

**Technical Communication**

**Submitted to**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Submitted by:** Ashish Gupta

2k16/MC/023

Department of Applied Mathematics

Delhi Technological University

Abstract

“Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties.

.”

Table of Contents

Table of Contents

[Book​ 12](#_Toc526175908)

[Newspaper 13](#_Toc526175909)

[Report 13](#_Toc526175910)

[Patent 13](#_Toc526175911)

[Brochure 14](#_Toc526175912)

[Interview 14](#_Toc526175913)

[Letter 14](#_Toc526175914)

[Website 14](#_Toc526175915)

Introduction

The report is divided into 4 parts. In the first part we will discuss what is and the need for image stenography along with the popular methods out there. A discussion in made on which method to use when and why to use it. A look into other methods is also mentioned briefly.

The second part of the report deals with the LCB encryption of images. LCB stands for **least significant bits.** We show how it is the fastest form of encryption. All the mathematics and images involved are thoroughly explained using diagrams and images. The theory includes what are images? How are images similar to giant matrices and why computers are so effective with images? We will then seek out how to hide data into images. We will see how to make data invisible to the naked eyes and undetectable using binary, a heart of digital computing.

The third part deals with implementation using Python, a data science and image processing power house, which owes much of it’s powers into image processing from OpenCV. A brief discussion on OpenCV and python is made. We will see how the images are manipulated as matrices using simple loops and how the process ends up consuming computation power. We will encrypt entire **Harry Potter and the Sorcerer’s Stone** into one image

We end the discussion with the modern day problems into data hiding and how this technique of data hiding is already transforming millions of people’s lives. We will see how copyright laws are enforced easily using this technique and why medical imaging of brains owes its origins to this technique. Later at the end everything is summarized in conclusions and future research into the topic is highlighted along with various sources for study.

Data Hiding

Data Hiding is a very ancient art. It is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message.

* Caesar cipher.
* Egyptians used symbolic language in their pyramids.
* Coded Language.
* Writing with invisible ink.

With the dawn of the Digital World, now just the methods have changed, but the aim is still the same.

In Modern Times, Data Hiding is associated with digital forms such as cryptography, steganography, and watermarking.

1. **Cryptography** is obscuring the content of the message, but not the communication of the message.
2. **Steganography** which is Greek for “covered writing” is hiding the very communication of the message.
3. **Watermarking** attempts to add sufficient metadata to a message to establish ownership, provenance, source, etc.

A natural question to ask is why data hiding is so necessary. There are numerous reasons:

* Personal, Private Data.
* Sensitive Data.
* Confidential Data, Trade Secrets.
* To avoid Misuse of Data.
* Unintentional damage to data, human error, accidental deletion avoidance
* Monetary and law purposes.
* Hide Traces of a crime.
* As a backup.
* Storing passwords.

Image Stenography

**Steganography** is also the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication.

The basic structure of Steganography is made up of three components: the “carrier”, the message, and the key. The carrier can be a painting, **a** **digital image**, an mp3, even a TCP/IP packet among other things. It is the object that will ‘carry’ the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light, or even lemon juice.

Thus in Image Stenography following are the 3 components:

1. **Carrier:** A digital image.
2. **Message:** Any text file or dataset will do that is <1/4th of size of image.
3. **Key:** LSB encryption and decryption.

The properties of Image Steganography may be substituted with audio mp3’s, zip archives, and any other digital document format relatively easily. Hence this report becomes a ground work into future exploration. It is impossible to tell the difference between a **carrier image** and **normal image** with naked eyes.

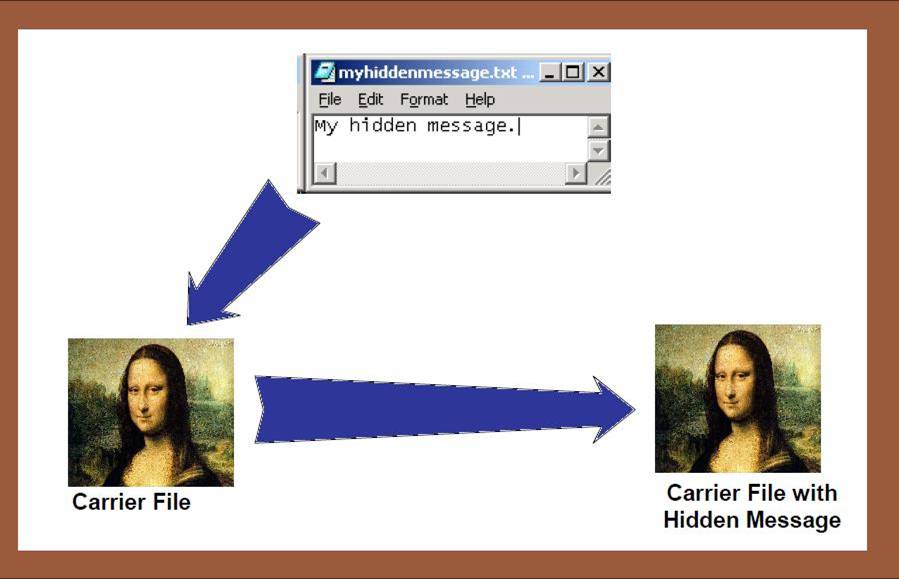


Image: depicts image stenography. Exactly same to eyes.

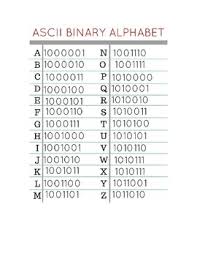
Theoretical Discussion

A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically grey images use 8 bits(XXXX-XXXX), whereas color utilizes 24 bits to describe the color model, such as RGB model(8bits-8bits-8bits). The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover image. The spatial domain techniques manipulate the cover image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).

The concept of LSB Embedding is simple. It exploits the fact that **the level of precision in many image formats is far greater than that perceivable by average human vision.** Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, this requires eight bytes of pixels to store 2 bytes of secret data.

Here are the steps involved in the stenography. It is important to remember the simplicity of the model makes it very powerful to use.

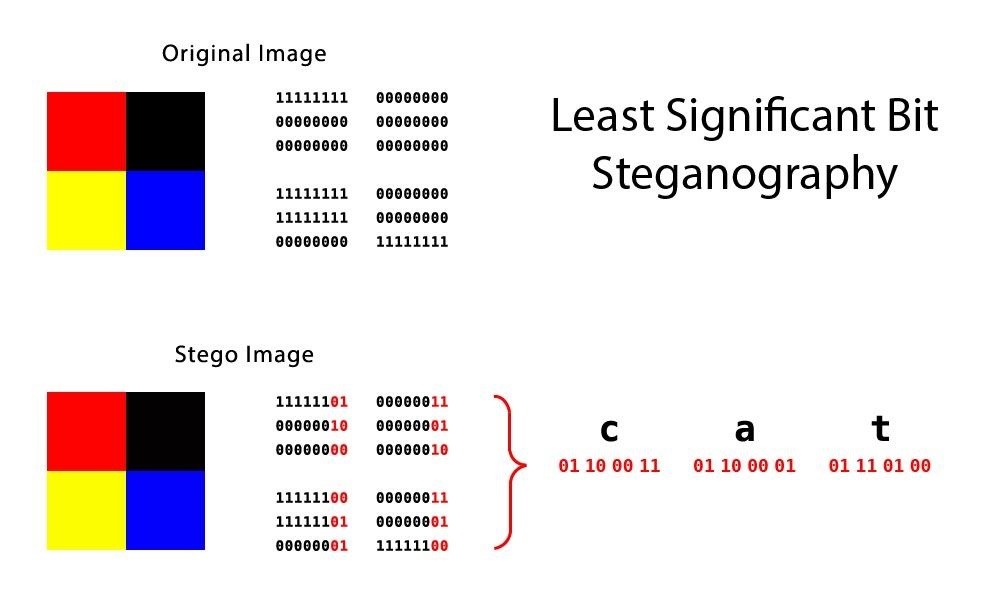
**Step 1: Convert the message to binary.** A message is converted to binary by using ascii table in Computer Science. A reference has been mentioned in the appendix 1 of this report. Here is a list of characters with ascii in binary:



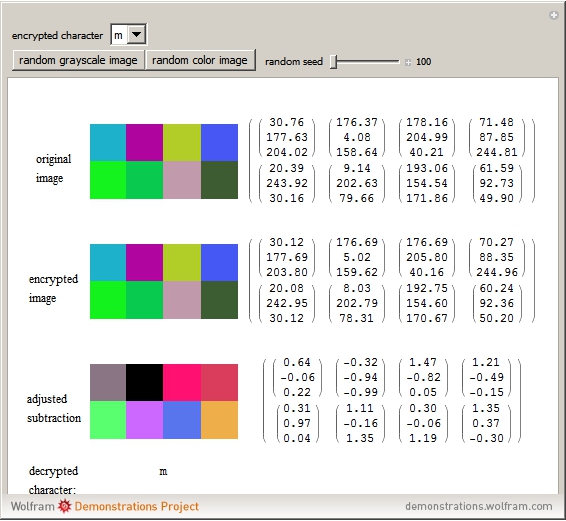
Hence the message “**This is hidden**” transforms to – **0101010001101000011010010111001100100000011010010111001100100000010010000110100101100100011001000110010101101110**

Note that a space has a separate binary number.

**Step 2: Encode the above message to image into the last 2 bits of each number.** So if the image is made of numbers, then those numbers range from 0-255 (only for images into computers.

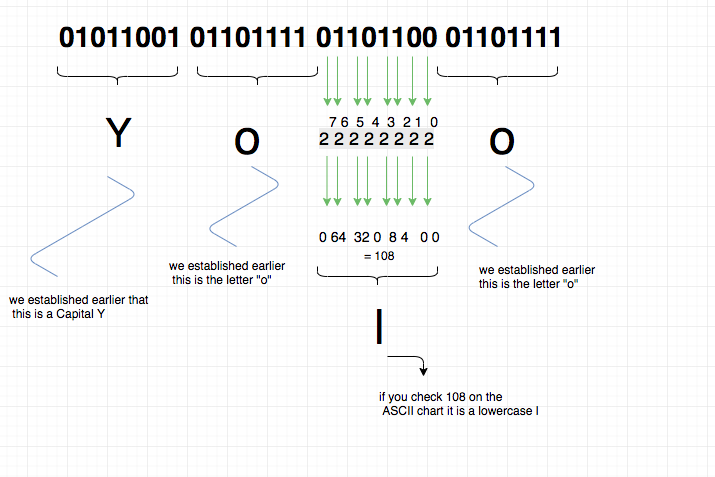


[Above] The red digits are the encrypted letters. See that 3 patterns are linked to 1 image due to 8bit-8bit-8bit nature of images.

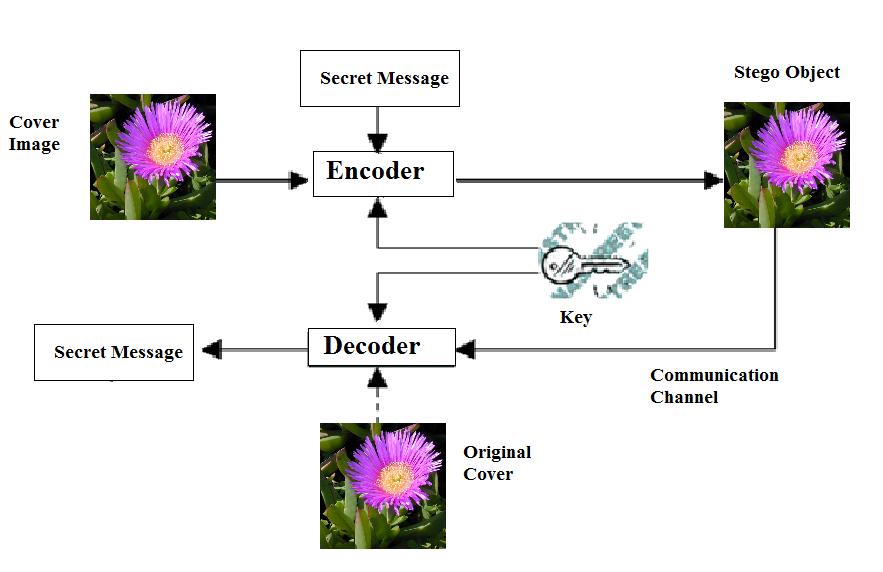


[Above] In implementation, numbers are altered to +/- 3 their values. Human eyes are not sensitive enough to notice change of +3 or -3 in this.

**Step 3: The image stenography is done.** Now the information can be reversed back from the image using the reverse technique.Take the last 2 bits of every number into image and convert it back to binary.

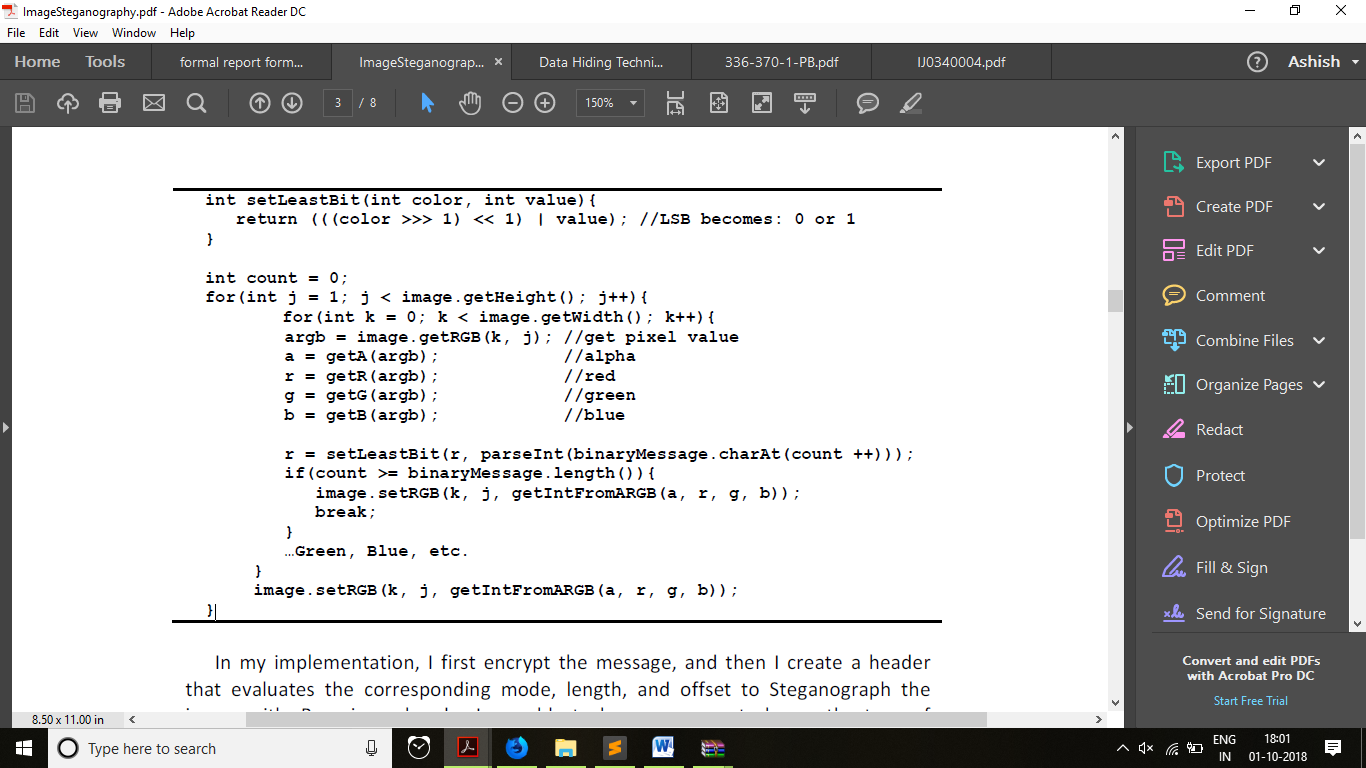


A simple demonstration of the conversion



[Above] To summarize the above information this is what it looks like.

# Algorithm:



**Embedding Algorithm (An explanation)**

In this process of encoding method, a random key is used to randomised the cover image and then hide the bits of a secret message into the least significant bit of the pixels within a cover image. The transmitting and receiving end share the steno key and random-key. The random-key is usually used to seed a pseudo-random number generator to select pixel locations in an image for embedding the secret message.

**Inputs:** Cover image, steno-key and the message

**Output:** steno image

**Instructions**

1) Read character from text \_le that is to be hidden and convert the ASCII value of the character into equivalent binary value into an 8 bit integer array.

2) Read the RGB colour image(cover image) into which the message is to be embedded.

3) Read the last bit of red pixel.

4) Initialize the random key and randomly permute the pixels of cover image and reshape into a matrix.

5) Initialize the steno-key and XOR with text to be hidden and give message.

6) Insert the bits of the secret message to the LSB of the Red plane's pixels.

7) Write the above pixel to Steno Image File.

**Extraction of Hidden Message**

In this process of extraction, the process takes the key and then random key. These keys take out the points of the LSB where the secret message is randomly distributed. Decoding process searches the hidden bits of a secret message into the least significant bit of the pixels within a cover image using the random key. In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the steno key.

**Inputs** Steno image, steno key, random key.

**Output**: Secret message.

1) Open the Steno image in read mode and from the image, read the RGB colour of each pixel.

2) Extract the red component of the host image.

3) Read the last bit of each pixel.

4) Initialize the random-key that gives the position of the message bits in the red pixel that are embedded randomly.

5) For decoding, select the pixels and Extract the LSB value of red pixels.

7) Read each of pixels then content of the array converts into decimal value that is actually ASCII value of hidden character.

8) ASCII values got from above is XOR with steno key and gives message, which we hide inside the cover image.

Conclusion

// Avoid jargon and add a summary of what the report was all about

// here everything comes together ?

// So, the video processing helps preserve data into videos and encrypts it into a video compressed using one of the various compression methods like mp4 or avi or png-Gif. And so on

Appendix 1: Ascii

Future research left

References

CPSC 350 Data Structures:

Image Steganography

Nick Nabavian

[nabav100@chapman.edu](mailto:nabav100@chapman.edu)

**Volume 3, No. 3, March 2012** *Journal of Global Research in Computer Science* **RESEARCH PAPER Available Online at www.jgrcs.info** © JGRCS 2010, All Rights Reserved 53

**IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY**

### [Chapter 3 LEAST SIGNIFICANT BIT STEGANOGRAPHY TECHNIQUE ...](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwik_Z-PoOXdAhUBUI8KHTmQDh8QFjABegQICRAE&url=http%3A%2F%2Fshodhganga.inflibnet.ac.in%2Fbitstream%2F10603%2F41637%2F10%2F10_chapter%25203.pdf&usg=AOvVaw1a8UECrjEPGdJzIWdVdv5M)

[shodhganga.inflibnet.ac.in/bitstream/10603/41637/10/10\_chapter%203.pdf](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwik_Z-PoOXdAhUBUI8KHTmQDh8QFjABegQICRAE&url=http%3A%2F%2Fshodhganga.inflibnet.ac.in%2Fbitstream%2F10603%2F41637%2F10%2F10_chapter%25203.pdf&usg=AOvVaw1a8UECrjEPGdJzIWdVdv5M)

<https://www.slideshare.net/SreelekshmiSree1/image-steganography-using-lsb>

<https://www.slideshare.net/prashant3535/data-hiding-techniques?from_action=save>

**References.** When incorporating the opinions, data, and illustrations of other sources into your writing, you must give credit to those sources. For information of how to paraphrase and quote sources, see [Appendix B](http://writing.engr.psu.edu/workbooks/documentation.html). In these writing guidelines, the format for bestowing that credit is an author-year referencing system. Within the text of the article or report, references should be cited by giving in brackets the last name of the author(s) and the year of publication of the reference. The year should always be enclosed in brackets; whether the name of the author(s) is enclosed depends on the context. The two possibilities are illustrated as follows:​

|  |  |  |
| --- | --- | --- |
|  | Recently, a new chemical process was developed for eliminating nitrogen oxide emissions from diesel engines [Perry and Siebers, 1986]. ​ Recently, Perry and Siebers [1986] developed a new chemical process for eliminating nitrogen oxide emissions from diesel engines |  |

        For three or more authors, just list the first author's name as follows: [Lee and others, 1972]. If there is no author listed, give the first word (not articles, conjunctions, or prepositions) of the document: [Manual, 1983] or ["Plastic", 1989]. If you have two documents with the same author and year (for example, two documents by Jones in 2003), then assign the reference listings as follows: [Jones, 2003a] for the citation that alphabetically appears first at the end, and [Jones, 2003b] for the citation that appears second at the end.  
        The full reference citations will appear in an alphabetical list at the end of your document. Given below are examples of the listings.

## Book​

|  |  |  |
| --- | --- | --- |
|  | **Author, Title in Initial Capitals and Italics, edition # (City of Publication: Publisher, Date of Publication).**  ​Fox, R.W., and A.T. McDonald, Introduction to Fluid Mechanics (New York: John Wiley & Sons, 1978). A Manual of Style, 12th ed. (Chicago: The University of Chicago Press, 1969).  McElroy, W.D., Cell Physiology and Biochemistry, 3rd ed., Foundations of Modern Biology Series (Englewood Cliffs, N.J.: Prentice-Hall, 1971). |  |

## Newspaper

|  |  |  |
| --- | --- | --- |
|  | **Author (if known), "Title in Initial Capitals and Quotation Marks,"Newspaper Name (Date), section #, page #s.**  Luoma, J.R., "U.S. Hunts New Ways to Clean Up Wastes," New York Times (3 January 1988), pp. 15, 18.  ​"Plastic Explosives Blamed for Airline Disaster," New York Times (3 January 1989) sec. 2, p. 11. |  |

## Report

|  |  |  |
| --- | --- | --- |
|  | **Author, Title in Initial Capitals and Italics, Report # (City of Publication: Publisher (Company or Agency), Date).**  Borcherdt, R.D., Results and Data From Seismologic and Geologic Studies Following Earthquakes of December 7, 1988, Near Spitak, Armenia SSR, vol. 1, USGS OFR 89-163-A (Washington, D.C.: U.S. Geological Survey, 1989). Guide to Operations, IBM Personal Computer Hardware Reference Library #1502490 (Boca Raton, Florida: IBM Corporation, 1984). Spent Fuel Storage Requirements, DOE RL-88-34 (Richland, WA: Department of Energy, 1988).  ​Sheldon, K.E., Analysis Methods to Control Performance Variability and Cost in Turbine Engine Manufacturing (Blacksburg, VA: Virginia Tech, 4 May 2001), pp. 156-158. |  |

## Patent

|  |  |  |
| --- | --- | --- |
|  | **Patent Holder, Patent # (Date of Patent).**  ​Lyon, R.K., U.S. Patent No. 3,900,554 (August 1975). |  |

## Brochure

|  |  |  |
| --- | --- | --- |
|  | **Author, "Title in Initial Capitals and Quotation Marks," brochure (City of Publication: Publisher (Company or Agency), Date).**  ​Cheng, D., "Chemtronix XT Manometer," brochure (Asheville, NC: Chemtronix Corporation, 1974). |  |

## Interview

|  |  |  |
| --- | --- | --- |
|  | **Speaker's Name, Speaker's Affiliation (City of Interview: Date of Interview), type of interview.**  ​Lee, R., Engineer at Apple Corporation (San Jose: 5 June 1987), phone interview |  |

## Letter

|  |  |  |
| --- | --- | --- |
|  | **Author, Affiliation (City: Date of Letter), recipient of letter.**  ​Alley, C.D., Plant Manager of Mason-Hanger Pantex Plant (Amarillo, TX: 3 March 1989), letter to Amarillo Globe News. |  |

## Website

|  |  |
| --- | --- |
|  | **Author, "Title," web listing in italics (City: Publisher, Date).**  ​Bassett, Vicki, "Causes and Effects of the Rapid Sinking of the Titanic," <http://writing.engr.psu.edu/uer/bassett.html> (University Park, PA: Undergraduate Engineering Review, November 1998).  Varian Corporation, "Smithsonian Researchers Use High-Tech Digital Imaging Device to Study C |