EECS 3482

Introduction to Computer Security

http://www.marw0rm.com/steganography-what-your-eyes-dont-see/

Instructor: N. Vlajic, Fall 2020

Learning Objectives

Upon completion of this material, you should be able to:

- Identify various motivations and implementation approaches to information hiding.
- Describe the basic concepts and uses of digital steganography.
- Explain the key principles pertaining to four common types of digital steganography: plaintext, image, audio and datagram.
- Enlist the common uses of digital watermarking.
- Explain the difference between digital watermarking and digital fingerprinting.

Required Reading

Computer Security, Stallings: Chapter 2

Introduction

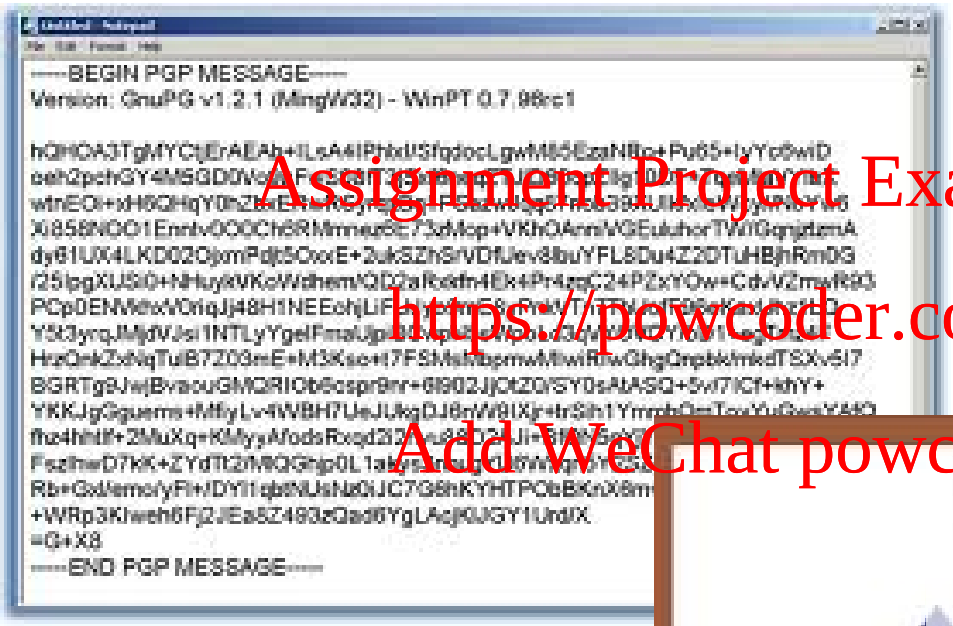
- **WHO Protects Information in Digital Age & WHY?**
  - companies: trade secrets, intel. prop., customer records, ...
  - governments: classified information, citizen records, ...
  - individuals: personal & sensitive information (protect from hackers and/or authorities)

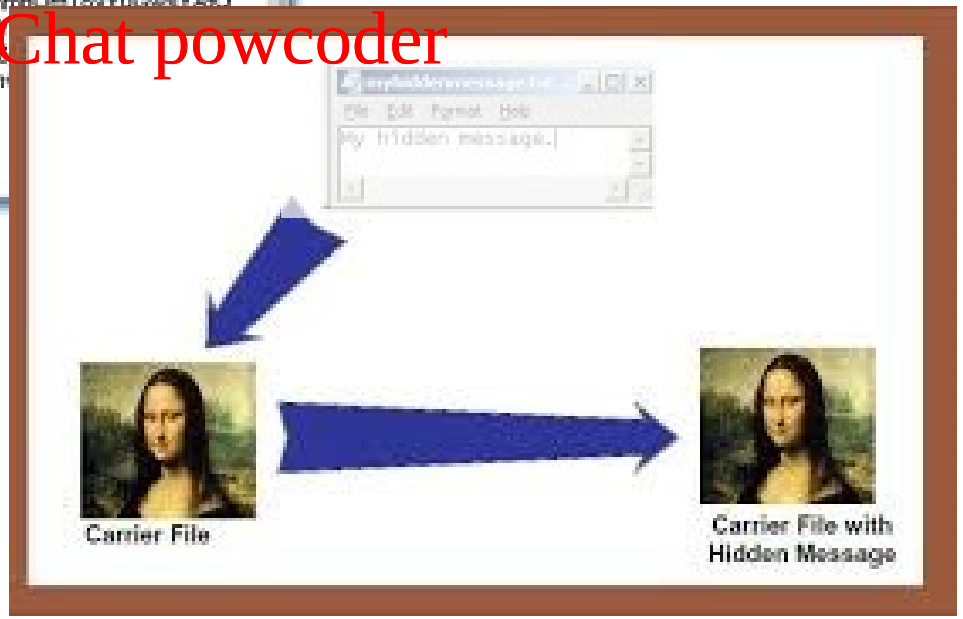
Introduction (cont.)

- **Information Protection in Digital Age** – techniques of digital information protection can be grouped in two major categories:
  - **Information Encryption**
    - the content is 'scrambled' using a crypto-key, so it becomes meaningless
    - however, the presence of encryption is 'obvious'
    - no matter how 'unbreakable', encrypted message will arose suspicion
  - **Information Hiding**
    - the goal is not just to prevent others from accessing hidden information, but to make others unaware of the very existence of the hidden information

Introduction (cont.)

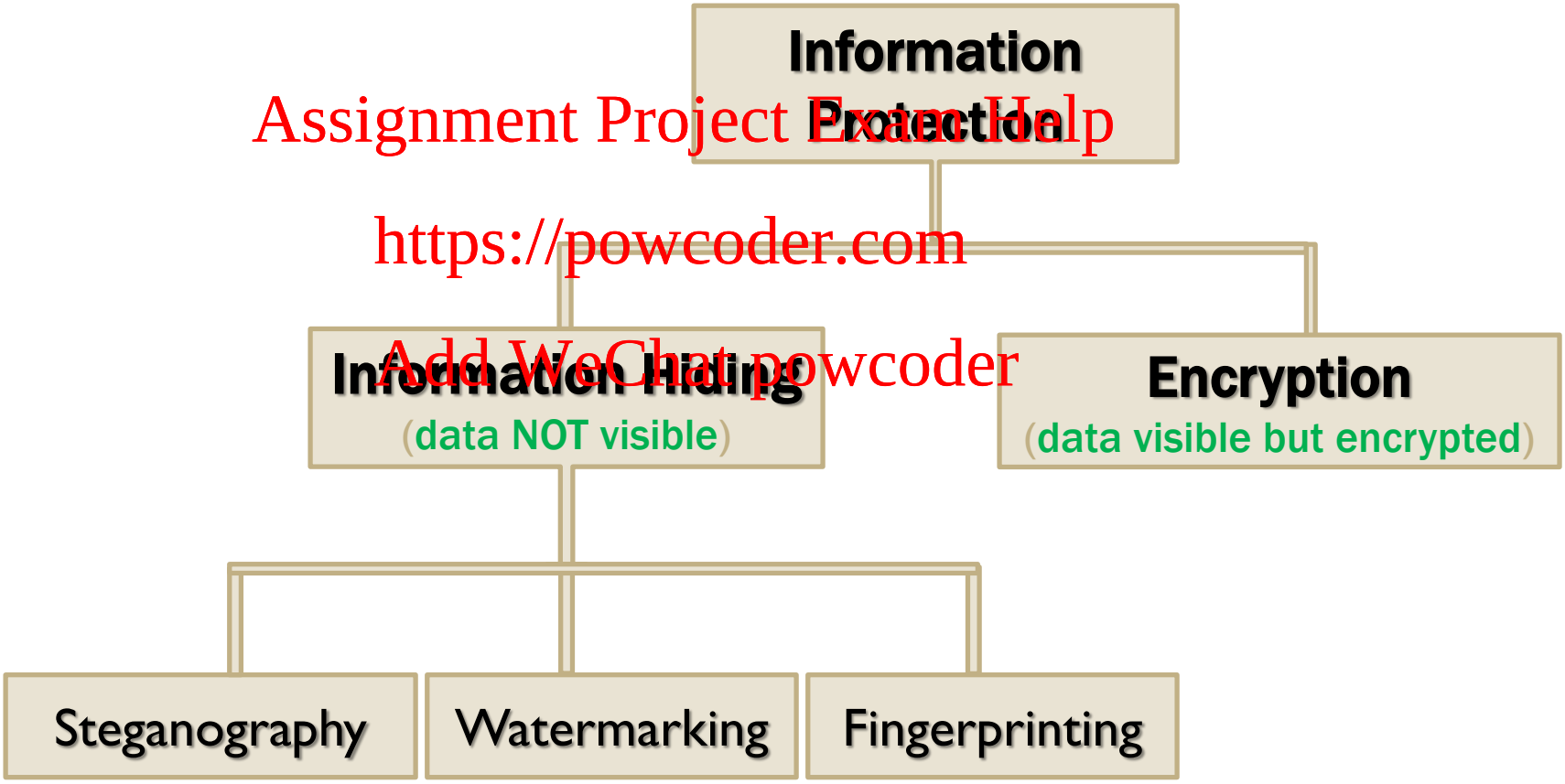
Example: Encryption vs. Information Hiding





Introduction (cont.)

- **Information Protection in Digital Age**

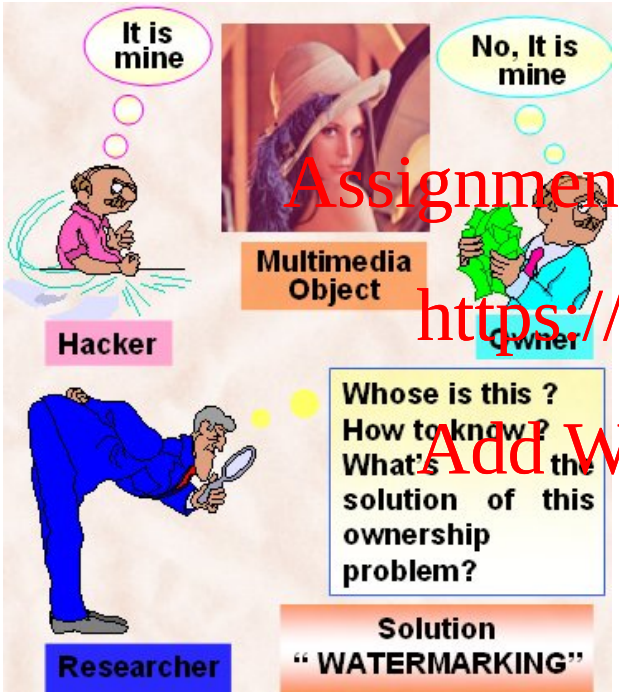


Introduction (cont.)

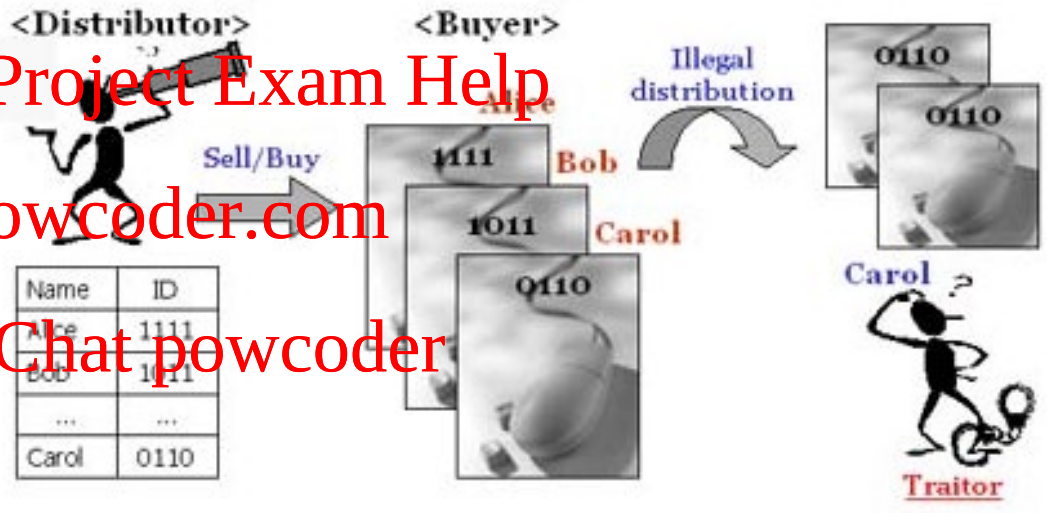
- **Techniques of Information Hiding**
  - **Steganography**
    - steganography – Greek word for "*concealed writing*"
    - art and science of hiding information in some cover media for the purpose of protecting information confidentiality
    - digital steganography – cover media: image, text, audio, video
  - **Watermarking**
    - also aims to make information invisible, but for the purpose of protection of intellectual property
  - **Fingerprinting**
    - embedding user-unique marking to different copies of content for the purpose of tracking of intellectual property

Introduction (cont.)

Example: Watermarking vs. Digital Fingerprinting



http://www.cse.unt.edu/~smohanty/Publications_Others/Mohanty_Masters_Thesis_Spring1999.html



http://itslab.inf.kyushu-u.ac.jp/research/fingerprint.html

The main difference between watermarking and fingerprinting is that the WM remains the same for all copies of the IP while the FP is unique for each copy. As such, FPs … enable tracking of IP misuse conducted by a specific user.

http://aceslab.org/sites/default/files/DeepMarks_ICMR.pdf

Information Hiding: Steganography

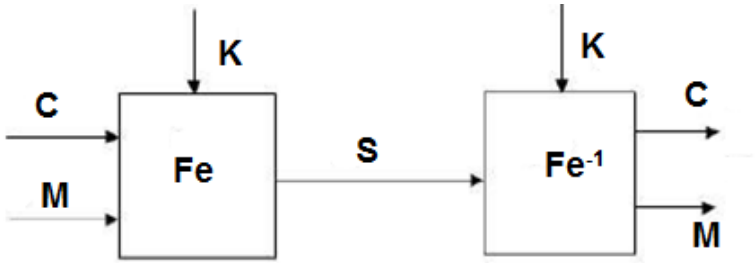
Classical Steganography

- **History of Steganography** – the need to protect information from unsolicited access, by making it obscure, precedes our digital age
  - in ancient Greece, a message would be tattooed on the shaved head of a messenger; the hair would be grown over
  - in era of printed press, different typefaces were used to 'encode' a message
  - in WW2, the French resistance used invisible ink (e.g., wax) to write messages on the back of regular currier

ahzemllyo

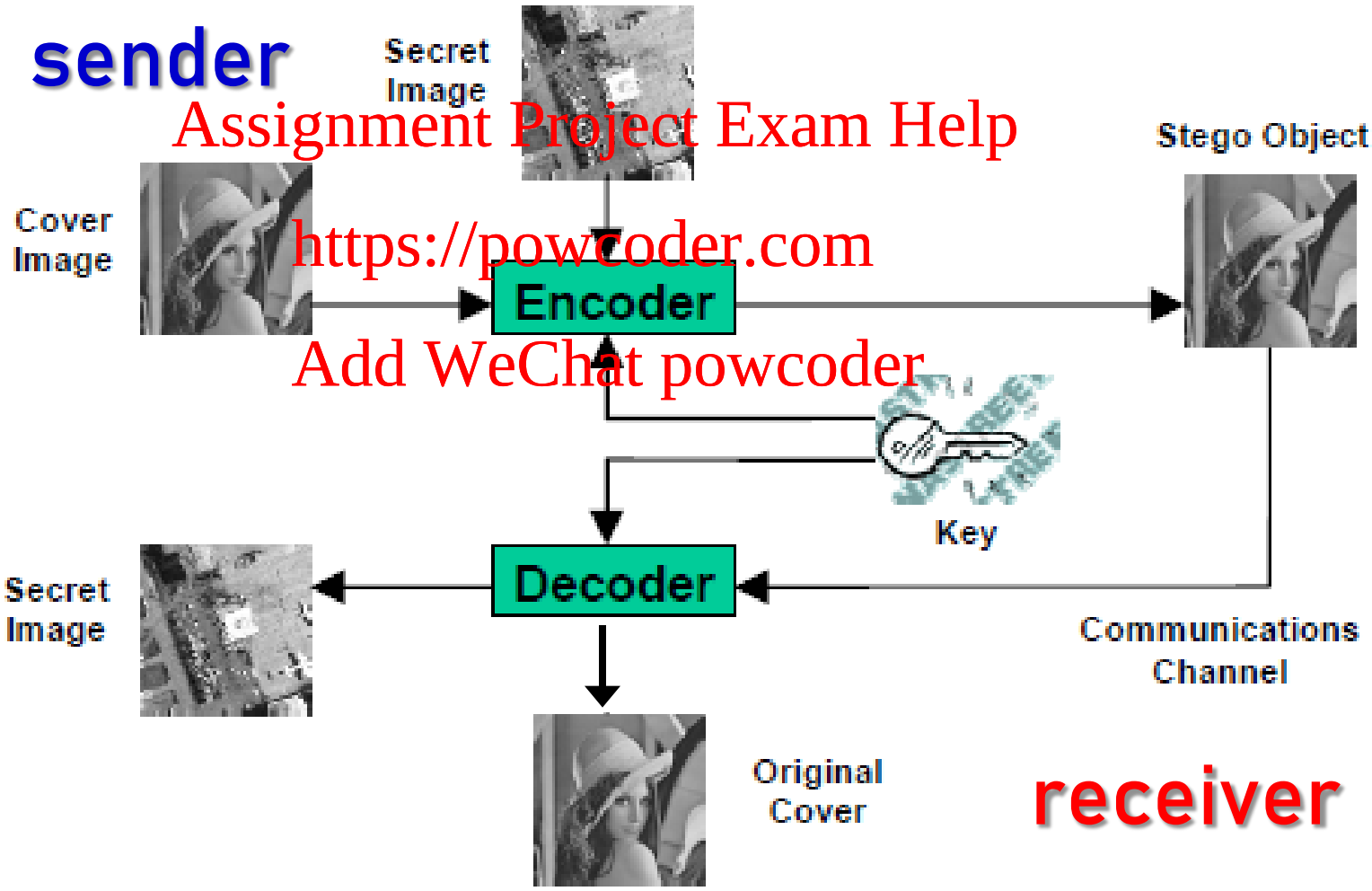
Digital Steganography

- **Digital Steganography**
  - process of hiding information in digital multimedia files and in network packets
  - elements of digital steganography system include
    - cover media (**C**) that will hold the hidden data
    - secret message (**M**) - may be plain text or any other type of data
    - stego function (**Fe**) and its inverse (**Fe^{-1}**)
    - an optional stego-key (**K**) or password to hide and unhide the message
    - stego object (**S**) = cover media + secret message



Digital Steganography (cont.)

Example: Steganography of 'Image inside an Image'



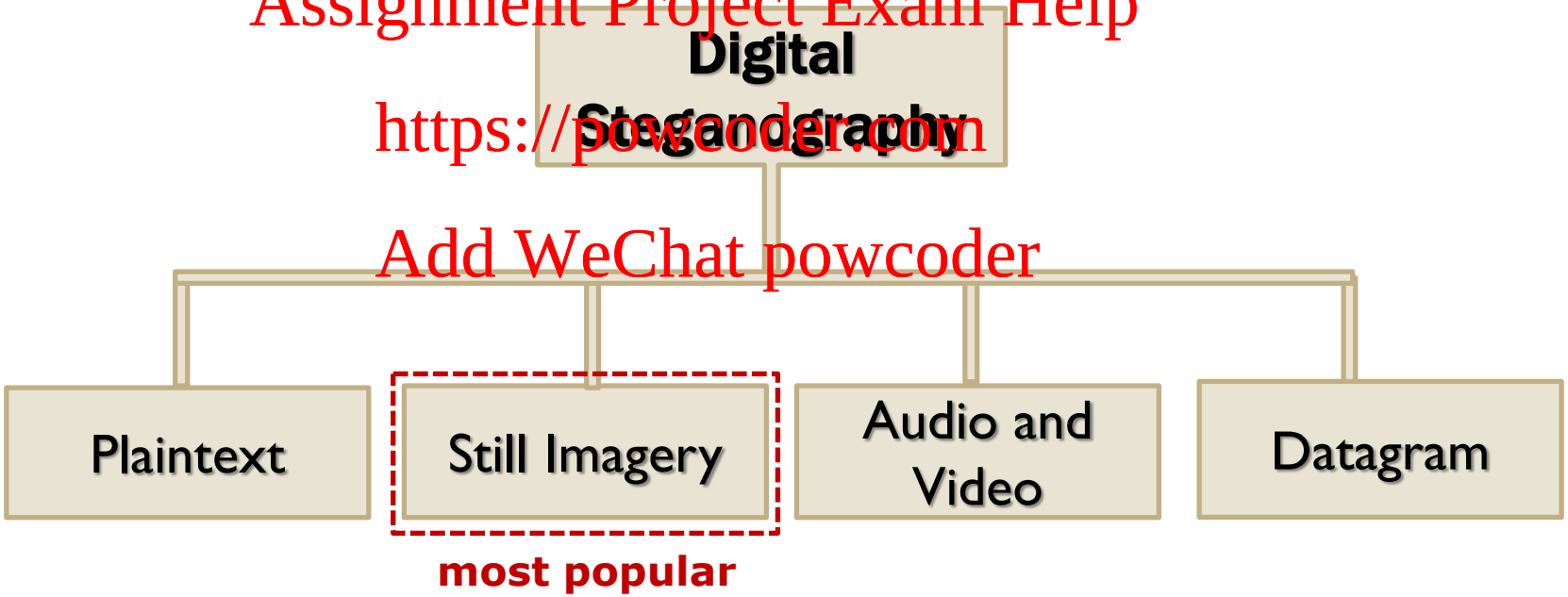
Digital Steganography (cont.)

- **What Makes Steganography Work?**
  - digital steganography takes advantage of
    1) space redundancy in cover media
    2) data redundancy in cover media in combination with inherent weaknesses of human perception

  - ➢ e.g., in computer/text file steganography, information can be hidden in unused areas of the file/text
  - ➢ e.g., in image steganography, information can be embedded in the Least Significant Bits (LSBs) of an image (introduced change is insignificant for human eye)
  - ➢ e.g., in audio steganography, information can be embedded in high frequencies of audio spectrum (human ear is insensitive to slight variations in high audio frequencies)

Digital Steganography (cont.)

- **Techniques of Digital Steganography**
  Based on Type of Cover Media



Plaintext Steganography

1.1) Plaintext Steganography: Use of Selected Characters in Cover Media

- sender sends
  1) text message = stego object
  2) a series of integer number = key
- secret message is hidden within the respective positions of subsequent words in cover media

Example: Plaintext Steganography with Selected Characters

The weather is sunny and wonderful.
They have gone running at the beach.

2 2 1 1 2 2 1 1 4 1 0 0 2

character in each word (to extract)

He is not here.