International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

An Image Steganography Algorithm by Encrypting Watermarked Speech

Nikita Mhase[1], Kalyani Akant[2]
[1,2] *Electronics and Telecommunication Engineering Department,GHRCE Nagpur*

Abstract -- The increasing development of data transfer through internet made it easier to send the data accurate and fast to the destination. There are many transmission mediums to transfer the data to destination like e-mails; at the same time it is easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any changes, there are many approaches like Cryptography and Steganography. This paper deals with the image encryption as well as with the audio watermarking and Steganography. A review of various papers referred is given in brief. The outstanding progress of digital technology has increased the ease with which digital data is produced again and transmitted. However, since the advantages of such a progress are broadly available, they offer increasing potential to legal and unauthorized data manipulation. Consequently, the necessity arises to protect of digital media against unauthorized recording attempts, knows as data piracy. Current research in image, audio and visual copyright protection exploits the fact that the human visual perception and auditory system cannot detect small changes in some temporal or frequency domains of the image and the audio signal, respectively. This property is called masking, according to which a light but perceptible signal becomes non-perceptible in the presence of another one under certain conditions.

Keywords:Cover signal, Cryptography, Encryption, Secret key, Secret signal, Steganography, Watermarking

I. INTRODUCTION

Steganography means concealing a file, message, image, or video within another file, message, image, or video. The word Steganography is the combination of the Greek words steganos meaning "covered, concealed, or protected", and graphia meaning "writing". the message hidden may be an invisible ink between the visible lines of a private letter. Steganography is the hiding of information within computer files. In digital steganography, electronic communications includes steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are popularly known for steganographic transmission because of their large size. For example, a sender might start with an offensive image file and adjust the color of every 200th pixel to correspond to a letter in the alphabet, a change is so subtle that someone not looking for it is unlikely to notice it. Most research methods consider a watermark signal that is produced in a different fassion by a function of one or more input keys. These keys can be dependent on both owner and signal. These keys generate a signal which is embedded on the original one. The embedding signal is known as a watermark or copyright label. The Temporal characteristics and frequency characteristics of the original signal should be taken into account in the watermark embedding process to reduce perceptible distortions in the watermarked signal. Each and every individual that produces or possesses digital data has a unique key that identifies its legal possession and the same key is required for the watermark detection. Besides copyright protection purposes, a watermark serves authentication purposes, as well.

A watermark must be statistically undetectable by others to prevent the efforts of its removal without authentication. This condition is fulfilled only if the number of keys that produce distinct watermarks is large enough to make sure about statistical safety. The detection scheme should be as statistically reliable. False acceptance or rejection of the existing watermark should be minimal. Finally, a watermark has to be robust to signal manipulation and must be impossible to be removed without significant alteration of the signal. In other words, a pirate should have to destroy the complete audio signal before he tries to destroy the watermark. The robustness should be extended to common signal processing operations, such as filtering, compression, resampling, requantization, cropping, noise, D/A conversion.

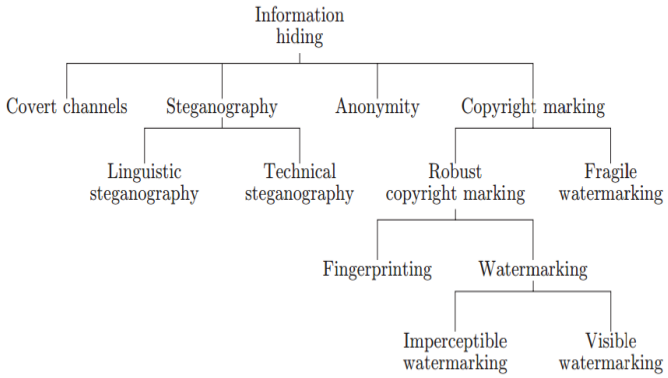
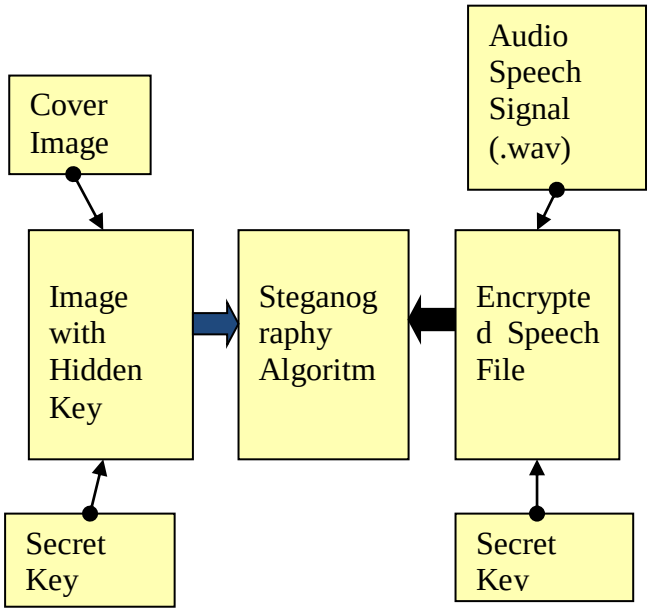


Fig.1: Information Hiding Techniques



II. PURPOSE OF STEGANOGRAPHY

The purpose of steganography is to hide data into other data. The main problem with this is, encrypted a file with strong crypto looks like a random stream of bytes. And random bytes are extremely rare in the computer world. At every level from the smallest TCP/IP packet that circulates through routers on the internet network, to the biggest DivX movie on your hard drive, information is formatted by fixed structures, defined file types, strict hierarchical models. Basically, computers do not have any random data. So, a sudden stream of random bytes appearing somewhere is as similar as an elephant in a supermarket. Very easy to detect in a flow of large number of structured bits. In other case, if you are of the curious type (or a FBI agent), a sudden stream of isolated random bytes is going to be flagged as suspicious. The point of cryptography is to transform intelligible and structured data (eg. text file) into a stream of random-looking bytes. The point

of steganography is quite contradict. It mixes the random-looking data with decoy information so that it will look like structured format.

1) Types Of Steganography

Steganography can be divided into two types, Fragile and Robust. The following section deals with the definition of these two different types of steganography.

a. Fragile

Fragile steganography involves embedding information into a file in which, if the file is modified, the information is destroyed. This method is not suitable for recording the copyright holder of the file because it can be removed very easily. But is very useful in certain situations where it is required to prove that the file has not been tampered, such as using a file as evidence in a court of law, since tampering the file would have removed the watermark. Fragile steganography techniques are easier to implement than robust methods.

b. Robust

Robust steganography aims to embed information into a file which cannot be destroyed easily. Although none of the mark is actually indestructible. We can consider a system robust if the amount of changes needed to remove the mark would render the file useless. Therefore the mark should be embedded in a part of the file where its removal would be easily noticed or perceived. There are two main types of robust marking. Fingerprinting includes hiding a unique identifier for the customer who originally acquired the file and hence is allowed to use it. Let the file be found in the possession of somebody else, the owner having the copyright can use the fingerprint to identify who violated the license agreement by distributing a file copy. Unlike fingerprints, watermark helps us to identify the copyright owner of the file, and not the customer. As fingerprints identify people who violated the license agreement, watermarks help in prosecuting who have an illegal copy. Ideally fingerprinting can be used in various applications, but for mass production of CDs, DVDs, etc it is not feasible to give each one a distinct fingerprint.

Watermarks are generally hidden to prevent their detection and removal; they are called as imperceptible watermarks. However this will not always be the case. Visible watermarks can also be used and can take the form of a visual pattern overlaid on an image. The application of visible watermarks is similar to the use of watermarks in non-digital formats.

III. LITERATURE REVIEW

A) Audio Watermarking by using Image Comparison(2014)

This Paper [1] focuses a new technique of Audio Watermarking which is based on Image Comparison. To make such algorithm more robust use a 2-D image matrix that will give good resultsrelated to performance, imperceptibility, robustness, and speed. This Watermarking technique gives good performance against the various attacks such as Additive White Gaussian Noise (AWGN), cropping, echo, low pass filter, requantization, and Resampling. The proposed technique is efficient and has stable performance against various attacks. It is computationally faster.

B) A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security(2016)

In this paper [2] a new algorithm is proposed. A symmetric key is generated which consist of secret arrangement of signal in the cover signal data bits. In this paper the authors have developed the encryption process on a secret speech/sound signal data bits to achieve higher strength of encryption which is hidden inside the cover image. The encryption algorithm is applied with embedding method. This is robust and secure method for data hiding**.**

C) New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique (2013).

In this paper [3], a new image encryption algorithm is proposed. It is already known that security of the algorithm is solely depended on the length of the key. The longer key length will always support

to good security and proposed algorithm used 128 bits key length which is provided too much security for the proposed algorithm. Crypto analysis of the proposed key is required to access original key which requires 2^{128} time to break the key which is almost impossible for any hacker. There is no chance to have floating point error because no such types of mathematical formula have been used in the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm was calculated.

D) Digital watermarking in audio for copyright Protection (2014)

This paper [4] focuses on an efficient and robust audio watermarking algorithm that is based on double transforms. Firstly, the original signal is decomposed by discrete wavelet transform (DWT). Then the approximation coefficients are divided in non-overlapping 2D blocks. Singular value decomposition (SVD) is applied on each block. The watermark is embedded in the singular values (SVs) for each block. Watermark extraction is non-blind and is done by performing the inverse operation of embedding process. This paper proposes a double transformation audio watermarking algorithm based on DWT and SVD. This two transforms are applied on the original signal. The insertion is done in the low frequency zone in order to ensure more robustness against common signal processing. In this case, the extraction is non-blind (the original audio signal is needed in the extraction phase)in order to improve the robustness of the watermark and the reliability of extraction process.The method uses a double key in order to add more security.

E) An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption,(2008)

RijnDael algorithm was introduced by Mohammad Ali Bani Younes and Aman Jantan [5] using the combination of image permutation. The original image was separated into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process. Then 'RijnDael' algorithm was applied on the generated image for encryption. Their results proved that the correlation between image pixel elements was significantly reduced by using the combination technique and thus higher entropy was achieved.

F) Secure and Robust High Quality DWT Domain Audio Watermarking Algorithm with Binary Image(2012)

To enhance robustness and security of digital audio watermarking algorithms, this paper[6] presents an approach based on mean-quantization in Discrete Wavelet Transform (DWT). A binary image is used as a watermark, and is encrypted with secret key. It is based on the embedding of an encrypted watermarked signal in the low frequency components using a two wavelet functions. The main reason for embedding the watermark in the low frequency components is that these components' have high energy which is enough to embed the watermark in such a way that the watermark is inaudible; therefore, it does not alter the audibility and is not easy to remove. The algorithm has a good security as only the authorized can detect the information embedded to the host audio signal. The watermark can be blindly extracted without any knowledge of the original signal. The method uses an encrypted binary image to decide whether or not to embed the watermark signal into the original host audio signal. In order to examine the robustness and transparency of the proposed audio watermarking method, watermark embedding and detection test of audio signals is conducted. The frame size affects the performance of the algorithm so that it must be adapted to give high PSNR(Signal to noise ratio) and NCC.

G) A Technique for Image Encryption using multi level and image dividing technique, (2003)

Chang- Mok Shin, Kyu-Bo Chol, SmJmng Kim, Dong-Hoan Seo, and Ha- Wmn Lee, [7] proposed the multi-level image encryption technique by using binary exclusive OR (X-OR)operation and image slicing technique. The multi-level image can be divided into binary images having the same

gray levels. The binary images are then converted to binary phase encoding and then encrypt these images with binary random images by binary XOR operation. Encrypted gray image was then obtained by combining each binary encrypted image.

H) Digital Audio Watermarking and Image Watermarking for Information Security(2015)

The article[8] proposes the contrast mapping (RCM), an integer transform by using sets of pixels. RCM is the invertible procedure. Contrast mapping procedure having very low mathematical complexity. Finally, RCM system is correlate with difference expansion system with respect to the bit rate hiding volume and to the mathematical complexity.

I) New Data Hiding Algorithm in MATLAB using Encrypted secret message(2011)

In this work Agniswar Dutta and Sankar Dashave[9] introduced a new method for encrypting any secret message inside a cover file. It follows a new bit exchange algorithm. Here the authors modified the steganographic method. Instead of changing the LSB of the cover file, the authors proposed to change LSB and LSB+3 bits and changing alternate bytes of the cover file. It means to hide eight bits of secret message the authors used 8 bytes of the cover file but out of 8 bytes 4 bytes were modified in LSB and LSB+3 bit positions and the alternate bytes remain unchanged. Before the actual embedding process starts the secret message was encrypted by using a simple bit exchange method. The number of times the secret message to be encrypted can be controlled by the user. The proposed bit exchange method is reversible that means decryption is done in a reverse way as that of encryption.

IV. CONCLUSION

In this paper we have presented a brief review of various papers. The detail analysis of watermarking techniques is discussed which will help the researchers in research areas. The comprehensive review of literature made has uncovered various aspects of Digital Image watermarking. There are different methods of watermarking like DWT, LSB, Image comparison which gives better PSNR.

REFERENCES

i. Eknath Kulkarni. Dr. S.P. Metkar Harshad C. Kamble. Kaustubh Masurkar "*Audio Watermarking by using Image Comparison*" IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014),
ii. Sheetal A. Kulkarni Shubhangi B. Patil *"A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security "* International Conference on Pervasive Computing (ICPC)
iii. Keerti Kushwah, Sini Shibu *"New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique,"* International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 61 – 65
iv. Mustapha Hemis and Bachir Boudraa *" Digital watermarking in audio for copyright protection"* 978-1-4799-8075-8/14/$31.00 c_ 2014 IEEE
v. Mohammad Ali Bani Younes and Aman Jantan, *"An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption"* IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.
vi. A.R.Elshazly, M.M.Fouad M.E.*Nasr " Secure and Robust High Quality DWT Domain Audio Watermarking Algorithm with Binary Image*" 978-1-4673-2961-3/12/$31.00 ©2012 IEEE
vii. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, *"Multilevel Image Encryption by Binary Phase XOR Operations"*, IEEE Proceeding in the year 2003.
viii. Rupali Warkar Priyanka More and Dattatray Waghole *"Digital Audio Watermarking and Image Watermarking for Information Security"* International Conference on Pervasive Computing (ICPC)
ix. Agniswar Dutta Abhirup Kumar Sen Sankar Das *"New Data Hiding Algorithm in MATLAB using Encrypted secret message"* International Conference on Communication Systems and Network Technologies 2011
x. Jasleen Kour& Deepankar Verma *,"STEGANOGRAPHY TECHNIQUES –A REVIEW PAPER"* International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5)May 2014
xi. R.Poornima and R.J.Iswarya," *AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY"* International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013