Presented By: Harrison Redd

FUBSWRJUDSKB DQG VWHJDQRJUDSKB VHFUHWV KLGGHQ LQ SODLQ VLJKW

Presented By: Harrison Redd

CRYPTOGRAPHY AND STEGANOGRAPHY SECRETS HIDDEN IN PLAIN SIGHT

Crypotology

- Cryptology is the science of encrypting messages to provide security and protection of vital information.
- The word cryptography comes from the Greek word kryptos, meaning hidden or secret.
- Cryptography has been used throughout history as a method of disguising secrets.

A Quick History

- In 100-44 BC Caesar used a simple substitution in the normal alphabet to encrypt government communications.
- In 1790 Thomas Jefferson invented the wheel cipher which was retooled until it became the Strip Cipher used in WW-II by the Navy
- Native American Code Talkers were used in both World Wars in order to encrypt military messages.

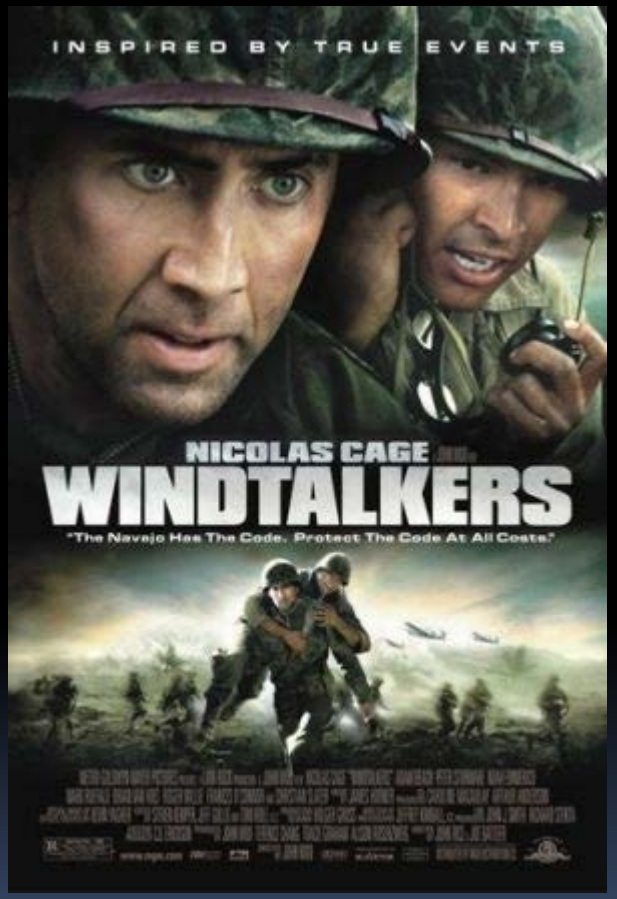
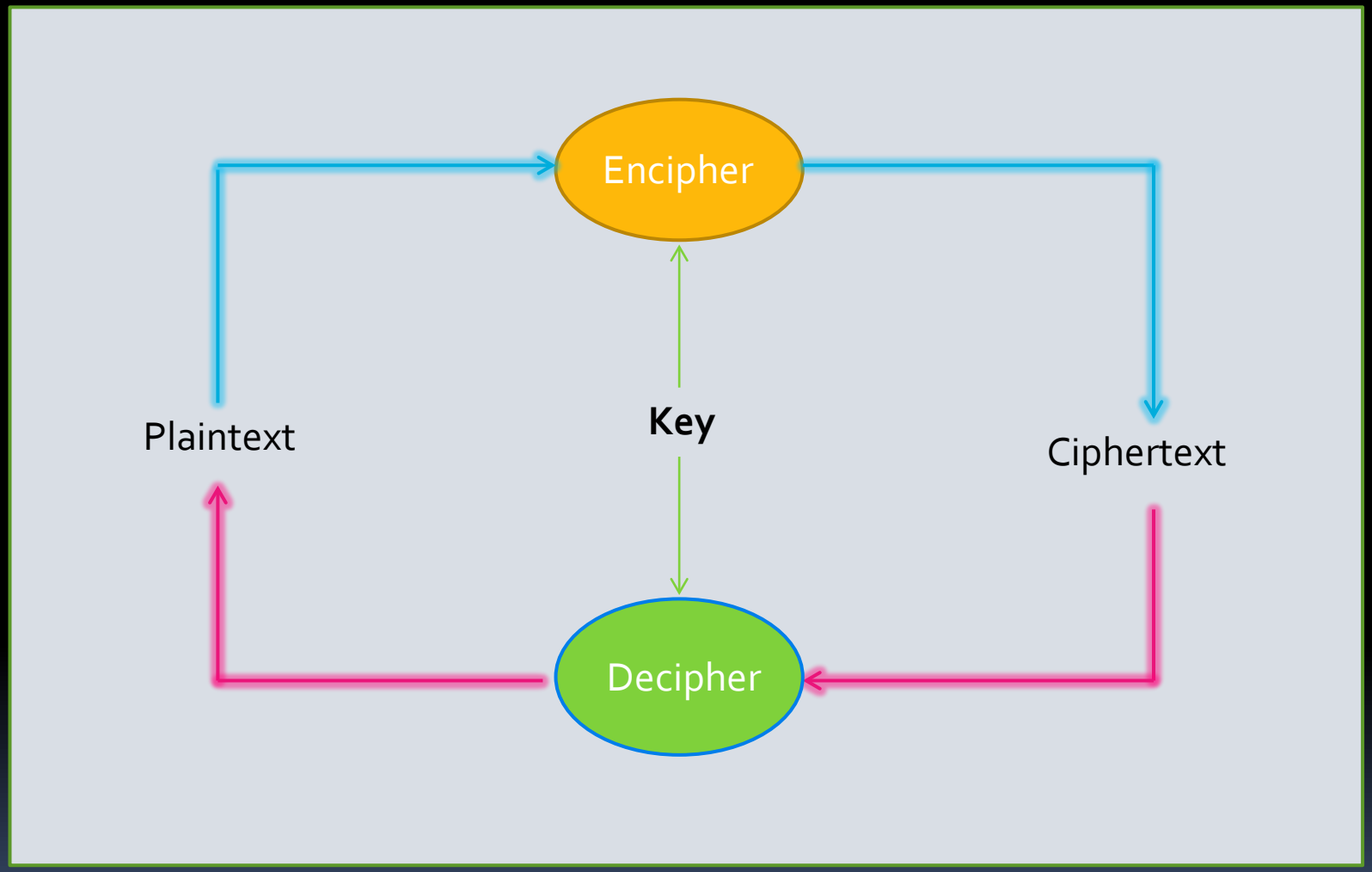


Image courtesy of imdb.com

Some Basic Terms

In order to understand Cryptography it is necessary to start at the basics with some common terms.

- **Plaintext**: Normal unencrypted writing
- **Encryption**: Process of encrypting a piece of plaintext
- **Ciphertext**: Text that has become encrypted
- **Decryption**: The Decrypting of cipher text
- **Key**: The program used to Decode and Encode text
- **Cipher**: The secret method of writing


Encipher
Plaintext
Key
Ciphertext
Decipher

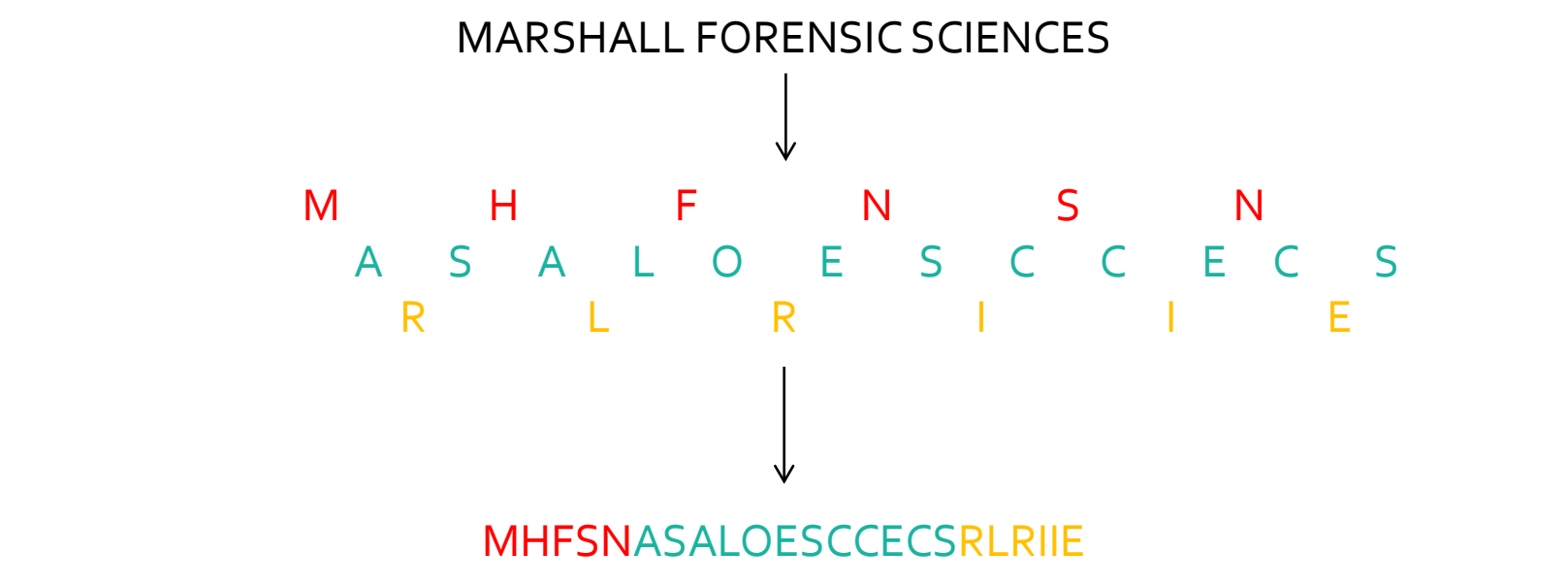
Categories of Ciphers

- There are two general categories of ciphers they include:
  - Transposition Ciphers
  - Substitution Ciphers

Transposition Ciphers

These ciphers rearrange bits of characters in the data. The cipher below is known as a railroad cipher.

- A Railroad Cipher arranges the data in angled rails and scrambles the letters by reordering the letters via the created rows.



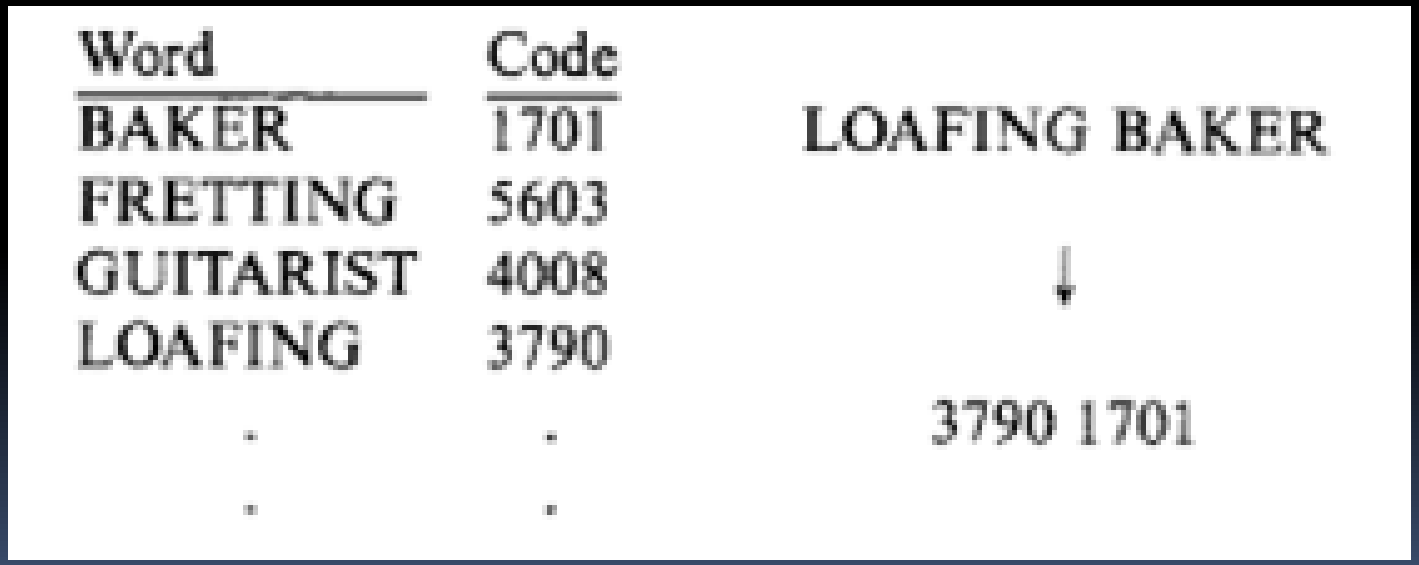
Substitution Ciphers

These ciphers replace bits, characters, or blocks of characters with substitutes.

- Below is an example of a Caesar Cipher in which each letter has been replaced with the one three letters to the right.

Code

- A code is a special form of substitution cipher that requires a "code book" as the key.



Word	Code
BAKER	1701
FRETTING	5603
GUITARIST	4008
LOAFING	3790
.	.
.	.

LOAFING BAKER

↓

3790 1701

Image courtesy of Handbook of Applied Cryptography

Cryptographic Systems

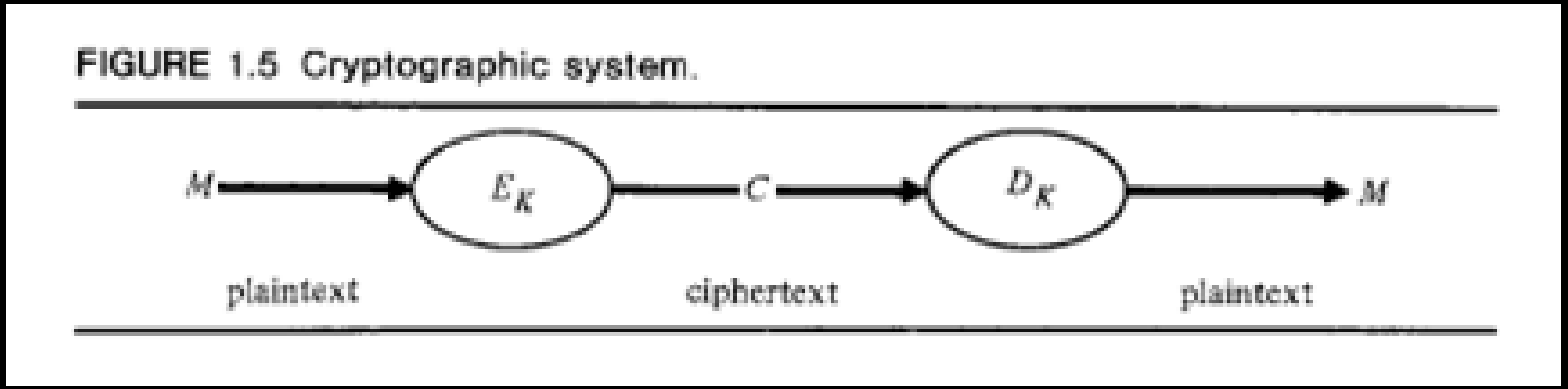


Image courtesy of Handbook of Applied Cryptography

Cryptographic Systems Cont.

There are three general requirements for all cryptographic systems:

1. The enciphering and deciphering transformations must be efficient for all keys
2. The system must be easy to use
3. The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithm.

1. Efficiency

The system must be efficient since cryptographic systems are primarily used in computer applications.

Since the enciphering and deciphering of data generally occurs at the time of transmission it is important that the process isn't held up by the algorithms.

2. Easy to Use

It is important that the cryptographer is able to find a key with an invertible transformation.

The word invertible means that it is possible to easily reverse the key to decode the message quickly.

3. Secrecy depends on the keys

This is one of the most important rules of cryptography. Most algorithms used in encryption are well known to the world and can be easily looked up in available texts or on the internet.

The algorithm is useless unless the key is known. For example if using a simple Caesar Cipher it is still very difficult to decipher without knowing how many letters across a person changed the system.

How is Cryptography used today

Some common place uses of Cryptography are within your computer and your ATM cards.

ATMs: The Pins that are given to you or set by for your ATM card are encrypted by an algorithm that is managed by banking institutions.

Computer Passwords

Your computer password is another point of encryption that controls the safety of your computer.

For example: A password Purplepandas is not that secure since it could easily be determined by an exhaustive attack

While a password like Enter57684#:/ is very random and will be difficult to determine.

3 Forms of Ciphers used Today

1. One-time Pad
2. Stream Cipher
3. Block Cipher

One-time Pad

This is considered an unbreakable code. A One-time pad uses a key that is randomly generated and will never be used again.

While this method is considered very secure it has some issues:

- The method requires a large amount of key material since each letter needs a corresponding key as well as very secure delivery of the key
- Also truly random numbers can be very hard to generate with today's computer systems.

One-time Pad Example

An example is as follows Alice is trying to send a message to Bob:

- Alice randomly generates a string of numbers to be used as the key: 1042
- Alice encrypts "Mark" by shifting each letter by a number in the key, using each number only once for each letter: NAVM
- Bob decrypts the ciphertext using the same string "1042": Mark
- Both Alice and Bob throw away the key "1042," never to be used again.

Stream Ciphers

A stream cipher is the attempt to imitate a one-time pad while attempting to reduce the size of the key to a 128 bit key.

The system attempts to make a unique key by stringing together various keys in a random stream.

Historic Uses of Stream Ciphers:

- WEP, used to encrypt wireless networks
- SSL, used for packets of data
- A5/1, used to encrypt voice over cell phones

All three of these have been replaced.

Problems with Stream Ciphers

- WEP has been found to be hacked in less than a minute.
- 4 years after an article was published with the problems of WEP, TJ Maxx was hacked in 2005 and credit card information was stolen.
- WEP has been replaced by WEP-2 which uses Block Ciphers

Block Ciphers

These are the most recent and most effective ciphers in use today.

- An example is separating a book into pages, taking a page of that text, and substitution and rearranging the words, then putting the book back together.

So Why all this Security?

Cryptanalysis is the science and study of methods of breaking ciphers.

Cryptanalysts use things called attacks in order to attempt to break ciphers.

These attacks can be broken into three general categories.

Attacks used in Cryptanalysis

1. Ciphertext-only attack
2. Known-plaintext
3. Chosen-plaintext

Chosen-plaintext Attack

- This is the most favorable situation for the cryptanalyst.
- This form of attack requires the cryptanalyst to acquire ciphertext related to specific plaintext.
- Databases are the most vulnerable to this form attack since an attacker can simply submit their own content and observe the encryption that occurs and reverse engineer the process.

Steganography

Steganography is a similar system to cryptography but the difference is that Steganography passes secret information in plain view and within total access to the common people.

How?

Steganography uses software and algorithms to hide confidential data within common files, audio, picture, pdf, video etc.

Steganography

Two main classes:

- Technical Steganography:
  - This is a scientific method to hide data
- Linguistic Steganography:
  - This technique hides the message within the carrier in non-obvious ways

Technical Steganography

5 Primary Techniques:

1. Video Steganography
2. Audio Steganography
3. Text Steganography
4. Image Steganography
5. Protocol Steganography

Video Steganography

Files are hidden within the audio and image files of the video.

A slight distortion may occur but it is almost imperceptible to humans.

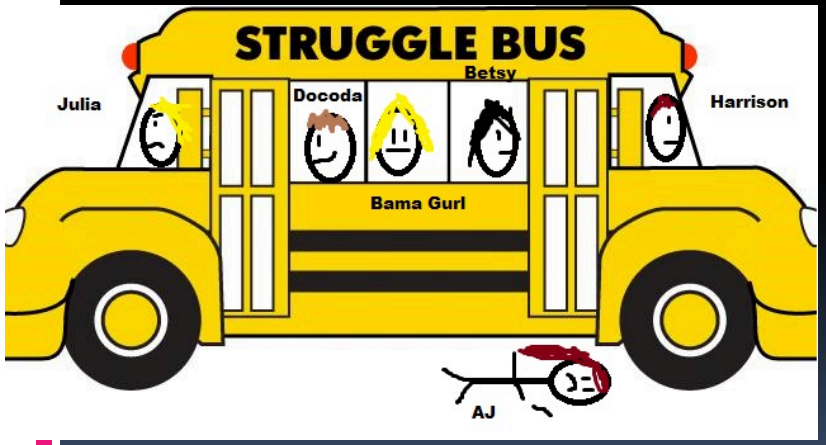
Audio Steganography

Secret messages are embedded in a digital sound.

The message is placed by slightly altering the binary sequence and a change in may be hardly noticeable without special auditory equipment.

Example of Technical-Image

- To show an example I hid the image on the left within the image on the right



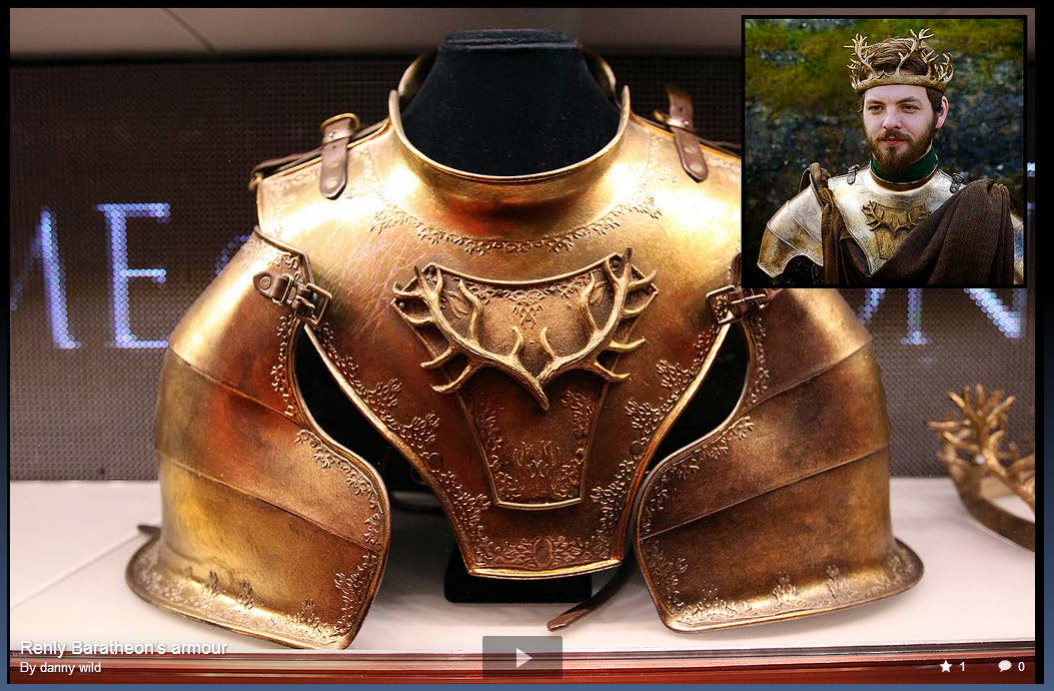


Image courtesy of Google Images

Image before Steganography

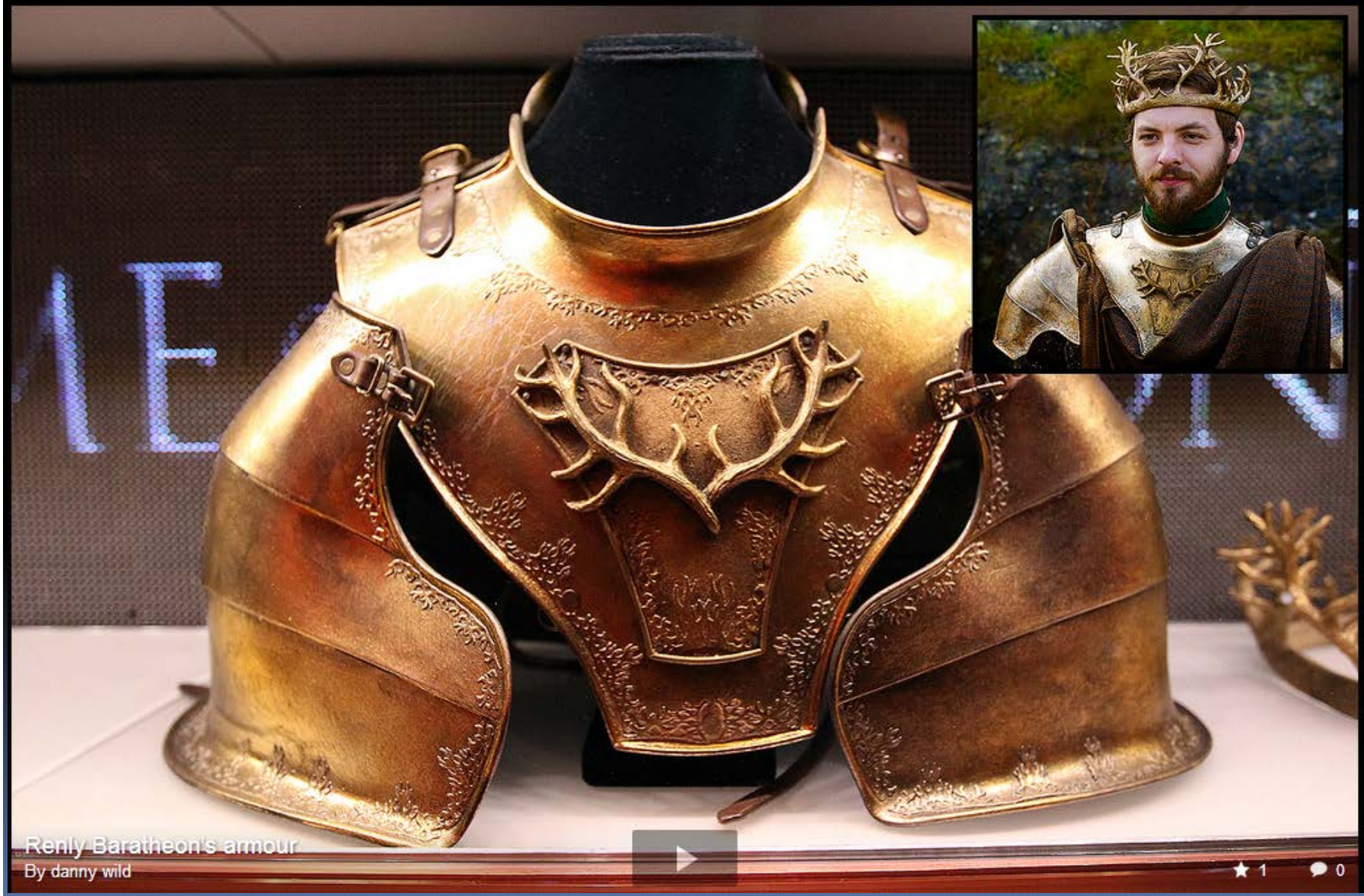
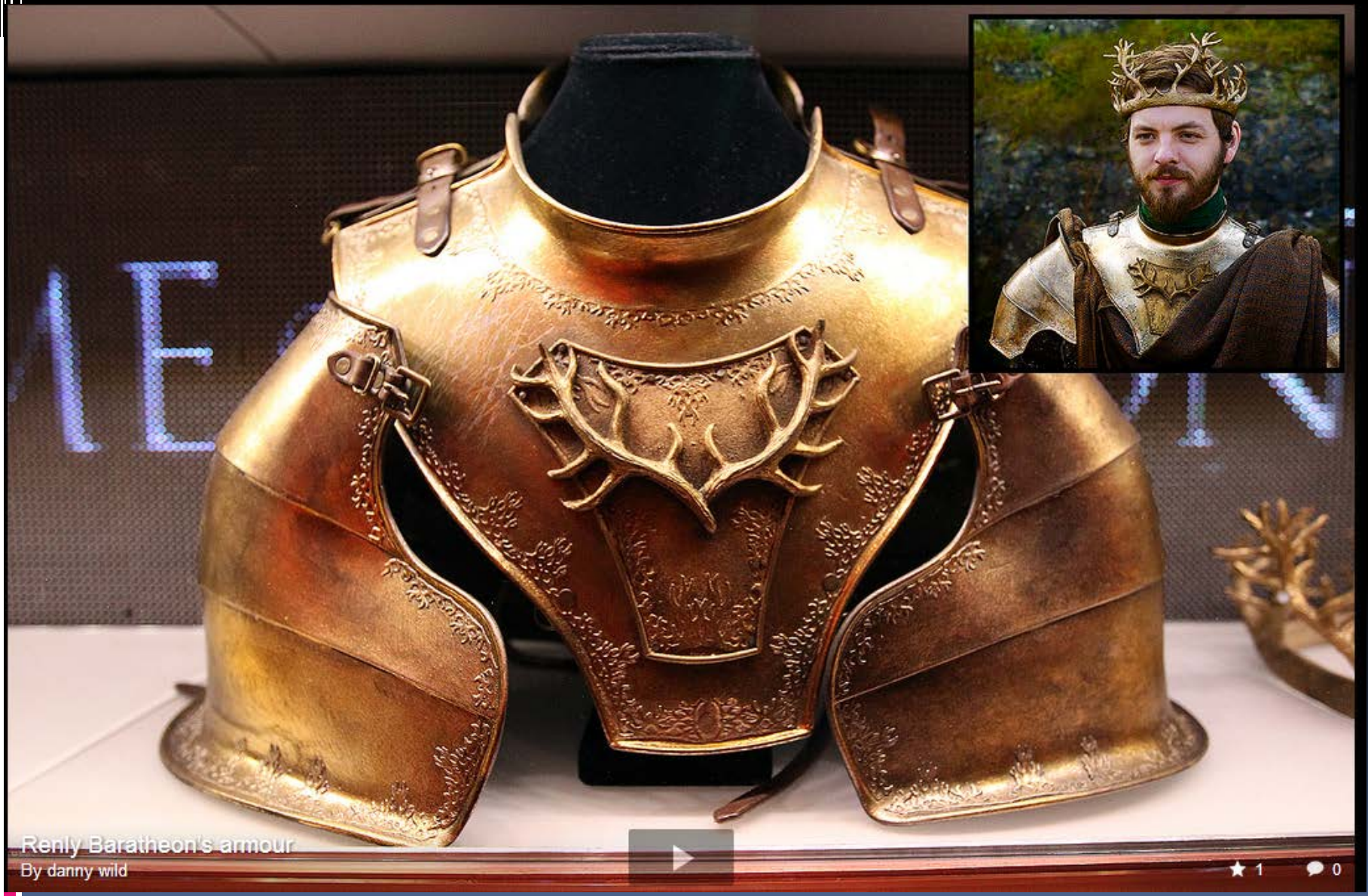
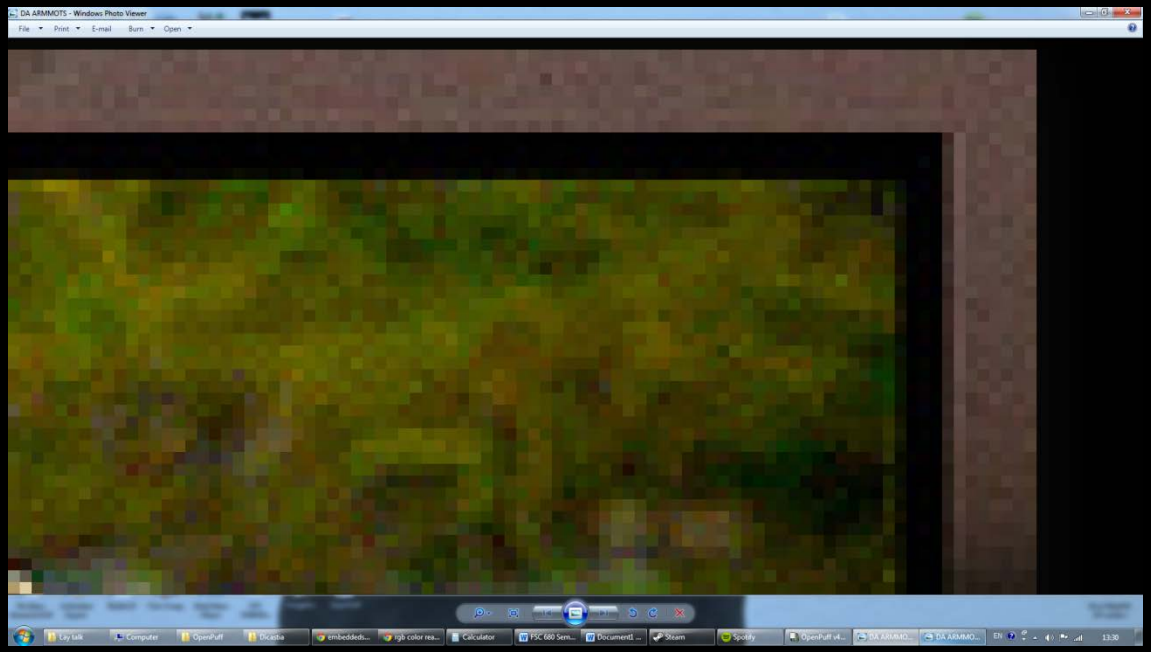


Image after Steganography

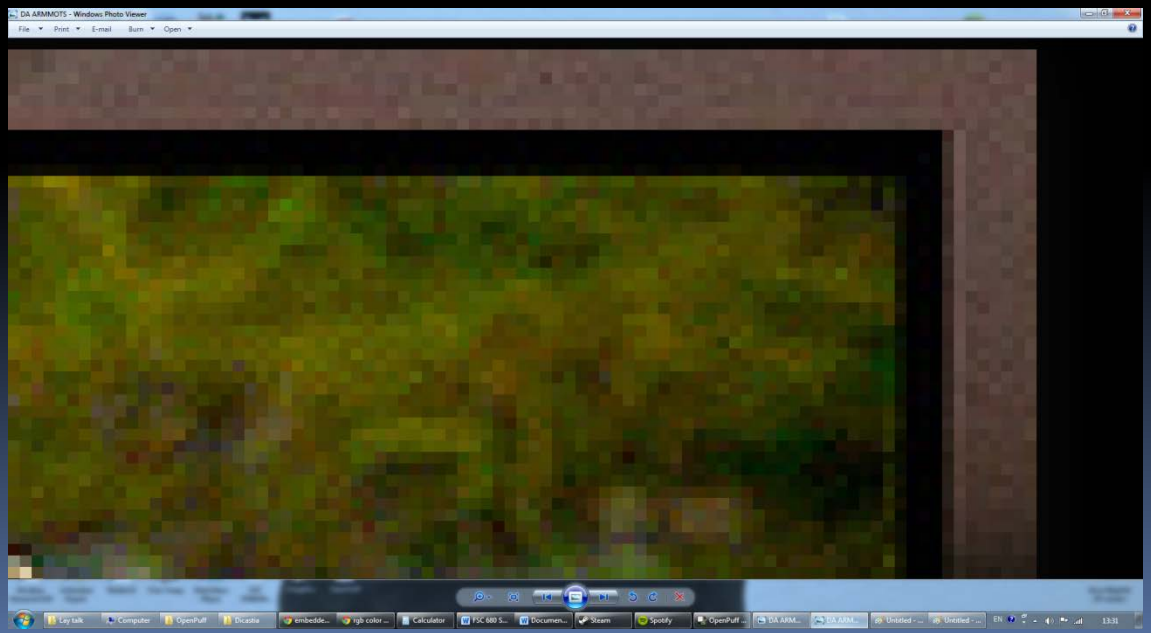


Close Up of the Picture

- Original



- Encrypted



Close Up of the Picture

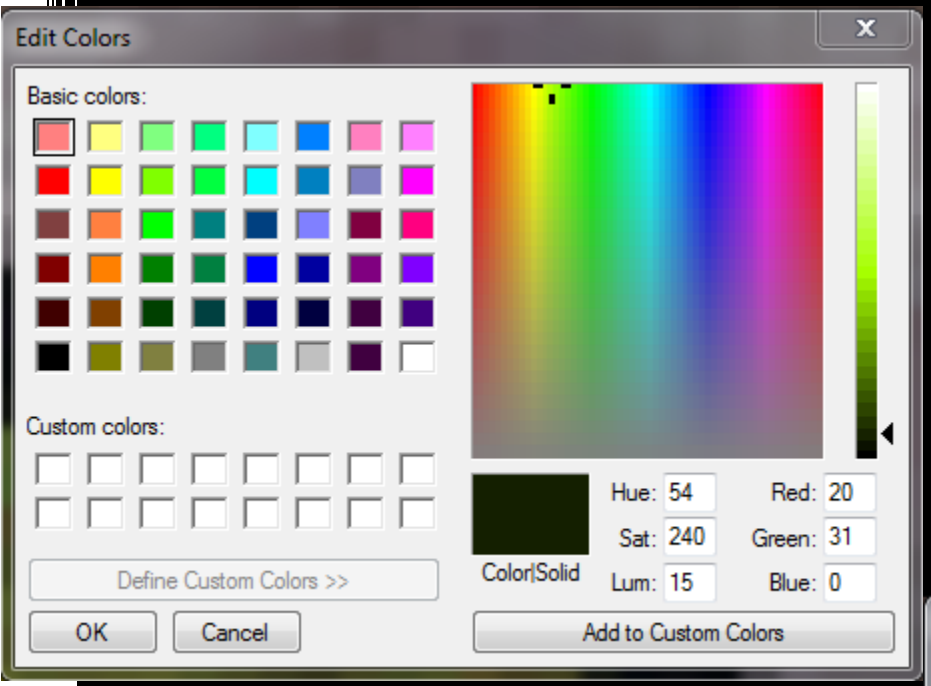
- Original

- Encrypted

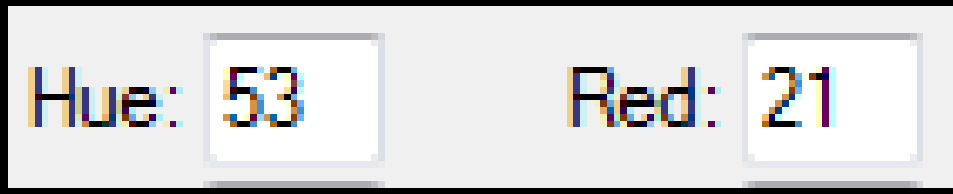
Pretty Much look the same…

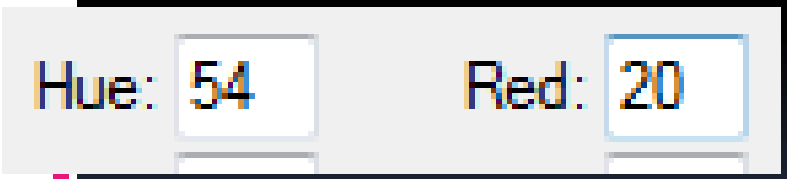
- Even on a pixel level the pictures look almost identical and there seems to be no difference

If You Look at the color Composition

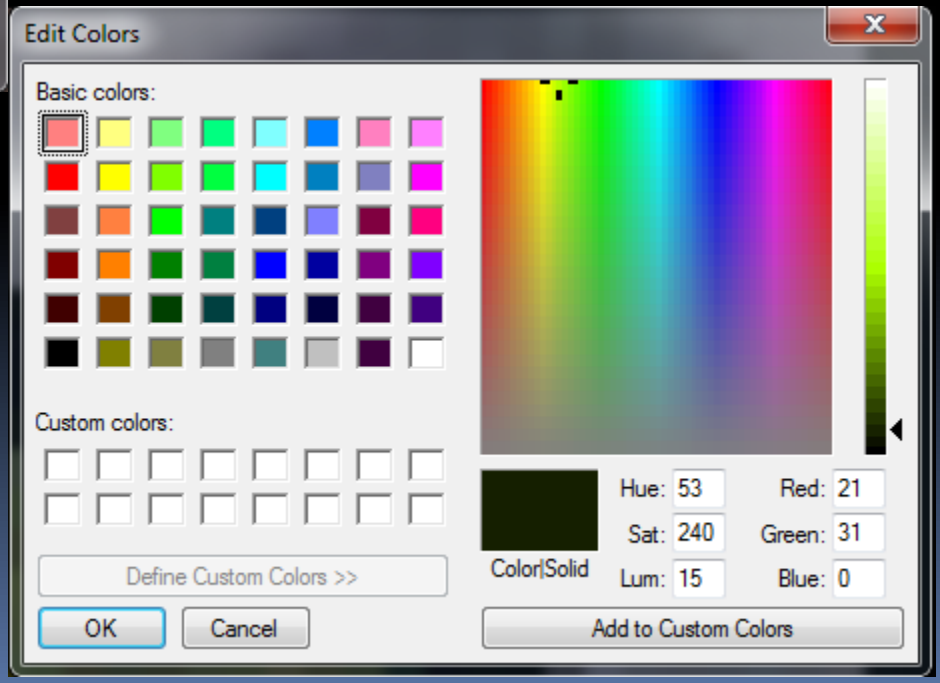


Encrypted ↓





↑ Original



There is a Difference!

- When hiding and image in an image a single number change on the color accounts for about 4 bytes of data so each pixel is changed by two numbers equaling 8 bytes per pixel.

- This is why the images are hard to tell apart because the differences are so minimal.

Linguistic Steganography Summary

- Linguistic Steganography focuses primarily on targeting specific groups
- A majority of its applications are using methods that would only be discernable by people that are "in the loop"
- Due to this element it is not commonly detected and can be very difficult to separate from common day to day interactions.

Future Directions

- Quantum Cryptography is being worked on by the NSA and they are currently in the process of developing a quantum computer based around it.
- If completed it would be exponentially faster than any computer in existence and able to break through any currently known ciphers.
- As the mediums of social media expand as do the possible targets for Steganography.

Acknowledgements

- Dr. Fenger
- Dr. Staton
- Alyssa
- AJ
- Julia
- Docoda

References

- Cheddad, J. Condell, K. Curran and P. McKevitt, "Digital Image Steganography: Survey and Analyses of Current Methods". Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.
- Bennett, Charles H., and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing." International Conference on COmputers, Systems & Signal Processisng (1984): 1-6.
- Collins, Daniel, Nicolas Gisin, and Hugues De Riedmatten *. "Quantum Relays for Long Distance Quantum Cryptography." Journal of Modern Optics 52.5 (2005): 735-53.
- Denning, Dorothy Elizabeth Robling. Cryptography and Data Security. Reading, MA: Addison-Wesley, 1983.
- Filiol, Eric. "Anti-Forensic Techniques Based on Malicious Cryptography." Proceedings of the 9th European Conference on Information Warfare and Security 9 (2010): 63-72.
- Garfinkel, Simson, Paul Farrell, Vassil Roussev, and George Dinolt. "Bringing Science to Digital Forensics with Standardized Forensic Corpora." Digital Investigation 6 (2009): S2-S11.

References

- Kessler, Gary C. "An Overview of Steganography for the Computer Forensics Examiner." Forensic Science Communications 6.3 (2004): 1-15.
- Menezes, A. J., Van Oorschot Paul C., and Scott A. Vanstone. Handbook of Applied Cryptography. 1st ed. Boca Raton: CRC, 1997.
- Pevny, T., and J. Fridrich. "Detection of Double-Compression in JPEG Images for Applications in Steganography." IEEE Transactions on Information Forensics and Security 3.2 (2008): 247-58.
- Provos, N., and P. Honeyman. "Hide and Seek: An Introduction to Steganography." IEEE Security & Privacy Magazine 1.3 (2003): 32-44.
- Sen, A. K., Susmita Dutta, and Sanjay Davadgaonkar. "Echo Hiding Approach in Video Forensic." INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING 1.1 (2013): 6-9.
- Singh, Nanhay, Bhoopesh Singh-Bhati, and R. S. Raw. "Digital Image Steganalysis for Computer Forensic Investigation." Computer Science and Information Technology (2012): 161-68.
- Wen, Che-Yen, and Kun-Ta Yang. "Image Authentication for Digital Image Evidence." Forensic Science Journal 5.1 (2006): 1-11.

Questions?