Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Secure Data Hiding Technique Using Video Steganography and Watermarking

Eric Sowah Badger
School of Technology
Ghana Institute of Management & Public Administration
GreenHill, Accra Ghana
E-mails: niihack.gh@gmail.com

ABSTRACT

The rapid development of data transfer through the internet made it easier to send the data accurately and faster to the destination. Besides this, anyone can modify and misuse valuable information through hacking at the same time. This paper presents video steganography with digital watermarking techniques as an efficient and robust tool for protection. This paper is a combination of Steganography and watermarking; which provides a strong backbone for its security. Here considers video as a set of frames or images and any changes in the output image by hidden data is not visually recognizable. This proposed system not only hides a large volume of data within a video; but also limits the perceivable distortion that might occur while processing it.

Keywords: Steganography, Digital watermarking, Least Significant Bit, Discrete Wavelet Transform, Discrete Cosine Transform

Proceedings Citation Format
Eric Sower Badger (2022): Secure Data Hiding Technique Using Video Steganography and Watermarking. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 113-117. www.isteams.net/ecowasetech2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P21

1. INTRODUCTION

Data security means protecting a database from destructive forces and the unwanted actions of unauthorized users. A huge amount of confidential information is being exchanged over the Internet (a publicly open medium) as this is the most cost effective and widely available way. This technological progress has also made digital data very much vulnerable to interception and then possible unauthorized access/use and has caused significant economical losses for the content producers and rights holders. To protect data on public channels, security measures need to be incorporated into data communication systems over the Internet. Steganography is one of the promising technologies helping to achieve the overall goal of secure delivery of information from its source to authorized end-users. Steganography is the art or practice of concealing a file, image, or message within another file, image, or message. The word steganography is of Greek origin and means "covered writing" or "concealed writing". Steganography is changing the digital media in a way that only the sender and the intended recipient are able to detect the message sent through it. On the other side steganalysis is the science of detecting hidden messages.

The objective of steganalysis is to break the steganography system and that condition is met if an algorithm can judge whether a given image contains a secret message. To reduce the possibility of attack, security needs to be kept secret i.e. invisible security. The important data can be inserted into multimedia documents in a way that cannot be spotted i.e., imperceptible (invisible) insertion of information into multimedia data. The Digital Watermarking technique is used to improve imperceptibility (i.e. invisibility) and robustness. Digital watermarking can be used on any digital image, an audio file, or text file. Digital watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal (also known as a watermark) can be used to identify the owner of the work, trace illegal copies, and authenticate the content of the work.

Steganography and watermarking differ in a number of ways including purpose, specification, and detection/extraction methods. The fundamental difference is that the object of communication in watermarking is the host signal with the embedded data providing copyright protection. In steganography, the object to be transmitted is the embedded message and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability. In addition, in steganography, the third party cannot detect the message in stego media but in watermarking, the third party cannot remove or replace the message. It mainly prevents illegal copies. Further, the existence of the watermark is often declared openly and any attempt to remove or invalidate the embedded content renders the host useless. The vitally important requirement for steganography is perpetual and algorithmic undetectability. Robustness against malicious attacks and signal processing is not the primary concern as it is for watermarking.

STEGANOGRAPHY: Steganography is changing the digital media in a way that only the sender and the intended recipient are able to detect the message sent through it. The following formula provides a very generic description of the pieces of the steganographic process [4]: cover_medium + hidden data + stego_key = stego_medium. In this context, the cover_medium is the file that is used to hide the hidden_data, which may be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Video and image file especially comply with this requirement that can be used for information hiding. Fig 1 shows the four main categories of file formats that can be used for steganography

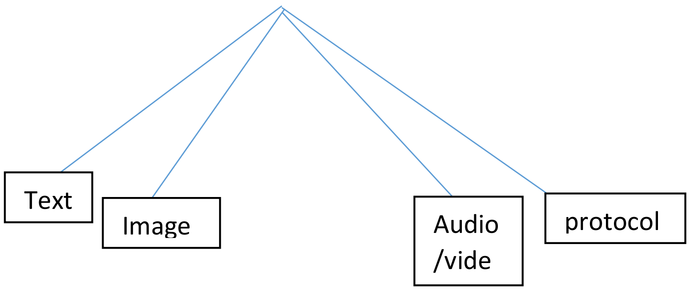

Fig 1: Four main categories of file formats that can be used for steganography

Discrete Wavelet Transform

DCT has strong robustness and is widely used in digital image watermarking. DCT transforms a time domain signal into its frequency components. Many frequency coefficients are obtained from DCT, such as single direct current DC coefficients, low frequency, mid-frequency coefficients, and high-frequency coefficients. These middle-frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high Frequency). Consider a subimage g(x,y) of size n×n whose discrete transform T(u,v), can be expressed in terms of general relation [7],

$$\mathrm{T(U,V)}= T(u,v) = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} g\,(\mathrm{x,y})\,\mathrm{r}\,(\mathrm{x,y},u,v) \qquad (1)$$

$$r(\mathrm{x,y,u,v}) = s(x,y,u,v) = a(u)a(v)\cos[\tfrac{(2x+1)u\pi}{2n}] + \cos[\tfrac{(2x+1)\mathrm{v}\pi}{2n}] \qquad (2)$$

Where

$$a(u)a(v) = \{\sqrt{\tfrac{1}{n}}\; for\; u = 0 \qquad (3)$$

$$\sqrt{\tfrac{2}{n}}\; for\; u = 1,2 \ldots\ldots\ldots\ldots n-1 \qquad (4)$$

Given T(u,v) , g(x,y) similarly can be obtained using inverse discrete transform

$$\mathrm{T(U,V)}= g(x,y) = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} T\,(\mathrm{x,y})\mathrm{s}(\mathrm{x,y},u,v) \qquad (5)$$

2. RELATED LITERATURE

Title Of Paper	Author(S)	Findings	Gaps	Recommendations	Policies & Design
Digital Watermarking	Ishtiaq Ahmad (2005)	Watermark can be used later to identify the owner of the work, trace illegal copies, and authenticate the content, of the work. Watermarks of varying degrees of obtrusiveness are added to presentation media as a guarantee of authenticity, quality, ownership, and source.	The existence of the watermark is often declared openly and any attempt to remove or invalidate the embedded content renders the host useless.	It should be robust and transparent. Robustness means it should be able to survive any alterations or distortions that the watermarked content may undergo, including common signal processing alterations and intentional attacks to remove the watermark and used to make the data more efficient to store and transmit so the owner can still be identified.	A watermark to be imperceptible so that it does not affect the quality of the content and makes detection
Authentication	Craver S., Memon N (1998, May)	Given the increasing availability of cheap yet high-quality scanners, digital cameras, digital copiers, and printers, the authenticity of documents has become difficult to ascertain. Especially troubling is the threat that is posed to conventional and well-established document-based mechanisms for identity authentication, like passports, birth certificates, immigration papers, driver's licenses, and picture IDs.	It has become easier for individuals or groups that engage in criminal or terrorist activities to forge documents using off-the-shelf equipment and limited resources	The document should be checked, the watermark should be extracted using a unique key associated with the source, and the integrity of the data is verified through the integrity of the extracted watermark	The watermark can or should also include information on the original document that can aid in undoing any modification and recovering the original.

3. CONCLUSIONS AND FUTURE SCOPE

We have presented an overview and summary of recent developments in binary document image watermarking and data hiding research. Although there has been little work done on this topic until recent years, we are seeing a growing number of papers proposing a variety of new techniques and ideas. Research on binary document watermarking and data hiding is still not as mature as for color and grayscale images. More effort is needed to address this important topic. Future research should aim at finding methods that offer robustness to printing, scanning, and copying, yet provide good data embedding capacity. Quantitative methods should also be developed to evaluate the quality of marked images. The steganographic capability of different techniques needs to be investigated and techniques that can be used in covert communication applications need to be developed.

Future Work may be further enhancement of results by applying some other algorithm than used in this thesis. We can also take two videos as input and can embed secret messages in both. Other quality metrics can be used to judge the performance of the algorithm.

REFERENCES

1. Muhammad Abdul Qadir, Ishtiaq Ahmad (2005) “digital text watermarking: secure content delivery and data hiding in digital documents “IEEE.
2. Jayeeta Majumder, Sweta Mangal (2012) “An Overview of Image Steganography using LSB Technique “IJCA.
3. Chotikakamthorn N. (1999). ―Document image data hiding techniques using character spacing width sequence coding‖. Proc. IEEE Intl. Conf. Image Processing, Japan.
4. Arvind kumar, km. Pooja (2010) “Steganography – A Data Hiding Technique” IJCA
5. Nikita Kashyap, G. R. Sinha (2012) “Image Watermarking Using 3-Level Discrete Wavelet Transform (Dwt)” IJMECS.
6. Vladimír BÁNOCI, Gabriel BUGÁR, Dušan LEVICKÝ (2011) “A Novel Method of Image Steganography in DWT Domain” IEEE.