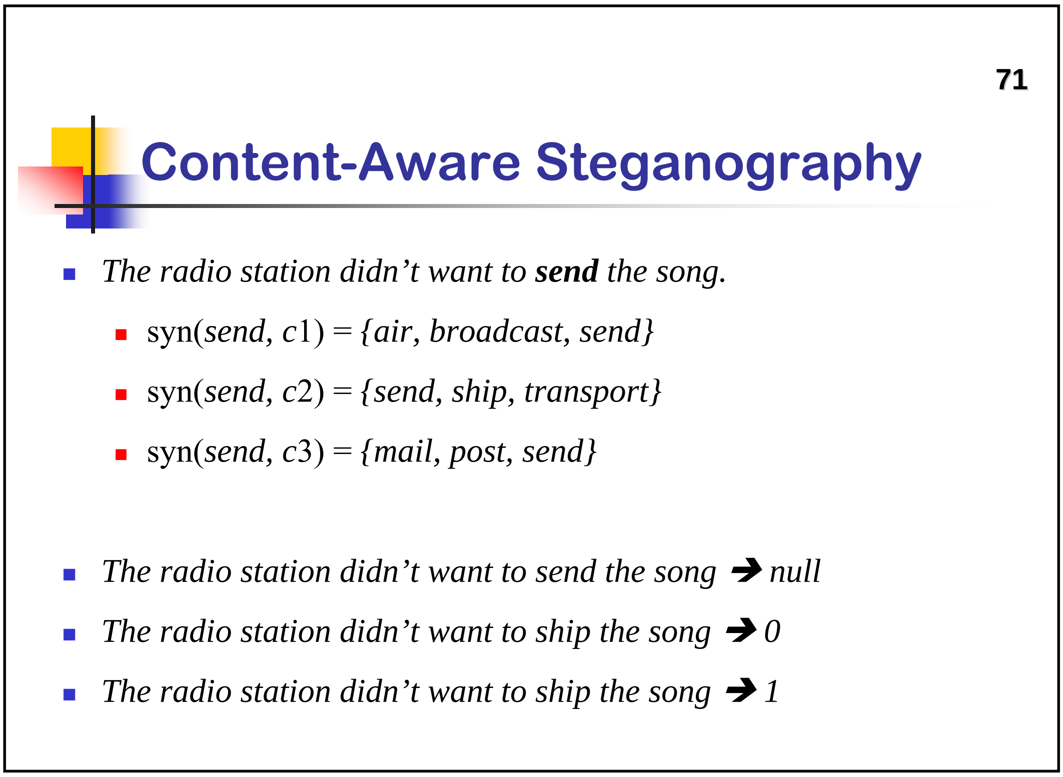
Injecting imperceptible delays

- Technique involves injecting imperceptible delays to packets sent over the network from the keyboard.
- Delays in keypresses in some applications (telnet or remote desktop) can mean a delay in packets
- There is no extra processor or network activity, so the steganographic technique is "invisible" to the user.
- This kind of steganography could be included in the firmware of keyboards, thus making it invisible to the system.

70

Content-Aware Steganography (CAS)

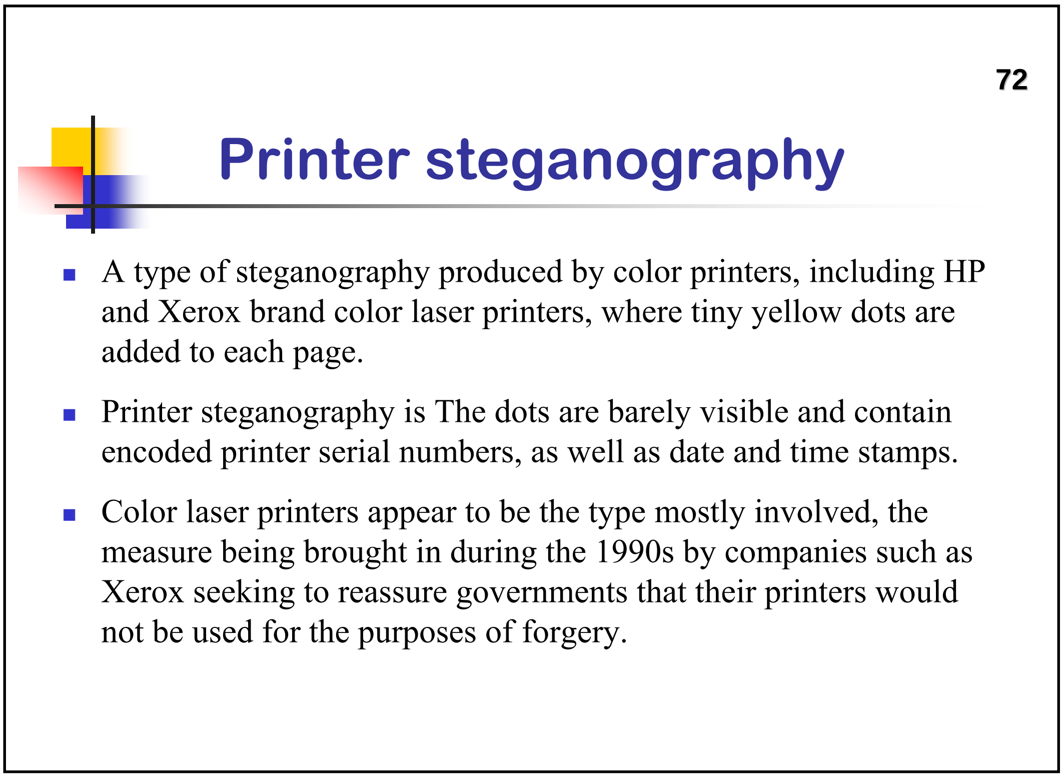
- As opposed to classic steganographic algorithms that only embed information in the syntactic representation of a datagram, CAS embeds secrets in the semantic interpretation which a human assigns to a datagram.
- CAS chooses stego objects in such a way that both the human sender and receiver can easily assign a secret semantic interpretation to the transmitted datagrams, whereas for a computer it is inherently difficult
- CASs are constructed in such a way that it require solving an Artificial Intelligence problem that up to now cannot be tackled with state-of-the-art algorithms.



Content-Aware Steganography

- *The radio station didn't want to **send** the song.*
  - syn(*send, c*1) = {*air, broadcast, send*}
  - syn(*send, c*2) = {*send, ship, transport*}
  - syn(*send, c*3) = {*mail, post, send*}

- *The radio station didn't want to send the song* ➔ *null*
- *The radio station didn't want to ship the song* ➔ *0*
- *The radio station didn't want to ship the song* ➔ *1*



Printer steganography

- A type of steganography produced by color printers, including HP and Xerox brand color laser printers, where tiny yellow dots are added to each page.
- Printer steganography is The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.
- Color laser printers appear to be the type mostly involved, the measure being brought in during the 1990s by companies such as Xerox seeking to reassure governments that their printers would not be used for the purposes of forgery.

73

Printer steganography

- The identification is by means of a watermark, often using yellow-on-white, embedded in the printout of each page, and in conjunction with other information can be used to identify the printer which was used to print any document originally produced on a wide range of popular printers.
- It may be text, or a repeated pattern of dots throughout the page, more easily visible under blue light or with a magnifying glass, and is intended to be very difficult to notice with the naked eye.
- In 2005, the Electronic Frontier Foundation cracked the codes and published an online guide to their detection.

74

Steganographic file system

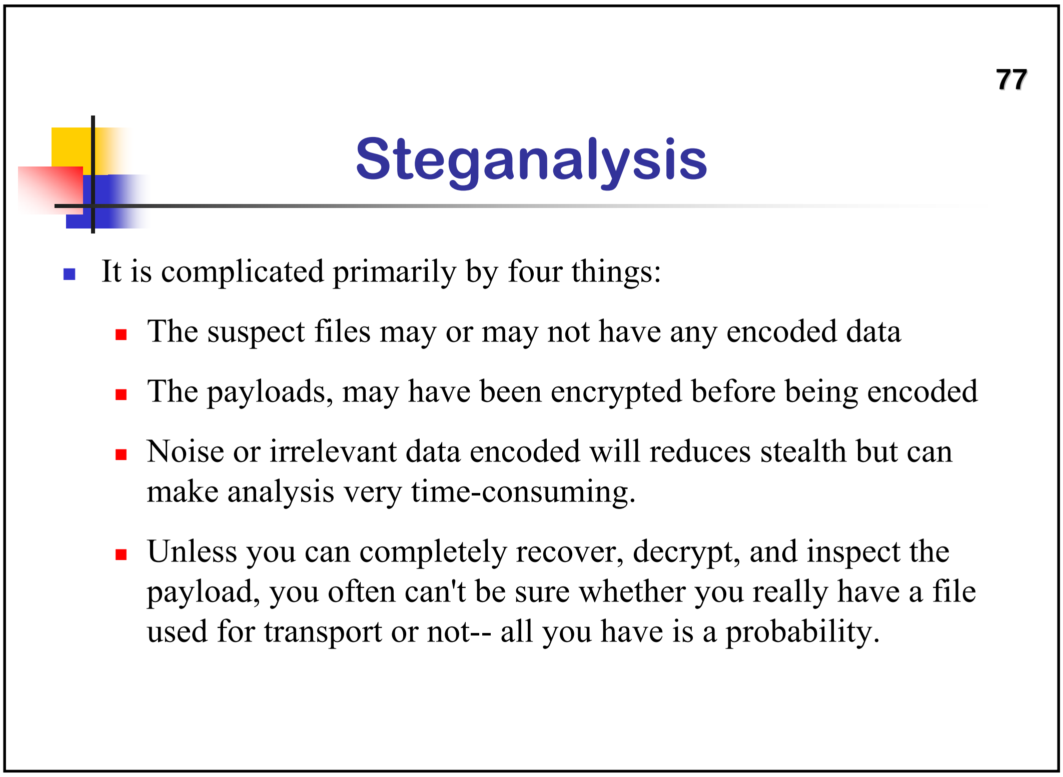
- Files are not merely stored, nor stored encrypted, but in which the entire partition is randomized
- Files strongly resemble randomized sections of the partition
- When files are stored, there is no easy way to discern between meaningless gibberish and the actual files.
- Locations of files are derived from the key for the files, and are hidden and available to only programs with the passphrase.
- Very quickly files can overwrite each other (Birthday Paradox);
- By writing files in multiple places the chance of loss is reduced.

Steganographic File System

- Generally, a steganographic file system is implemented over a steganographic layer, which supplies just the storage mechanism.
- For example, the steganographic file system layer can be some existing MP3 files, each file contains a chunk of data (or a part of the file system).
- The final product is a file system that is hardly detected (depending on the steganographic layer) that can store any kind of file in a regular file system hierarchy.

Steganalysis

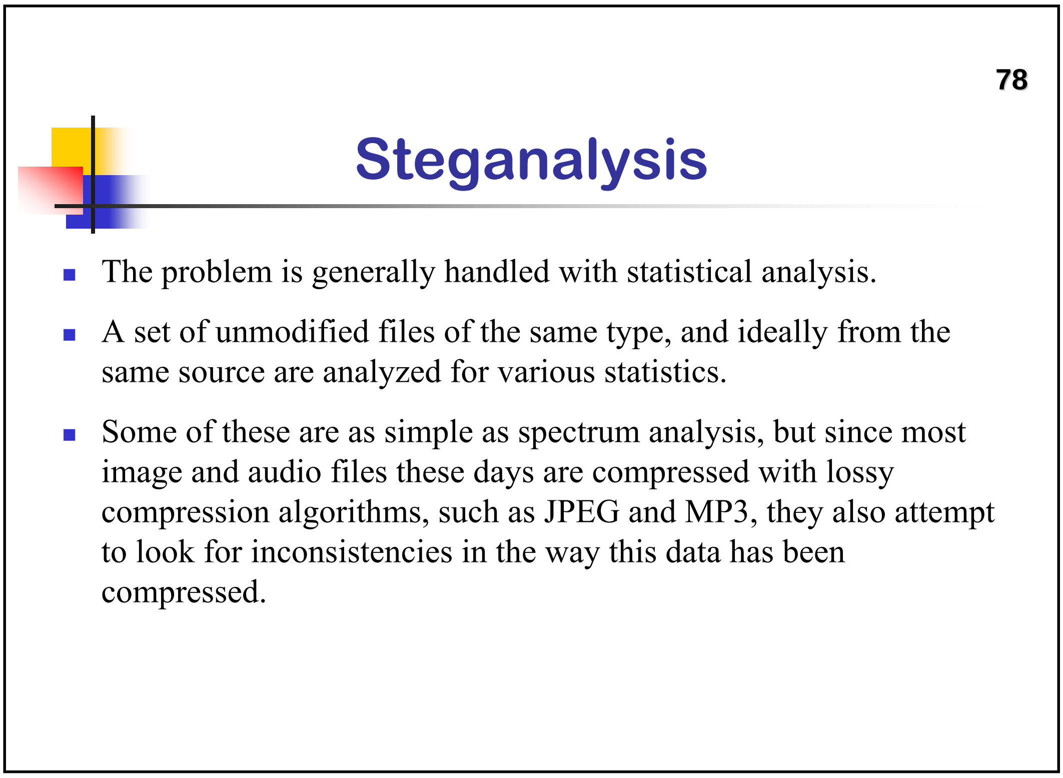
- The art and science of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography.
- The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload.
- Unlike cryptanalysis, where it is obvious that intercepted data contains a message, steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a payload.



77

Steganalysis

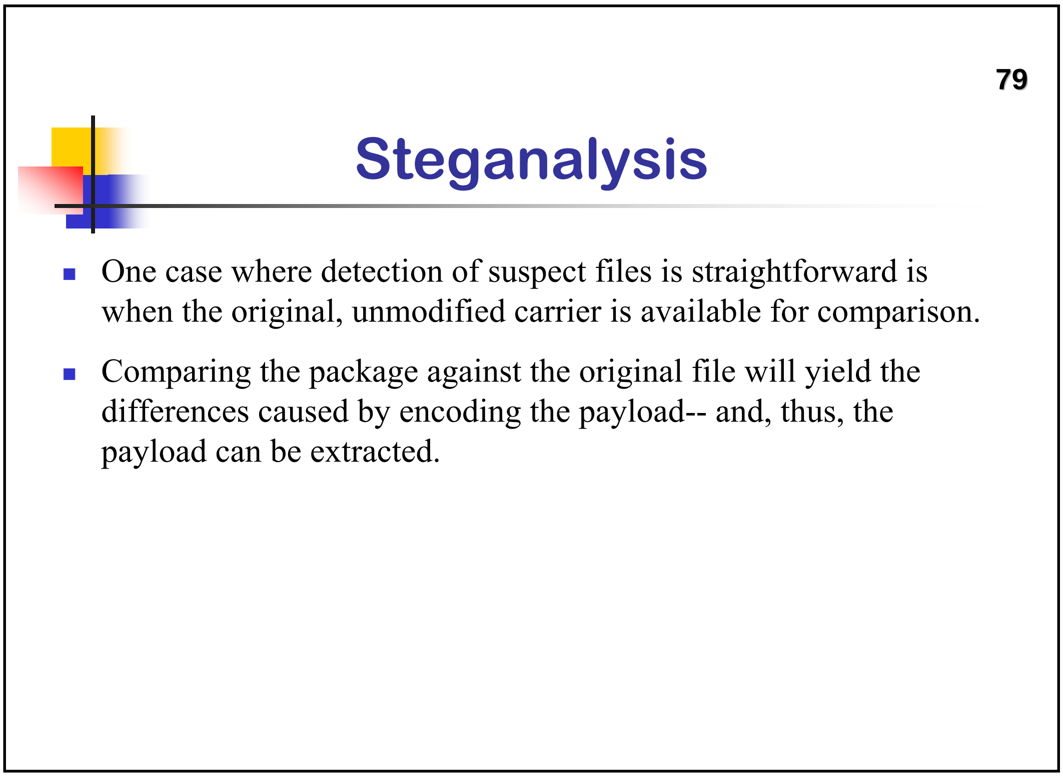
- It is complicated primarily by four things:
  - The suspect files may or may not have any encoded data
  - The payloads, may have been encrypted before being encoded
  - Noise or irrelevant data encoded will reduces stealth but can make analysis very time-consuming.
  - Unless you can completely recover, decrypt, and inspect the payload, you often can't be sure whether you really have a file used for transport or not-- all you have is a probability.



78

Steganalysis

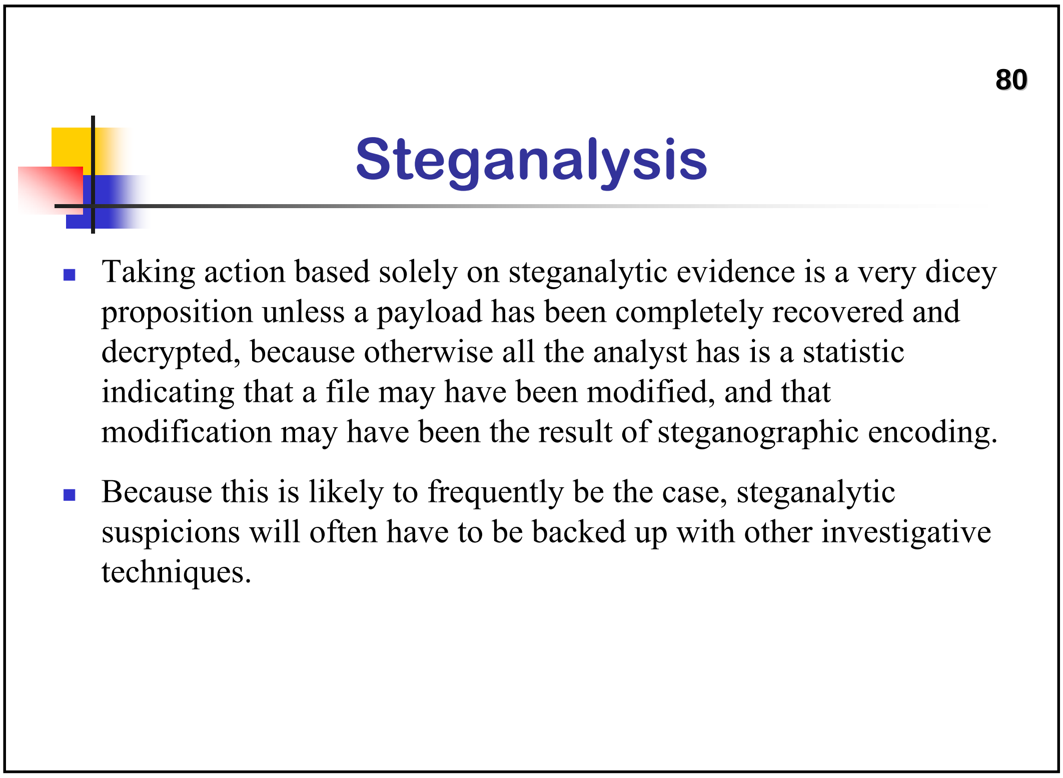
- The problem is generally handled with statistical analysis.
- A set of unmodified files of the same type, and ideally from the same source are analyzed for various statistics.
- Some of these are as simple as spectrum analysis, but since most image and audio files these days are compressed with lossy compression algorithms, such as JPEG and MP3, they also attempt to look for inconsistencies in the way this data has been compressed.



79

Steganalysis

- One case where detection of suspect files is straightforward is when the original, unmodified carrier is available for comparison.
- Comparing the package against the original file will yield the differences caused by encoding the payload-- and, thus, the payload can be extracted.



80

Steganalysis

- Taking action based solely on steganalytic evidence is a very dicey proposition unless a payload has been completely recovered and decrypted, because otherwise all the analyst has is a statistic indicating that a file may have been modified, and that modification may have been the result of steganographic encoding.
- Because this is likely to frequently be the case, steganalytic suspicions will often have to be backed up with other investigative techniques.

81

Noise Floor Consistency Analysis

- In some cases, such as when only a single image is available, more complicated analysis techniques may be required.
- In general, steganography attempts to make distortion to the carrier indistinguishable from the carrier's noise floor.
- In practice, however, this is often improperly simplified to deciding to make the modifications to the carrier resemble white noise as closely as possible, rather than analyzing, modeling, and then consistently emulating the actual noise characteristics of the carrier.

82

Noise Floor Consistency Analysis

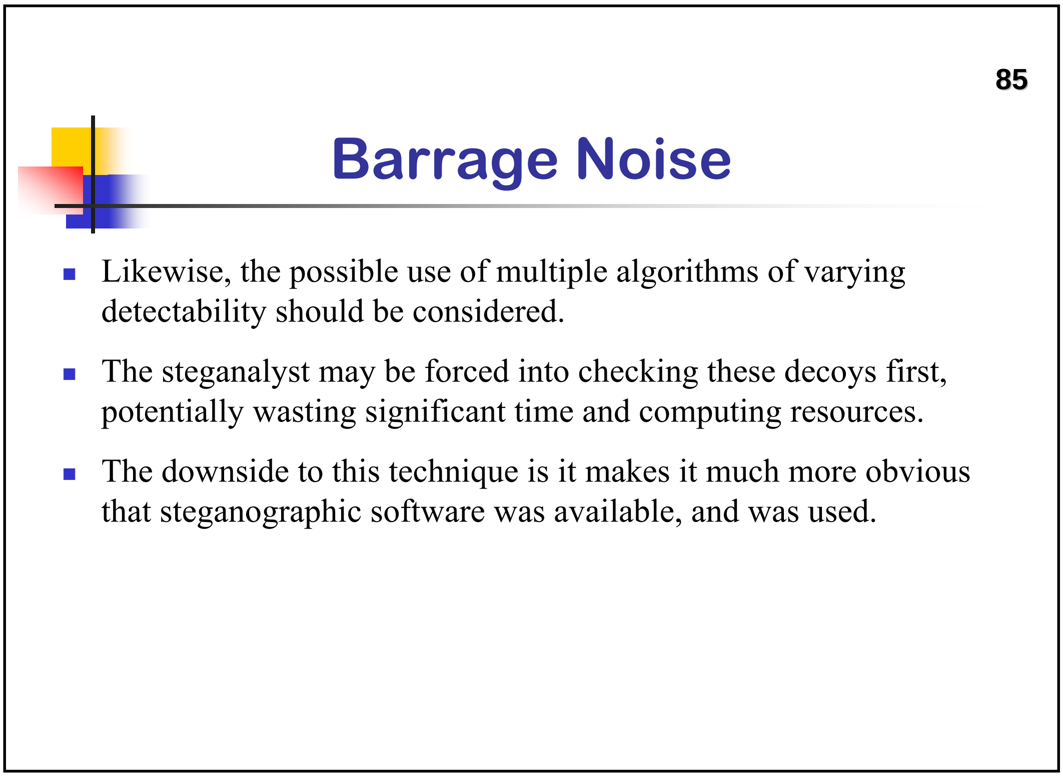
- In particular, many simple steganographic systems simply modify the least-significant bit of a sample; this causes the modified samples to have not only different noise profiles than unmodified samples, but also for their LSBs to have different noise profiles than could be expected from analysis of their higher-order bits, which will still show some amount of noise.
- Such LSB-only modification can be detected with appropriate algorithms, in some cases detecting encoding densities as low as 1% with reasonable reliability

Detecting Encrypted Payloads

- Detecting a probable steganographic payload is often only part of the problem, as the payload may have been encrypted first.
- Encrypting the payload is not always done solely to make recovery of the payload more difficult.
- Many encryption techniques have the desirable property of making the payload appear much more like well-distributed noise, which can make detection efforts more difficult, and save the steganographic encoding technique the trouble of having to distribute the signal energy evenly

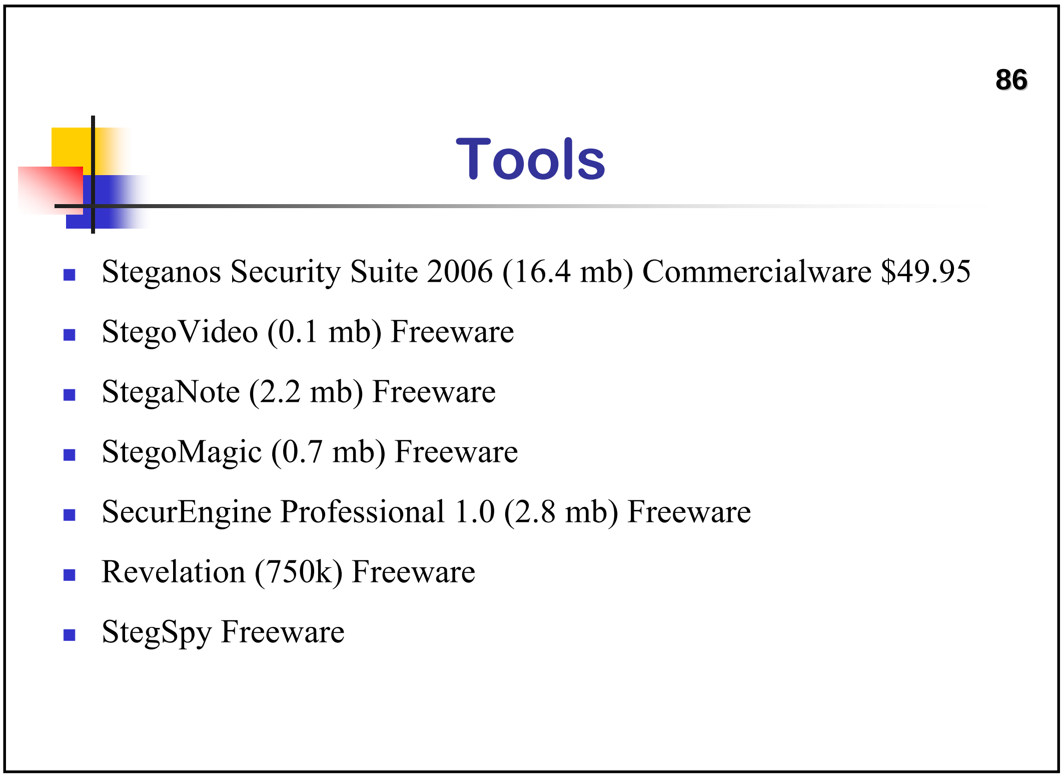
Barrage Noise

- If inspection of a storage device is considered very likely, the steganographer may attempt to barrage a potential analyst with, effectively, misinformation.
- This may be a large set of files encoded with anything from random data, to white noise, to meaningless drivel, to deliberately misleading information.
- The encoding density on these files may be slightly higher than the "real" ones;



Barrage Noise

- Likewise, the possible use of multiple algorithms of varying detectability should be considered.
- The steganalyst may be forced into checking these decoys first, potentially wasting significant time and computing resources.
- The downside to this technique is it makes it much more obvious that steganographic software was available, and was used.



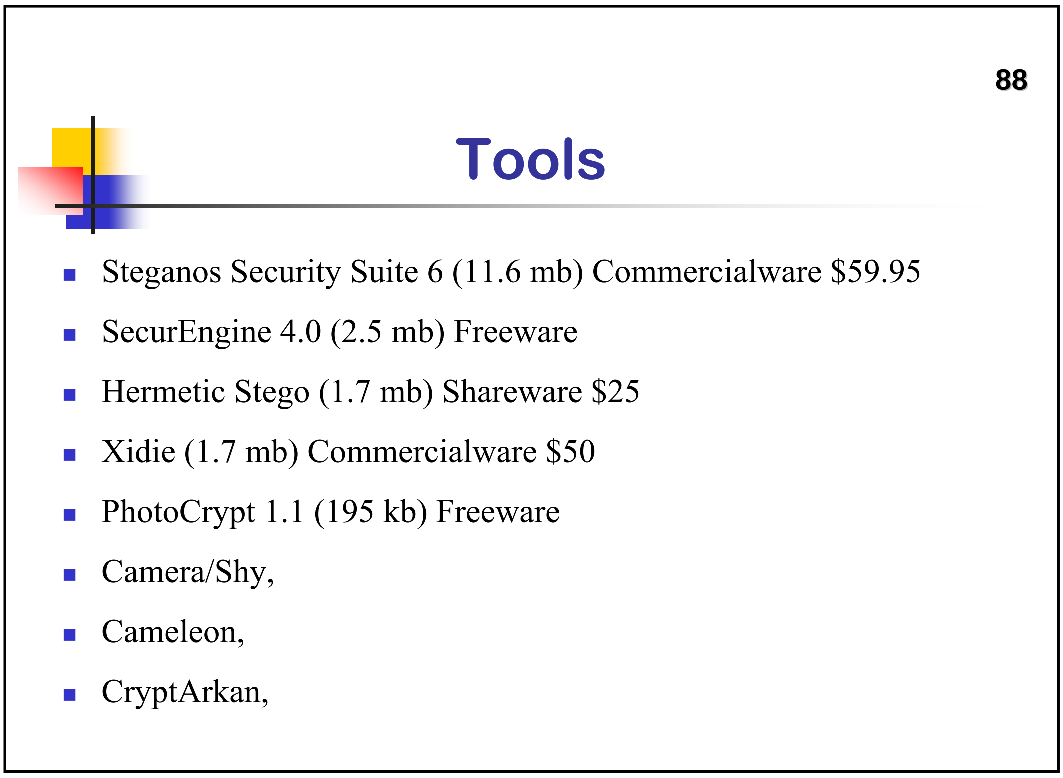
Tools

- Steganos Security Suite 2006 (16.4 mb) Commercialware $49.95
- StegoVideo (0.1 mb) Freeware
- StegaNote (2.2 mb) Freeware
- StegoMagic (0.7 mb) Freeware
- SecurEngine Professional 1.0 (2.8 mb) Freeware
- Revelation (750k) Freeware
- StegSpy Freeware

87

Tools

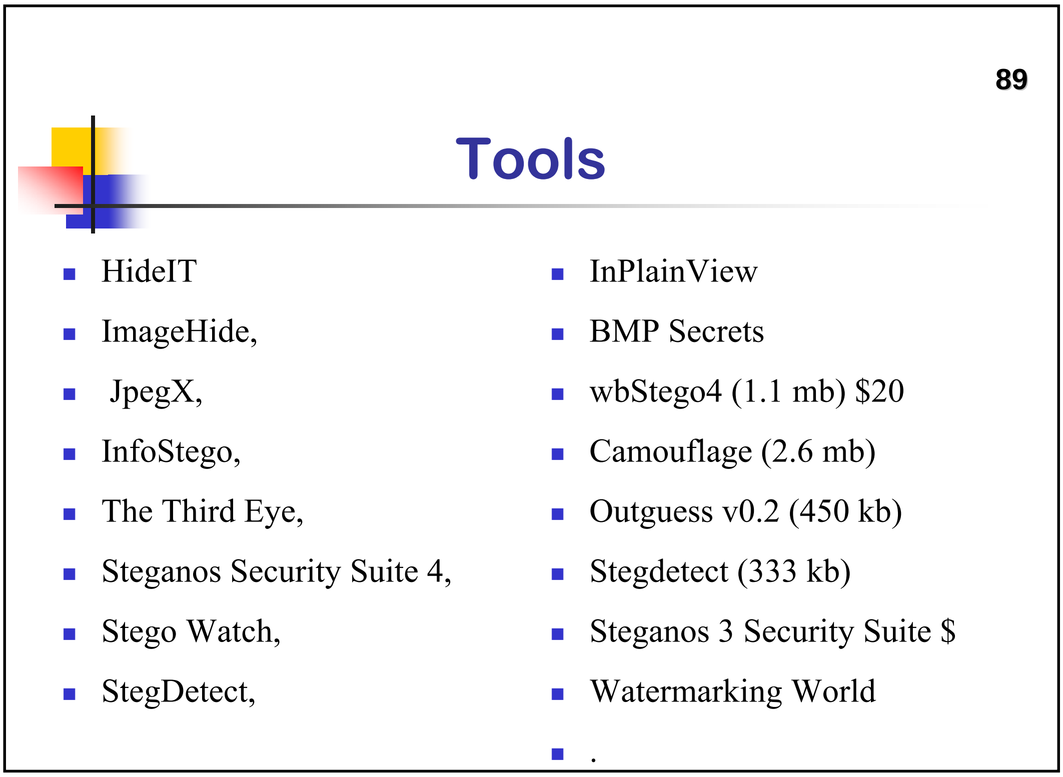
- Puff (452 kb) Freeware
- bmpSteg (18 kb) Freeware
- Stego Machine (Java),
- Stegtunnel (Unix),
- Steganos Security Suite 7.0 (Win),
- wbStego4open (Win/Unix),
- Steganography 2.8 (Win),
- CryptoBola (Win).



88

Tools

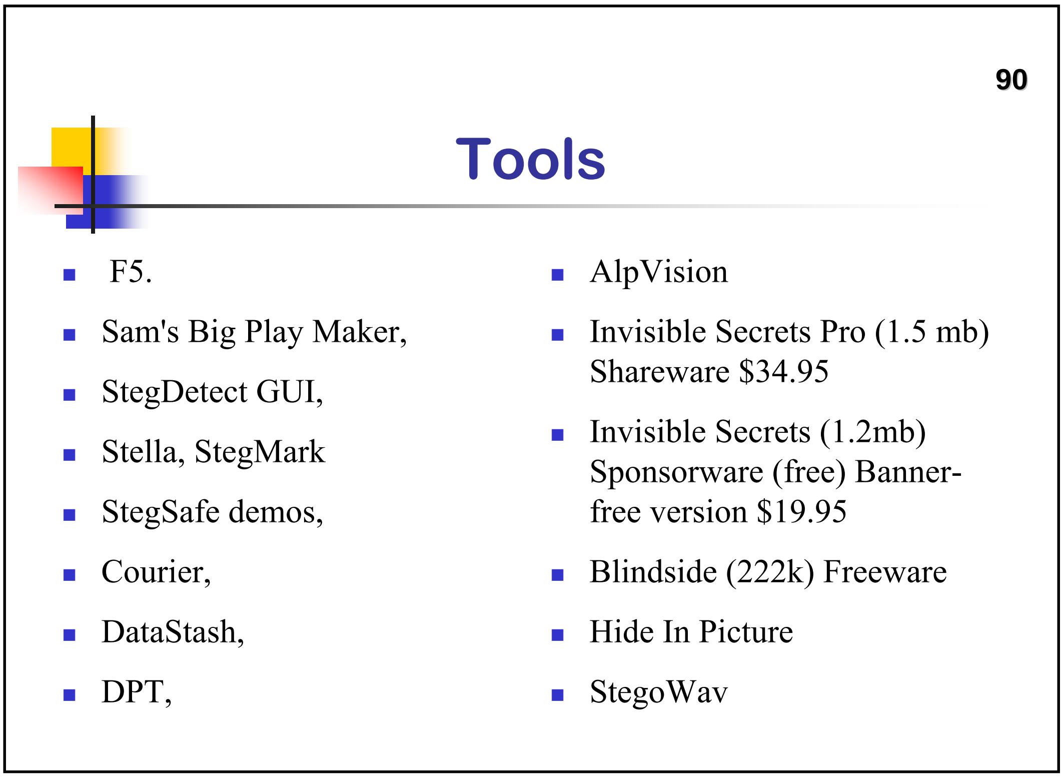
- Steganos Security Suite 6 (11.6 mb) Commercialware $59.95
- SecurEngine 4.0 (2.5 mb) Freeware
- Hermetic Stego (1.7 mb) Shareware $25
- Xidie (1.7 mb) Commercialware $50
- PhotoCrypt 1.1 (195 kb) Freeware
- Camera/Shy,
- Cameleon,
- CryptArkan,



89

Tools

- HideIT
- ImageHide,
- JpegX,
- InfoStego,
- The Third Eye,
- Steganos Security Suite 4,
- Stego Watch,
- StegDetect,
- InPlainView
- BMP Secrets
- wbStego4 (1.1 mb) $20
- Camouflage (2.6 mb)
- Outguess v0.2 (450 kb)
- Stegdetect (333 kb)
- Steganos 3 Security Suite $
- Watermarking World
- .



90

Tools

- F5.
- Sam's Big Play Maker,
- StegDetect GUI,
- Stella, StegMark
- StegSafe demos,
- Courier,
- DataStash,
- DPT,
- AlpVision
- Invisible Secrets Pro (1.5 mb) Shareware $34.95
- Invisible Secrets (1.2mb) Sponsorware (free) Banner-free version $19.95
- Blindside (222k) Freeware
- Hide In Picture
- StegoWav

91

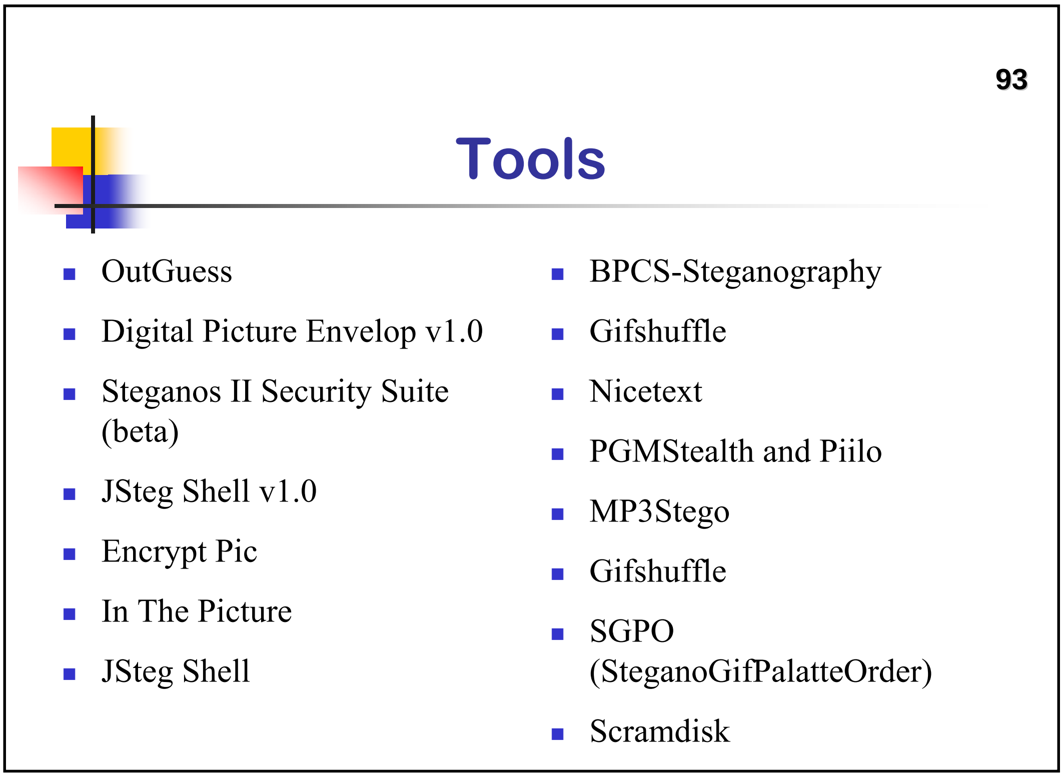
Tools

- StirMark,
- UnZign,
- 2Mosaic
- StegFS,
- JP Hide and Seek,
- SubiText,
- Stealthencrypt,
- DataMark Technologies,
- Stash,
- Invisible Encryption,
- Visible Encryption.
- StegFS (114k) Freeware
- JP Hide and Seek (184k) Freeware
- SubiText (2.4mb) Free Demo/Commercialware $89.50

92

Tools

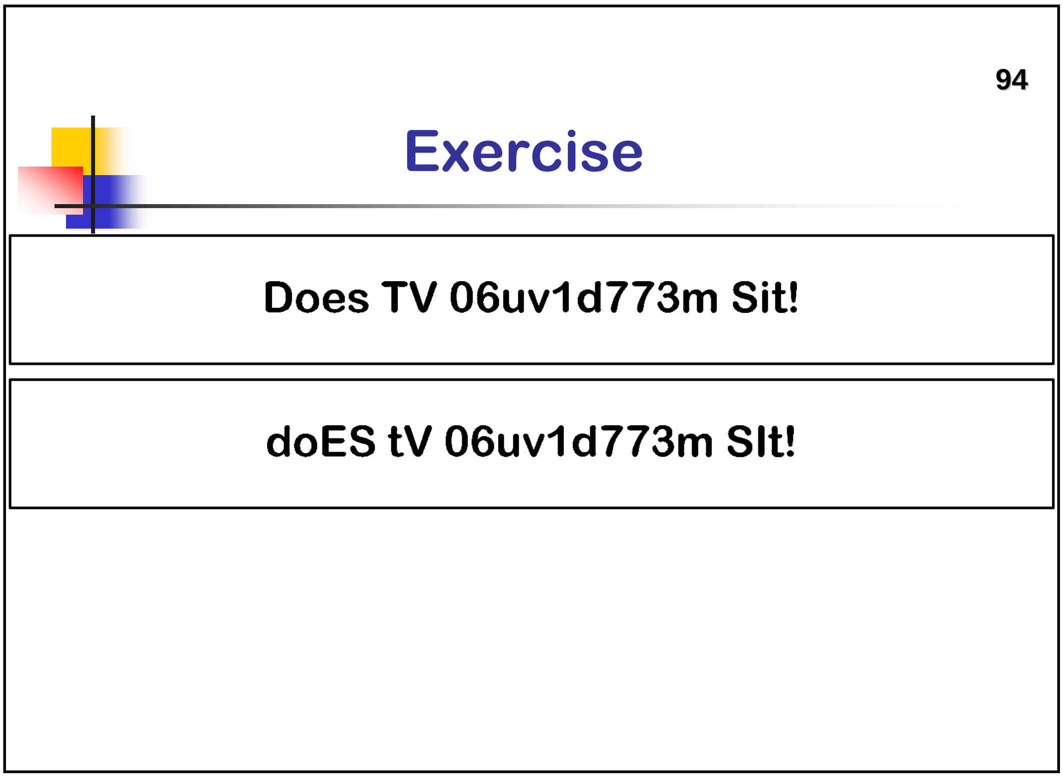
- Stealthencrypt Commercialware
- DataMark Technologies Commercialware
- Stash v1.1 (278k) Freeware
- Invisible Encryption (IVE) (78k) Freeware
- Visible Encryption (VE) (64k) Shareware $40
- Hide4PGP v2.0 (114k)
- S-Mail
- StegParty
- Steganos II Release 4
- Steghide 0.3, release 1
- wbStego99
- Contraband Hell Edition
- Steganos II Security Suite - Final Release



93

Tools

- OutGuess
- Digital Picture Envelop v1.0
- Steganos II Security Suite (beta)
- JSteg Shell v1.0
- Encrypt Pic
- In The Picture
- JSteg Shell
- BPCS-Steganography
- Gifshuffle
- Nicetext
- PGMStealth and Piilo
- MP3Stego
- Gifshuffle
- SGPO (SteganoGifPalatteOrder)
- Scramdisk

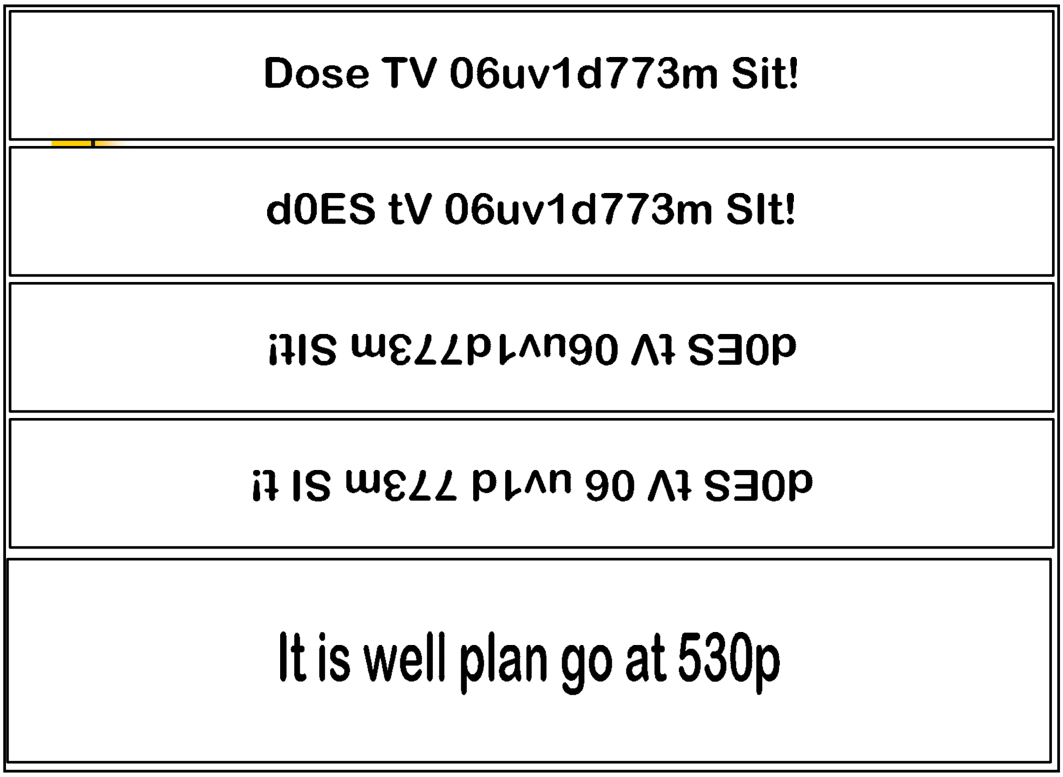


94

Exercise

Does TV 06uv1d773m Sit!

doES tV 06uv1d773m SIt!



Dose TV 06uv1d773m Sit!

d0ES tV 06uv1d773m SIt!

d0ES tV 06uv1d773m SIt!

d0ES tV 06 uv1d 773m SI t!

It is well plan go at 530p