International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Review on Various Approaches for Image Steganography

Urvashi[1], Amninder Kaur[2]

[1]Research Scholar, PURICTIM Punjab, India

[2]Assistant Professor, PURICTIM Punjab, India

Abstract: ***Steganography is art of hiding the fact that communication is taking place, by hiding information in other information. Digital images are the most popular file formats that are used because of their high frequency on the internet. Many stenographic and encryption techniques are used to hide information of images. Some of the techniques are better than other, some have advantages and disadvantages. In this paper, we will discuss the review on steganography, its techniques and the encryption algorithms.***

Keywords: LSB, ISB, MLSB, AES, Blow Fish Stegnalysis and steganography

1. Introduction

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images.

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

Two technologies that are close to steganography is watermarking and fingerprinting. Watermarking is typically used to identify ownership of the copyright of signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright and for banknote authentication. Like traditional watermark, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

Fingerprint functions may be seen as high-performance hash functions used to uniquely identify substantial blocks of data where cryptographic hash function may be unnecessary. Audio fingerprints algorithms should not be confused with this type of fingerprint function.

1.1 Types of steganography

All the digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

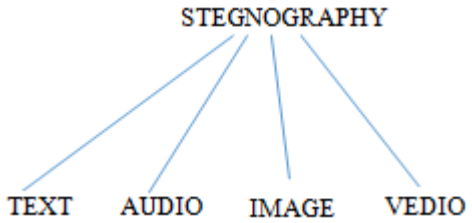

Figure 1: Types of Steganography

1. Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textualelements (e.g., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader. These criteria, reliable decoding and minimumvisible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques. Thedocument format file is a computer file describing the document content and page layout (or formatting), using standard format description languages such as PostScript2, TeX, @off, etc. It is from this format file that the image - what the reader sees - is generated.

- **Line-Shift Coding**
  This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely. This encoding may be applied either to the format file or to the bitmap of a page image.
- **Word-Shift Coding**
  This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely. This encoding can be applied to either the format file or to the bitmap of a page image. Decoding may be performed from the format file or bitmap.
- **Feature Coding**
  This is a coding method that is applied either to a format file or to a bitmap image of a document. The image is examined for chosen text features, and those features are altered, or not altered, depending on the codeword.

Image Steganography

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganography expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited.

- **Least Significant Bits**
  A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence.
- **Masking and filtering**
  Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image.
- **Transformations**
  A more complex way of hiding a secret inside an image comes with the use and modifications of discrete cosine transformations.

Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. We are going to have a brief introduction on some of them.

- **LSB Coding**
  Sampling technique followed by Quantization converts analog audio signal to digital binary sequence. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.
- **Phase Coding**
  Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio.
- **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. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated.

Video Steganography

Although BMP files are perfect for steganography use, they are able to carry only small files. So there is a problem, how to get much enough files to hide our message, and what to do to read them in a correct order? Good way out is to hide information in a video file, because as we know, AVI files are created out of bitmaps, combined into one piece, which are played in correct order and with appropriate time gap. Keeping that in mind all we have to do is to get out is file single frames and save them as BMP files. If we'll use algorithm for hiding data in digital pictures, we can hide our message in bitmap obtained in this way, and then save it into new AVI file.

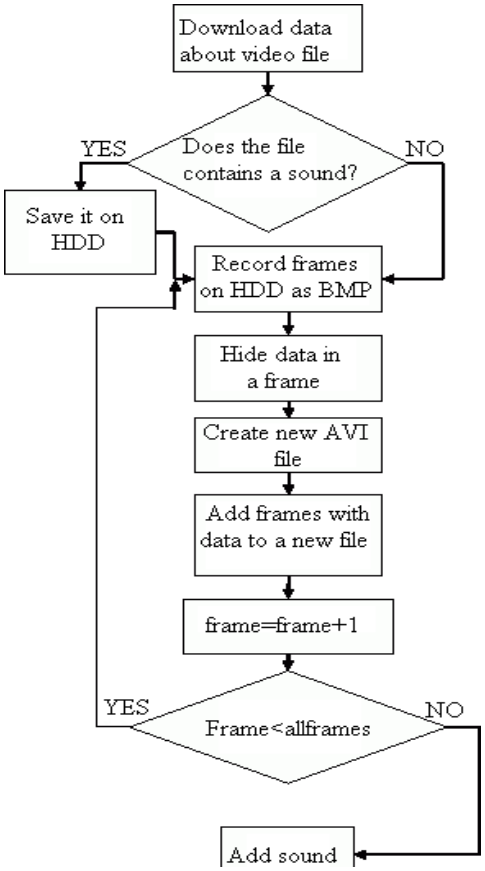

Figure 2: AES Encryption algorithm

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

As a cipher, AES has proven reliable. The only successful attacks against it have been side-channel attacks on weaknesses found in the implementation or key management of certain AES-based encryption products. The BEAST browser exploit against the TLS v1.0 protocol is a good example; TLS can use AES to encrypt data, but due to the information that TLS exposes, attackers managed to predict the initialization vector block used at the start of the encryption process.

2. Techniques used in steganography

2.1 Blowfish encryption algorithm

The data transformation processes for Pocket Brief uses the Blowfish Algorithm for Encryption and Decryption, respectively. The details and working of the algorithm are given below.

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses.

Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16times. The block size is 64 bits, and the key can be any length up to 448 bits. Althoughthere is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encrypt. It issignificantly faster than most encryption algorithms when implemented on 32-bitmicroprocessors with large data caches.

The Blowfish Algorithm:

- Manipulates data in large blocks
- Has a 64-bit block size.
- Has a scalable key, from 32 bits to at least 256 bits.

Uses simple operations that are efficient on microprocessors e.g, exclusive-or, addition, table lookup, modular-multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps. Employs pre-computable sub keys. On large-memory systems, these sub keys can be pre-computed for faster operation. Not pre-computing the sub keys will result in slower operation, but it should still be possible to encrypt data without any pre-computations. Consists of a variable number of iterations. For applications with a small key size, the trade-off between the complexity of brute-force attack and a differential attack make a large number of iterations Superfluous. Hence, it should be possible to reduce the number of iterations with no loss of security (beyond that of the reduced key size). Uses sub keys that are a one-way hash of the key. This allows the use of long passphrases for the key without compromising security. Have no linear structures that reduce the complexity of exhaustive search.. Uses a design that is simple to understand. This facilitates analysis and increase. The confidence in the algorithm. In practice, this means that the algorithm will beefiest iterated block cipher.

2.2 Two fish encryption algorithm

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.

Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, thepseudo-Hadamard transform (PHT) from the

SAFER family of ciphers. Two fish has a Feistel structure like DES.

On most software platforms Twofish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but it is somewhat faster for 256-bit keys.

Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson; the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, Tadayoshi Kohno, and Mike Stay.

The Twofish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the two fish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the OpenPGP standard (RFC 4880). However, two fish has seen less widespread usage than Blowfish, which has been used longer.

3. Related Work

T. Morkel, M.S. Olivier gave an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganography techniques are more suitable for which applications. Although "Steganographia" is the work that we derive the term steganography from, it is certainly not the first example of hidden writing. Currently, the emphasis has been on various forms of digital steganography. Commonly there are a number of digital technologies that the community is concerned with, namely text files, still images, movie images, and audio. It is beyond the scope of this paper to go into the details of steganography methods; suffice it to say that there are two primary groups. "Image Domain tools encompass bit-wise methods that apply least significant bit (LSB) insertion and noise manipulation.

Mehdi Hussain explained that Steganography is going to gain its importance due to the exponential growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image (used as the carrier to embed message into) and generate a stego-image (generated image which is carrying a hidden message). In this paper we have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification, applications.

Ravali.S.V.Kexplained that the basic idea behind the paper is to provide a good, efficient for hiding the data from hackers and transmits to the receiver in a safer manner. In this proposed system mainly based on audio Steganography and cryptography to ensure secure data transfer from transmitter to receiver. Blowfish algorithm is used, which is most powerful technique to encrypt and decrypt the data file. Blowfish algorithm is efficient algorithm among other cryptographic techniques such as RSA, DES, Triple DES and other encrypting algorithms. The Cryptography, Spread Spectrum, Steganography, Stego Object. Main benefits of Spread spectrum system are robust against interference and inherent security. A simple compression algorithm is used to suitable for any size and CRC algorithm is to check the integrity of the data file.

Hemlata Sharma presents a scenario, any communication of internet and networks application requires security. Lots of data security and data hiding algorithms have been developed in the last decade. Cryptography and steganography are the two major techniques for secret communication. In this paper, the secret image is first encrypted by using BLOWFISH algorithm which has very good performance and is a most powerful technique compared to other Algorithms. Now this encrypted image is embedded with video by using LSB Approach of steganography. Our proposed model gives two layers of security for secret data, which fully satisfy the basic key factors of information security system that includes: Confidentiality, Authenticity, Integrity and Non – Repudiation.

4. Conclusion

Steganography, in its multitude of forms, has been in use literally for thousands of years. It appears to have been utilized primarily and most effectively in time of war or civil strife. It would appear that based on the variety of forms that steganographic messages can take that there could be steganographic content on the internet. Location of some forms of steganographic content would require techniques other than statistical profiling not the least of which could be visual examination notwithstanding the ability to encrypt. While practical uses of steganography, with the exception of watermarking, seems to be relatively limited with the abundance of other techniques freely available, it will likely fill a niche for some activities.

References

[1] Behera, S.K. *"Colour Guided Colour Image Steganography"*, Universal Journal ofComputer Science and Engineering Technology**,** vol. 1, no. 1, pp. 16-23, IEEE, 2010.
[2] Gutub, A. *"Pixel Indicator High Capacity Technique for RGB Image Based Steganography*", WOSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E., pp. 154-159,IEEE,2008.
[3] Gutub, A. *"Pixel Indicator Technique for RGB Image Steganography",* Journal of Emerging Technologies in Web Intelligence, vol. 2, no.1, pp. 193-198,IEEE,2010.
[4] Marwaha, P. *"Visual cryptographic steganography in images"***,**Second Internationalconference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.
[5] Bailey, K. *"An evaluation of image based steganography*

methods", Journal of Multimedia Tools and Applications, vol. 30, no. 1, pp. 55-88, IEEE, 2006.

[6] Mahata, S.K. *"A Novel Approach of Steganography using Hill Cipher*", International Conference on Computing, Communication and Sensor Network (CCSN), pp 0975-888, IEEE, 2012.

[7] Chapman, M. Davida G, and Rennhard M. *"A Practical and Effective Approach to Large Scale Automated Linguistic Steganography"* found online at http://www.nicetext.com/doc/isc01.pdf.

[8] Mehboob, B.*"A stegnographyimplementation"*, Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium, ISSN 978-1-4244-2427-6, pp 1 – 5, IEEE, 2008.

[9] JawaharThakur,Nagesh Kumar, "DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis" in International Journal of Emerging Technology and Advanced Engineering Volume1,Issue 2,December 2011