Steganography: An Enticing Exploration

Nisha Mannukkunnel BalanPillai

Abstract— **Steganography dates back to ancient Greece and had been in use for at least 2500 years by now. It has been widely used for military, diplomatic, personal and intellectual property applications. However, advanced techniques are often overlooked. Briefly stated, steganography is the art of hiding information within every day, innocuous objects and concealing the fact that communication is taking place.**

***Index Terms*— Cryptography, Security, Steganalysis Steganography.**

I. INTRODUCTION

Steganography (from Greek steganos and graphie) is the science of concealing the presence of data even when it is being sought.[2] Cryptography might hide the essence of the message, but this has proven to be inadequate for many applications. Steganography employs various technologies like digital signal processing, cryptography, information theory, data compression, math, and human audio/visual perception etc. The goal often is a tradeoff between the security and the amount of data that can be hidden as, the chances of third parties finding out that there is a hidden communication going on increase with the increase in the amount of hidden data. Steganographic robustness is another target, that watermarking is not concerned with. The hidden data must withstand image/audio manipulations such as contrast, brightness, cropping, stretching, analog-to-digital-to-analog conversion, etc. There is a large commercial interest in watermarking for digital rights management. Author of [2] argues that there are three levels of failure for steganography: 1) detection, 2) extraction, and 3) destruction. Even if somebody detects the data, extraction and destruction of the data must be difficult. A third party can insert random data once the algorithm is known. He rates the perceptibility in 3 levels: 1) Indistinguishable, 2) can see/hear distortion when looking/listening closely for it, 3) blatantly obvious to a casual observer. [2]

II. HISTORY

Steganography has been used for ages and they date back to ancient Greece. Ancient methods relied on physical steganography where the carriers were simple covers like wax tablets with inscriptions in the underlying wood. Other methods are microdot technology which employed tiny dots drawing hardly any attention, the use of invisible inks like lemon juice, milk etc. that turn dark when heated, and the messages written on silk balls that the ancient Chinese messengers swallowed.

Manuscript received November 12, 2013.

Nisha M B, Masters in Comp science from Manipal Institute of Technology where her research elective was Security. She Worked on Virtualization for 7+ years with 4+ years exclusively on security features of various Virtualization technologies.

III. USES

1. Confidential communication where it protects not only the data but also the parties involved
2. Secret data storage. Sensitive and private information can be stored safely in a location.
3. Implementation of watermarking.
4. e- commerce transaction verification.
5. Communication concerning national security
6. The transportation of sensitive data past eavesdroppers.

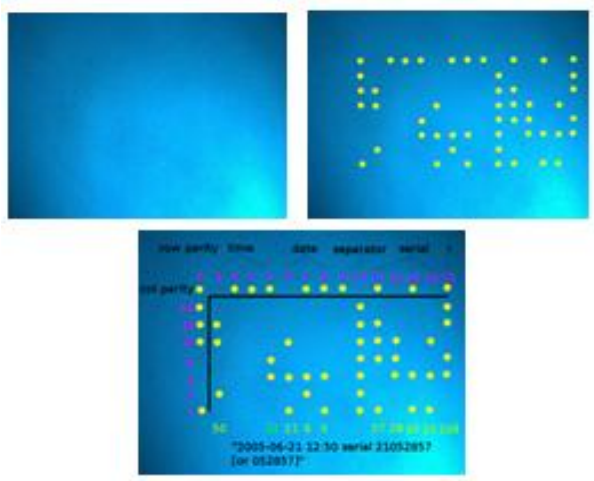

Fig. 1. Eric Hernandez [12]

IV. STEGANOGRAPHY AND CRYPTOGRAPHY

Cryptography scrambles messages and transforms it into a new file through an algorithm where steganography hides a file within another object. With cryptography, anybody can see that there is an encrypted message. Advances in steganography are always countered by advances in steganalysis which defeats steganographic techniques. Existing methods of hiding information can be significantly improved by combining encryption and steganography, as a solution. A basic method of combining the two is to encrypt the message before attempting to hide it. The main advantage is that the detection of message alone does not defeat the system.

V. STEGANOGRAPHIC TECHNIQUES

A. Least Significant Bit (LSB)

It is a simple technique which modifies only the least significant portions of the image. The Most Significant Bit (MSB) of the hidden image that contributes ½ the information is inserted into the Least Significant Bit (LSB) of the cover

image that contributes 1/256th of the information. This difference is not perceivable to unsuspecting human eyes.

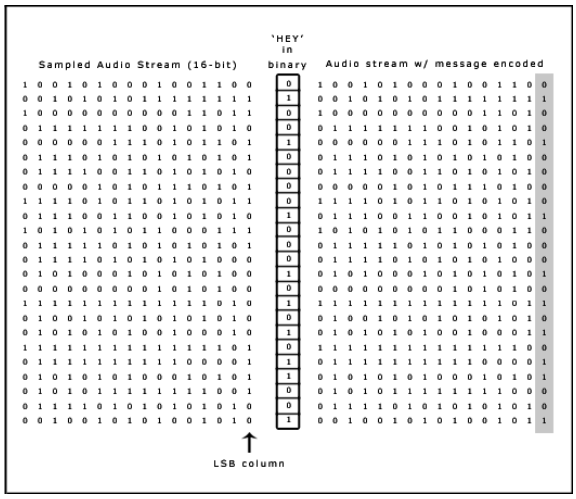

Fig. 2. Eric Hernandez [12]

B. *Bit Plane Complexity Segmentation (BPCS)*

BPCS is similar to LSB, but calculates the complexity of regions within an image and replaces those regions with complexity above a certain value with new data. It can be used for 24-bit true colour or 8-bit gryscale images but not on paletted images.

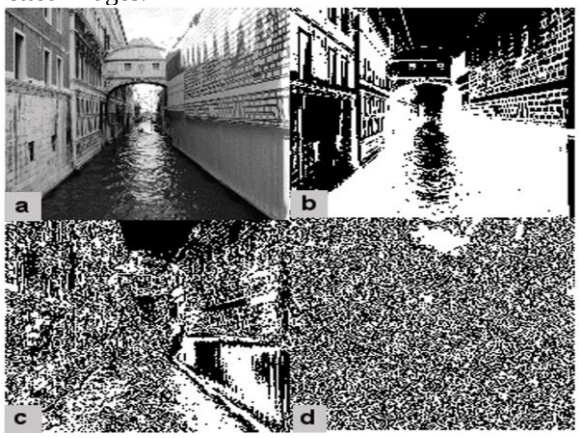

Fig. 3. Daniel Stoleru [10]

C. *Direct Cosine Transformation*

DCT based image compression relies on quantization of the image's DCT coefficient and their entropy coding. Even though vulnerable to noise, it distributes data more evenly and in a more robust way compared to the LSB method.

D. *Wavelet Transformation*

Wavelet transformations are better at high compression levels. In this method, the coefficients of the wavelets are altered with the noise within tolerable levels. It has a promising future in research.

E. *Spread Spectrum*

Spread spectrum systems encode data as a binary sequence which sounds like noise but which can be recognized by a receiver with the correct key. The technique has been used by the military since the 1940s because the signals are hard to jam or intercept as they are lost in the background noise. Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium.

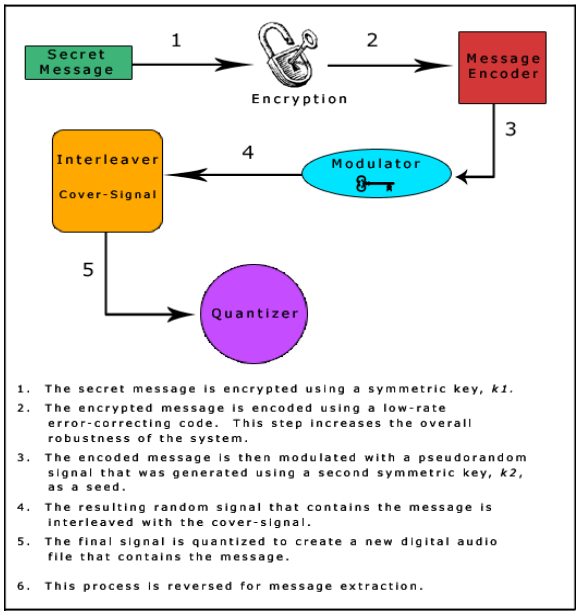

Fig. 4. Eric Hernandez [12]

VI. LIMITATIONS

The usefulness of steganography ends at the point where the recipient and non-recipient possess the same knowledge level of the information. The intended recipient might miss the information unless there is a 'shared secret' [11]. There arises the need for another secretive information exchange which complicates things.

Steganography excessively depends on the medium that is used to hide the message. This excessive dependence restricts room for improvement.

Comparison of original image and the stego-image can be fatal. Therefore original image must be destroyed prior to communication.

Beginning of a new exchange can be suspicious. Similarly the pattern of images sent should not create doubts to third parties. The exchange must look as genuine as possible.

VII. DETECTION

The need to detect steganographic data arises when terrorists and pedophiles use it as a medium for illegal activities. The main problem steganalysis faces is the sheer volume of data to be analysed. Recognizing stego images online and in spam mail does not seem like a finite task. The dynamic nature of internet is another hurdle. Images and data appear and disappear in seconds. The vast variety of hiding techniques make detection difficult, too.

VIII. SOME KNOWN USAGES

Steganography is a continually advancing field, and researchers are always coming up with ways to improve steganography, steganalysis, and watermarking.

Steganography is used by some color laser printer manufacturers to identify counterfeiters. It contains the encoded printer serial numbers, date and time stamps

In 2001 , daily newspaper in USA reported "Terror groups hide behind Web encryption". In October 2001, the New York Times published an article claiming that terrorists had used steganography to encode messages into images, and then transported these via e-mail and possibly via USENET to prepare and execute the September 11, 2001 terrorist attack.

IX. PRESENT RESEARCH & FUTURE

Pascal Schöttle and Rainer Böhme proposed an approach of combining game theory with content-adaptive steganographic security in 14th Information Hiding Conference, 2012 held in California. They defined a new kind of adaptive embedding, the so-called strategic adaptive steganography, which takes into account the knowledge of the attacker by being able to recover (or estimate) the adaptivity criterion. As per them a rigorous understanding of content-adaptive steganography in theory and practice remains a relevant target for future investigations.

Dola Saha, Aveek Dutta, Dirk Grunwald and Douglas Sicker proposed another approach called Dirty Constellation to implement high capacity,covert channel by encoding covert information in the physical layer of common wireless communication protocols, in IH conference 2012. This can ensure high degree of undetectability.

In the future, digital camera manufacturers could implement steganographic features as a part of camera firmware to annotate pictures with the photographer's copyright information. Camcorder manufacturers could also follow suit and implement steganography and watermarking techniques for protecting video content captured on camcorders and video cameras. Going forward, legitimate applications such as tagging of multimedia content with hidden information could become an important application area for steganography.

X. CONCLUSION

The field needs more research in order to develop undetectable techniques. Steganography has increased appeal in areas where encryption is outlawed. With the advances in Steganalysis, Steganography will have to develop more sophisticated techniques.

Digital watermarking is a potential future application. It can track the owners of copyrighted work and prevent illegal distribution.

The future of research in steganography may be limited by the law as there are reports claiming that steganography is employed by terrorists. Developing new applications for steganography becomes important at this point. Future developments will include the applications to media other than images.

Future research will include the application to vessels other than 24-bit images. The advantages and disadvantages of existing methods have to be studied extensively in order to develop more sophisticated approaches.

Encryption and steganography combined sensibly can be a powerful data hiding method. Efforts should be made for the techniques to survive image manipulation techniques and attacks. Also the selection of covers and the degradation of quality resulting from the steganographic technique of the vessel requires careful consideration.

Theft and false representation are just some of the issues that need to be resolved.

REFERENCES

[1] Counterintelligence News and Developments, Volume 2, June 1998 “Hidden in Plain Sight-Steganography” URL: www.nacic.gov/pubs/news/1998/jun98.htm

[2] An Introduction to More Advanced Steganography

[3] International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[4] Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned

[5] A Survey of Data Mining Techniques for Steganalysis: Farid Ghareh Mohammadi and Mohammad Saniee Abadeh Faculty of Electrical and Computer Engineering, Tarbiat Modares University Iran

[6] Steganography in Different Colour Models Using an Energy Adjustment Applying Wavelets: Blanca E. Carvajal-Gámez, Francisco J. Gallegos-Funes, Alberto J. Rosales-Silva and Rene Santiago-Cruz National Polytechnic Institute, Higher School of Mechanical and Electrical Engineering, Edif. Z-4, 3er. Piso, ESIME SEPI-Electrónica, Col. Lindavista, México DF., México

[7] RABS: Rule-Based Adaptive Batch Steganography: Hedieh Sajedi Tehran University, Tarbiat Modares University, Iran

[8] Contemporary Approaches to the Histogram Modification Based Data Hiding Techniques: Yildiray Yalman1, Feyzi Akar2 and Ismail Erturk1 1Turgut Ozal University, 2Turkish Naval Academy, Turkey

[9] Lossless Steganography for Speech Communications: Naofumi Aoki Graduate School of Information Science and Technology, Hokkaido University, Japan

[10] Visual Cryptography and Bit-Plane Complexity Segmentation: Daniel Stoleru

[11] Current State of Steganography: Sophie Engle

[12] Survey of steganography: With an emphasis on audio techniques by Eric Hernandez

[13] Secret Agent Radio : Covert communication through dirty constellations : Dola Saha, Aveek Dutta, Dirk Grunwald and Douglas Sicker, IH conferene 2012

[14] A Game-Theoretic Approach to Content-Adaptive Steganography : Pascal Schöttle and Rainer Böhme, IH Conference 2012

[15] "Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and When You Made Your Print", Electronic Frontier Foundation.

Nisha M B., VMware Inc
Nisha did Masters in Comp science from Manipal Institute of Technology where her research elective was Security. She Worked on Virtualization for 7+ years with 4+ years exclusively on security features of various Virtualization technologies.