Multimedia Data Hiding Evaluation Metrics

ALAA A. JABBAR AL-TAAY¹, SHAHRIN BIN SAHIB²
Faculty of Information & Communication Technology¹,²
Universiti Teknikal Malaysia Melaka
Melaka, MALAYSIA
College of Science, Al-Mustansiriyah University¹
Baghdad, Iraq
alaaj@student.utem.edu.my, shahrinsahib@utem.edu.my

MAZDAK ZAMANI
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, MALAYSIA
mazdak@utm.my

Abstract: - This paper intends to give a literature review on multimedia data hiding, its uses and techniques. It also attempts to give a literature review on steganalysis techniques.

Key-Words: - multimedia security; digital data hiding; steganography; watermarking

1 Introduction

Art of data hiding in digital media, steganography and watermarking, aims to embed secret data into cover with purpose of identification, copyright protection, and annotation. The main constraint factors of this process are message data quantity, necessity of invariability of embedded data under distortions like lossy compression, third party removal, or modification. Data hiding techniques fall into three categories of cryptography, steganography, and watermarking. Watermarking and particularly steganography tend to conceal presence of hidden data while cryptography makes data gibberish [1-5].

Digital data hiding falls into different classes like embedding copyright information in different digital media formats such as text, audio, image, or video with the least possible perceivable degradation effects on the host signals. For example, effects must be inaudible or invisible to its observers. Data hiding techniques are distinct from encryption techniques as they aim to make the embedded data unrecoverable and inviolate-able [6-9].

Today there are various applications of information hiding. Knowledge of data hiding might be used either in ethical or unethical ways. However, data hiding algorithms cannot easily be categorized either in steganography or watermarking categories as there is no transparent boundary between these two terms and mostly the classification relies on application of the algorithm. Therefore regardless classifying data hiding applications the most common data hiding applications are fingerprinting, secret communication, secure storage, covert communication, and copyright protection [10-16].

Fingerprinting allows tracing originator or recipients of particular copy of the media be traced by means of watermarking. The employed watermarking technique must support high degree of robustness against both intentional and unintentional attacks. For instance, in advance of distributing plentiful copies of digital multimedia products among users, the copies can be watermarked by embedding various identity or serial numbers [17, 24].

Secret communication can be established by means of hiding secret information within digital media covers to hide presence of communication. This application falls in category of steganography rather than watermarking [25-28].

Secure storage means utilizing the cover digital media as secure storage for some sensitive information. For instance, drug prescriptions or medical records of patients need to be kept secure at storing and transmission time because of the consequences it may cause if be abused by unauthorized people for illegal activities or identity theft to fraud insurance [29].

Covert communication for some organizations or people might be vital to keep their data safe against unauthorized people. For instance, army can use this...
method to make covert transmission of technical information of battle plans against attackers which could harm whole operation if the data be compromised [30].

Copyright protection helps to protect dedicated resources to production of intellectual properties. Specifically in industrial societies reproduction expenditure of an intellectual property is far less than creation of it. To protect the copyright some data which represents the property owner information will be embedded within the host digital media. The watermarking algorithm is expected to be robust against attacks and let the owner prove the ownership in court cases. Fragile watermarking also might be used for host signal tampering. In addition, watermarking can be used for controlling access policy or limiting particular copies [31].

2 A Literature Review on Multimedia Data Hiding

Salma, Maha and Chokri [32] explain that audio watermarking is science of embedding inaudible data into digital audio cover without perception of listener. They talk about an audio watermarking model which relies on LSB technique in multi-resolution domain which uses characteristics of MP3 compression and PEAQ audio quality algorithm. To achieve highest level of inaudibility they adapted PEAQ algorithm for selecting proper audio band for embedding data in least significant bits of the multi resolution coefficients. Furthermore, they utilized MP3 data compression techniques for enhancing their algorithm robustness. The proposed model delivers desirable robustness against Uacks, StirMark, and compression. In addition it lets watermark data blind retrieval without necessity of original file.

Kondo [33] evaluates a stereo audio signal data hiding algorithm which uses added echoes polarity in high frequency channels for data embedment. Performance of the algorithm also compared with the usual spread spectrum data hiding methods and the practices which use various delayed echo techniques. Embedded data with added 20 dB SNR are almost free of error; especially for MP3 coders no error was detected. However, in their proposed method cropping random bits and converting sample bits did not show any affection on data while other techniques like spread spectrum returned considerable number of errors. Audio quality tests by MUSHRA method showed modest degradation with higher quality in comparison with other techniques.

Kraetzera, Dittmann, and Langa [34] describe general definition of “transparency” in term of attack-based digital watermarking evaluation algorithms, digital watermarking, and steganography. To do so, definition of transparency described for each one of the fields and then consequently they give unique definition which covers all three of them. They evaluated practicality of their given definition by using steganographic, audio watermarking, and attack-based evaluation algorithms which were convenient for audio watermarking benchmarking (StirMark for audio SMBA). For this purpose particular attacks from the SMBA were chosen to be modified for transparency enhancement measures which use psychoacoustic model. They compared result of original and modified attacks on robustness and transparency evaluation of watermarking algorithms and results shown that transparency benchmarking resulted in new information according algorithms and their usages.

3 Multimedia Data hiding evaluation metrics

Gupta and Biswas [35] conducted a research on performance evaluation of different JPEG steganography techniques. They say that first category of steganography methods is spatial domain techniques which in it secret messages will be embedded directly. The most common spatial algorithm is using Least Significant Bits (LSB). In second category, frequency domain schemes, the secret data will be embedded in a cover image which is transformed by techniques like DCT, DWT, or DFT. Capacity of data embedding of first category, spatial domain, is higher than capacity of second one while robustness of frequency domain techniques is better than first one. Since robustness is very important steganography factor then frequency domain techniques are used widely.

Majority of image data hiding techniques use uncompressed formats like BMP or GIF because potentially they have much visual redundancy and therefore are able to accommodate higher volume of secret data. Although uncompressed formats are more convenient for data hiding algorithms, because of size JPEG is used more than every format in the internet. Gupta and Biswas [35] focused on evaluation of Direct Cosine Transform (DCT) technique for JPEG files to find most efficient algorithm. Their research experiment on evaluation
of different algorithms proved that Outguess and F5 are most reliable data embedding algorithms for JPEG files.

Amer et al. [36] developed a toll for evaluation of image watermarking algorithms. Measuring output of processed images shows degradation happened due to data embedment. Quality evaluation of watermarking algorithms aims to compare behaviors of them consisting three evaluation approaches of objective quality evaluation, subjective quality evaluation, and attack robustness. Amer et al. [10] tried to run attack on watermarked images and then compare result with original watermarked image to calculate its robustness.

Watermarking attacks can be classified in intentional and unintentional attacks. For intentional attacks, attacker aims is to eliminate watermarked data in a way that has minimum effect on the media. Unintentional attacks will happen with purpose of processing, storing, or transmitting the media and will hurt watermarked data unintentionally. Developed tool by Amer et al. [36] will assist watermarking algorithm designers to evaluate robustness of their proposed algorithms against intentional and unintentional attacks.

Bailey and Curran [37] investigated and evaluated seven different implementations of image steganography techniques on GIF files to analyze weaknesses and strengths of chosen methods. Choosing methods was based on different resistance strength to different steganalysis types or their ability for maximum message storage size. 1-bit, 2-bit, 3-bit, 4-bit, color cycle, 1-bit prng, and stego Fridrich were seven chosen methods. All seven chosen methods were LSB or color rearrangement based for generating significant bit or parity patterns corresponding to hidden message.

Tiwar and Shandilya [38] evaluated vulnerability of different LSB based steganography techniques. In this research they chose GIF image file format due to its popularity in the internet environment. Image steganography techniques were employed along with cryptography techniques to achieve higher security. Different steganography schemes were compared and their vulnerability analyzed. Tiwari and Shandilya [38] also discussed about steganography applications in network security.

Boato, Conotter, and Natale [39] developed a new genetic based evaluation tool for testing robustness of watermarked images. By running all possible attack types the software returns best copy of un-watermarked image in term of Weighted Peak signal to Noise Ratio (WPSNR). Their software tries to find most convenient attack or combination of attacks on given cover which has less possible quality degradation in term of human perception.

Liu et al. [40] explains that for evaluating steganalysis performance information hiding ratio is important factor. Beforehand some publications clearly described relevance of detection performance and image complexity. In their research they propose an image complexity parameter and then adopt Generalized Gaussian Distribution (GGD) shape parameter of wavelet domain for measuring complexity of image. For detecting existence of LSB steganography data they proposed different correlation features. In comparison with HCFHOM, HOMMS, A.HCFCOM, and C.A.HCFCOM for gray images, and HCFCOM and HOMMS for color images their proposed feature has better performance. Acquired experience during running the project shown that in addition of information hiding ratio, image complexity is also a key factor in performance detection and features’ statistical significance. Detection performance and significance decreases when complexity of image increases and hiding ratio decreases. However, if the image contains complicated textures or has low hiding ratio thee steganalysis of LSB matching table would be very challenging.

Xiu-ying and Jia-jun [41] proposed an evaluation metric for color stego images. They say that whether PSNR is widely used for steganographic algorithms evaluation, but it is not accurate metric for performance evaluation. More important shortage is lack of imperceptibility of color stego images. In their paper on basis of HVS model and analysis of color space, color masking weight has been calculated and a new imperceptibility metric of CYIQ has been proposed. Gathered data and experimental results prove that CYIQ is more accurate metric than PSNR and reflects luminance masking, color masking, and texture masking of human visual system.

Reddy et al. [42] in their paper talk about philosophy of steganography and covert communication and then elaborates advantages of using least significant bits in order to hide secret messages. They also propose a LSB embedding technique which can hide secret information in 8-bits and 24-bits grayscale images. Also in continue they offer a new evaluation metric which supports various file formats.

Zhang et al. [43] talk about reasons like image transmission, storage, compression, processing, and acquisition which impress quality of digital images. Therefore assessing quality of images especially
after watermarking is very vital. Different developed applications use different watermarking techniques and for evaluating each algorithm there are different criteria. One of main watermarking evaluation shortages is lack of comprehensive method be able to evaluate a watermarking algorithm form different aspects. Zhang et al. propose a watermarking evaluation method which can assess invisibility, capacity, security, and robustness of watermarking algorithms.

Nguyen et al. [44] tried to answer two questions which helped them to find proper watermarking transparency assessment metric. Their first question is “how to find a particular metric which delivers best discrimination to watermarking artifacts?” and second one is “what are the watermarking artifact sensitive metrics?” To answer these questions they choose statistical approach for investigation of used objective quality metric performance in their literature to find most convenient watermarking transparency evaluation quality metric.

To answer first question they statistically analyzed a group of quality metrics to find the most convenient metric which delivers best discrimination to watermarking artifacts. Some subjective tests were done to answer second question to find the correlation between Mean Opinion Score (MOS) and each quality metric. Gathered results from both subjective and objective investigations answered the questions.

References:


[34] Christian Kraetzera, Jana Dittmann and Andreas Langa Transparency Benchmarking on Audio Watermarks and Steganography.


