MAT JOURNALS

Journal of Android and IOS Applications and Testing
Volume 1 Issue 2

Review on Steganography-An Art of Hiding Data

Ashwini S. Jadhav

Department of CSE, Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra, India

E-mail: ashwinijadhav1410@gmail.com

Abstract

Steganography is that the art of coated or hidden writing. The aim of steganography is covert communication-to hide the existence of a message from a third party. This paper is meant as a high-level technical introduction to steganography for those unacquainted the sector. It is directed at rhetorical laptop examiners WHO would like a sensible understanding of steganography while not delving into the arithmetic, though references square measure provided to a number of the continuing analysis for the one who wants or desires further detail. Though this paper, provides a historical context for steganography, the stress is on digital applications, that specialize in activity info in on-line image or audio files. Samples of code tools that use steganography to cover knowledge inside alternative files similarly as code to notice such hidden files will be bestowed.

Keywords: *Steganography, cryptography, communication, audio, video, images*

INTRODUCTION

In today's world, the communication is that the basic necessity of each growing space. Everybody needs the secrecy and safety of their human action knowledge. In our way of life, we tend to use several secure pathways like net or phone for transferring and sharing info, however, it is not safe at a precise level. So, as to share the knowledge during a hid manner two techniques can be used. These mechanisms square measure cryptography and steganography. In cryptography, the message is changed in associate degree encrypted type with the assistance of encoding key that is thought to sender and receiver solely. The message cannot be accessed by anyone while not victimisation the encoding key. However, the transmission of encrypted message might simply arouse attacker's suspicion, and also the encrypted message might, therefore, be intercepted, attacked or decrypted violently. So, as to beat the

shortcomings of science techniques, steganography techniques are developed. Steganography is that the art and science of human action in such some way that it hides the existence of the communication. Thus, steganography hides the existence of knowledge in order that nobody will find its presence. In steganography the method of concealing info content within any multimedia system content like image, audio, video is referred as associate degree "Embedding".

Steganography may be a Greek word which implies hid writing. The word "steganos" suggests that "covered" and "graphical" suggests that "writing". Thus, steganography is not solely the art of concealing information, however, additionally concealing the actual fact of transmission of secret information. Steganography hides the key information in another come in such some way that solely the recipient is aware of the existence of message. In ancient time, the information was protected by concealing it on the rear of wax, writing tables, and abdomen of rabbits or on the scalp of the slaves. However, today's most of the folks transmit the information within the type of text, images, video, and audio over the medium. So, as to soundly transmission of confidential information, the multimedia system object like audio, video, pictures square measure used as a canopy sources to cover the information.

TYPES OF STEGANOGRAPHY

Text Steganography

It consists of concealment info within the text files. During this technique, the key knowledge is hidden behind each ordinal letter of each words of text message. Numbers of ways square measure out there for concealment knowledge in computer file. These methods are: i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

Image Steganography

Hiding the info by taking the duvet object as image is referred as image steganography. In image steganography constituent intensities area unit would not to hide the info. In digital steganography, pictures area unit wide used cowl supply as a result of their area unit range of bits presents in digital illustration of a picture. The foremost wide used technique these days is activity of secret messages into a digital image. This steganography technique exploits the weakness of the human sensory system (HVS). HVS cannot find the variation in luminosity of color vectors at higher frequency facet of the visual spectrum. An image is often

diagrammatic by a set of color pixels. The individual pixels are often diagrammatic by their optical characteristics like 'brightness', 'chroma' etc. Every of those characteristics are often digitally expressed in terms of 1s and 0s. For example: a 24-bit ikon can have eight bits, representing every of the three-color values (red, green, and blue) at every constituent. If we tend to take into account simply the blue there will be two eight completely different values of blue. The distinction between 11111111 and 11111110 within the price for blue intensity is probably going to be undetectable by the human eye. Hence, if the terminal recipient of data is nothing, however, human sensory system (HVS) then the smallest amount important Bit (LSB) may be used for one thing else then again color information. This method may be directly applied on digital image in icon format yet as for the compressed image format like JPEG. In JPEG format, every element of the image is digitally coded victimisation distinct cos transformation (DCT). The LSB of encoded DCT parts may be used because the carriers of the hidden message. The main points of higher than techniques square measure explained below: Modification of LSB of a canopy image in 'bitmap' format [1]. During this methodology binary equivalent of the message (to be hidden) is distributed among the LSBs of every element. An example as an instance we are going to attempt to hide the character 'A' into an 8-bit color image. We tend to square measure taking eight consecutive pixels from prime left corner of the image. The equivalent binary bit pattern of those pixels may be like this: - 00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111. The only drawback with this system is that it is terribly susceptible to attacks like compression and data format. Apply of LSB technique throughout distinct circular function transformation (DCT) on cowl image. The subsequent steps square measure followed during this case: 1. The Image is broken into knowledge units every of them consist of eight x eight block of pixels. 2. Performing from top-left to bottom-right of the duvet image, DCT is applied to every picture element of every knowledge unit. 3. Once applying DCT, one DCT constant is generated for every picture element in knowledge unit. 4. Every DCT constant is then quantal against a reference quantisation table. 5. The LSB of binary equivalent the quantal DCT constant may be replaced by a small amount from secret message. 6. Coding is then applied to every changed quantal DCT constant to provide compressed Stego Image. Hand aspect image is that the

original cowl image, whereas hand aspect will embedding a computer file into the duvet image create the stego image [2].

Audio Steganography

It involves activity knowledge in audio files. This methodology hides the information in WAV, AU and MP3 sound files. There square measure totally different ways of audio steganography. These methods are:

Low Bit Encoding

Sampling technique followed by division converts analog audio signal to digital binary sequence. During this technique, LSB of binary sequence of every sample of digitized audio file is replaced with binary equivalent of secret message. An example if we wish to cover the letter 'A' (binary equivalent 01100101) to an digitized audio file, wherever, every sample is drawn with 16 bits, then LSB of 8 consecutive samples (each of 16 bit size) is replaced with every little bit of binary equivalent of the letter 'A'.

Phase Coding

Human Auditory System (HAS) cannot acknowledge the state change in audio signal as straightforward it can acknowledge noise within the signal. The part secret writing technique exploits this truth. This method encodes the key message bits as part shifts within the part spectrum of a digital signal, achieving a supersonic encryption in terms of signal-to- noise magnitude relation [3].

Spread Spectrum

There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct-sequence spread spectrum (DSSS) is a modulation technique used in telecommunication. Like different unfold spectrum technologies, the transmitted signal takes up a lot of information measure than the data signal that is being modulated. Direct-sequence spread-spectrum transmissions multiply the information being transmitted by a "noise" signal. This noise signal may be a pseudorandom sequence of one and 1 values, at a frequency a lot of on top of that of the first signal, thereby, spreading the energy of the first signal into a far wider band. The ensuing signal resembles dissonance. However, this noise-like signal is wont to precisely reconstruct the first information at the receiving finish, by multiplying it by a similar pseudorandom sequence (because $1 \times 1 = 1$, and $-1 \times -1 = 1$). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted

Pseudorandom Noise (PN) sequence with the receiver's assumed sequence. For de-spreading to figure properly, transmit and receive sequences should be synchronised. This needs the receiver to synchronize its sequence with the transmitter's sequence via some form of temporal arrangement search method. In distinction, frequency-hopping unfold spectrum pseudo-randomly retunes the carrier, rather than adding pseudo-random noise to the info, which ends during a uniform distribution whose breadth is set by the output vary of the pseudo-random range generator.

Video Steganography

It is a way of concealment any reasonably files or information into digital video format. During this case video (combination of pictures) is employed as carrier for concealment the information. Typically, separate trigonometric function remodel (DCT) alter the values (e.g., 8.667 to 9) that is employed to cover the information in every of the pictures within the video, that is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats employed by video steganography. Video files are typically consists of pictures and sounds, therefore, most of the relevant techniques for concealment information into pictures and audio also are applicable to video media. Within the case of Video steganography sender sends the key message to the recipient employing a video sequence as cowl media. Facultative secret key 'K' may be used throughout embedding the key message to the duvet media to provide 'stego-video'. At the moment the stego-video is communicated over public channel to the receiver. At the receiving finish, receiver uses the key key in conjunction with the extracting algorithmic rule to extract the key message from the stego-object. The original cover video consists of frames represented by Ck (m, n) where $1 \leq k \leq N$. 'N' is the total number of frame and m, n are the row and column indices of the pixels, respectively. The binary secret message denoted by Mk (m, n) is embedded into the cover video media by modulating it into a signal. Mk(m, n) is defined over the same domain as the host Ck(m, n).The stego-video signal is represented by the equation $Sk(m, n) = Ck(m, n)+\alpha k (m, n) Mk(m, n)$, $k = 1, 2, 3 \ldots N$ where $\alpha k (m, n)$ is a scaling factor. For simplicity $\alpha k (m, n)$ can be considered to be constant over all the pixels and frames. So the equation becomes: $Sk(m, n) = Ck(m, n)+\alpha (m, n) Mk(m, n)$, $k = 1, 2, 3 \ldots N$.

Network or Protocol Steganography

It involves activity the data by taking the

network protocol similar to communications protocol, UDP, ICMP, IP etc., as cowl object. Within the OSI layer network model there exist covert channels wherever steganography will be used. This can be another approach of steganography that employs activity knowledge within the network datagram level during a TCP/IP primarily based network like web. Network Covert Channel is that the equivalent word of network steganography. Overall goal of this approach to create the stego datagram is undetectable by Network watchers like somebody, Intrusion Detection System (IDS) etc. During this approach data to be hide is placed within the informatics header of a TCP/IP datagram. A number of the fields of informatics header associated communications protocol header in an IPv4 network are chosen for knowledge activity. Initial we will demonstrate, however, 'Flags' and 'Identification' field of Ipv4 header will be exploited by this system.

CONCLUSION

As steganography becomes a lot of wide employed in computing, there are problems that require being resolved. There are a large form of totally different techniques with their own benefits and drawbacks. Several presently used techniques do not seem to be strong enough to stop detection and removal of embedded knowledge. The utilization of benchmarking to guage techniques ought to become a lot of common and a lot of commonplace definition of hardiness is needed to assist overcome this. For a system to be thought-about strong it ought to have the subsequent properties: a) the standard of the media should not perceptibly degrade upon addition of a secret knowledge. b) Secret knowledge ought to be undetectable while not secret data, usually the key. c) If multiple knowledge is gift they ought to not interfere with one another. d) The key knowledge ought to survive attacks that do not degrade the perceived quality of the work. This work presents a theme that may transmit giant quantities of secret info and supply secure communication between two communication parties. Each steganography and cryptography may be plain-woven into this theme to form the detection additional difficult. Any quite text information may be utilized as secret monosodium glutamate. The key message using the conception of steganography is shipped over the network. In addition, the planned procedure is straightforward and straightforward to implement. Also, the developed system has several sensible, personal and military applications for each

point-to-point and point-to multi-point communications.

REFERENCES

1. Available at: http://www.garykessler.net/library/steganography.html.
2. Available at: http://www.ermt.net/docs/papers/Volume_3/5_May2014/V3N5-190.pdf.
3. Available at: Wikipedia.