FPGA Implementation of Data Hiding In Images

[1]Prof. Chopda Priyanka, [2]Prof. Pawar Ganesh, [3]Prof. BambKalpesh

[1,2,3]DepartmentElectronics and Telecommunication Engg
[1,2,3]SNJBs K B Jain College of Engineering, Chandwad, Nashik(MS) India

Abstract

It is the process of embedding data within the domain of another data, this data can be text, image, audio, or video contents. The embedded watermark can be visible or invisible (hidden in such a way that it cannot be retrieved without knowing the extraction algorithm) to the human eye, specified secret keys are taken into consideration in order to enhance the security of the hidden data. Achieving the purpose of information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy to enhance the sound embedded in the way nature to be addressed. The results showed that the proposed algorithm has a very good hidden invisibility, good security and robustness for a lot of hidden attacks. However, the limitation of capacity has led us to think about an improved approach which can be achieved through hardware implementation systems with the help of a programmable gate array (FPGA) board.

This paper proposed LSB Information Hiding algorithm which can lift wavelet transform image. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels

Keyword: Stenography, LSB (Least significant bits), Encryption

Introduction

Cryptography is the practice of ‘scrambling’ messages so that even if detected, they are very difficult to decipher. The purpose of Steganography is to conceal the message such that the very existence of the hidden is ‘camouflaged’. However, the two techniques are not mutually exclusive. Steganography and Cryptography are in fact complementary techniques. No matter how strong algorithm, if an encrypted message is discovered, it will be subject to cryptanalysis. Likewise, no matter how well concealed a message is, it is always possible that it will be discovered. By combining Steganography with Cryptography we can conceal the existence of an encrypted message. In doing this, we make it far less likely that an encrypted message will be found. Also, if a message concealed through Steganography is discovered, the discoverer is still faced with the formidable task of deciphering it. The historical examples given earlier show that the use of Steganography is not limited to a new medium. It should therefore come as no surprise that techniques have been developed to work with digital media. It is now possible to hide any sort of digital media inside any other type of digital media. For example, it is possible to hide a text message, encrypted or plain text, inside of a digital picture or sound file. It is also possible to conceal one type of digital media inside of the same type of digital media. For example an image of a famous painting could be used to conceal a photograph of schematics of some type. Steganography has been in the news recently as it was members of the al-Qaeda terrorists were communicating by embedding Arabic messages inside digital files, such as JPEGs and MP3s, and distributed over the internet. Steganography is the art of concealing the presence of information within an innocuous container

STEGONOGRAPHY

Steganography is the process of hiding a secret message within a larger one insuch a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is theprocess of making a message unintelligible. In other words, Steganography attemptsto hide the existence of communication.

Stenography is the art of embedding information in such a way that prevents the detection of hidden messages. It means hiding secret messages in graphics, pictures, movie, or sound. Stenography comes from the Greek word steganos, which means ‘covered’, and graphy, which means ‘writing’. Covered writing has been manifested way back during the ancient Greek times around 440 B.C.

Some of old stenography examples are shaving the heads of slaves and tattoo messages on them. Once the hair had grown back, the message was effectively hidden until the receiver shaved the heads once again. Another technique was to conceal messages within a wax tablet, by removing the wax and placing the message on the wood underneath .The most popular and frequently method of Stenography is the Least Significant Bit embedding (LSB). The level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. If we are using the least significant bits of the pixels' color data to store the hidden message, the image itself is seemed unaltered, and changing the LSB’s value will have no effect on the pixel’s appearance to human eye. This art of covert communication is very ancient. Till date, multitudes of methods and variations have been developed, for hiding information. Hiding the secret message under a wax coating of a wax coated tablets is one of the oldest methods. The message can be camouflaged in text message.

TYPES OF STEGANOGRAPHY

Communication between people and organizations through the use of thephone, the fax, computer communications, radio, and of course all of thesecommunication should be secure. There are basically three Steganography types:-

1.Pure Steganography.
2.Secret key Steganography.
3.Public key Steganography.

CHARACTERISTIC OF STEGANOGRAPHY

a) Embedding Capacity:
The embedding capacity in data hiding indicates the total number of bits hiddenand successfully recovered by the Stego system.

b) Robustness:
Robustness refers to the ability of the embedded data to remain intact if thestego system undergoes transformation, such as linear and non-linear filtering,addition of random noise; and scaling, rotation, and compression.

c) Undetectable:
The embedded algorithm is undetectable if the image with the embeddedmessage is consistent with a model of the source from which images are drawn.

d) Invisibility (Perceptual Transparency):
Invisibility is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that contain hidden information and those that do not contain any hidden information.

e) Security:
It is said that the embedded algorithm is secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key.

METHODOLOGY

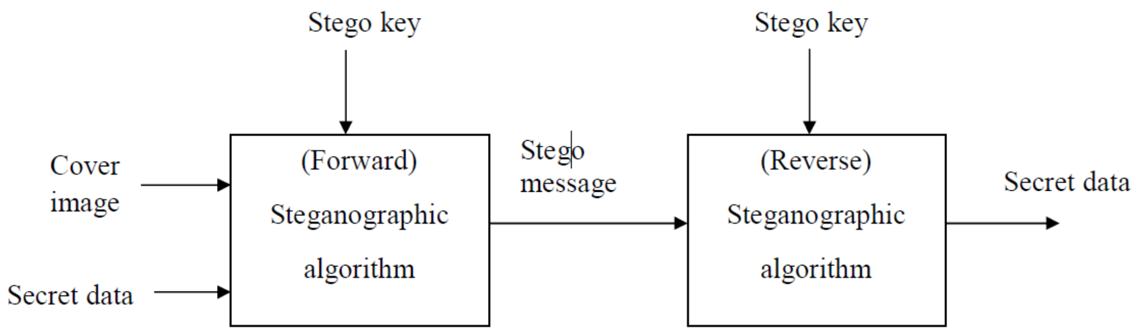

Stego key
Stego key
Cover image
Secret data
(Forward) Steganographic algorithm
Stego message
(Reverse) Steganographic algorithm
Secret data

Fig. 1 block diagram of steganography

The principles of Steganography system is shown in Fig. .1. It is assumed that the sender wishes to send messages via a communication channel, to a receiver. The sender starts with a cover message, which is an input to the stego-system, in which the embedded message will be hidden. The hidden message is called the embedded message. A Steganographic algorithm combines the cover message with the embedded message, which is something to be hidden in the cover. The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded message again. The output of the Steganographic algorithm is the stego message. The cover message and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message.

DESIGN STAGES

The design of the hardware architecture for data hiding consists of 5 main stages as follows:
1) First data acquisition (sequential) and realization of histogram.
2) Sequential calculations of LMs and RMs partial.
3) Concurrent computation of LM and RM final.
4) Sequentially calculating LN and RN.
5) Second data acquisition (parallel) and calculation of multiple pixels of the stego image.

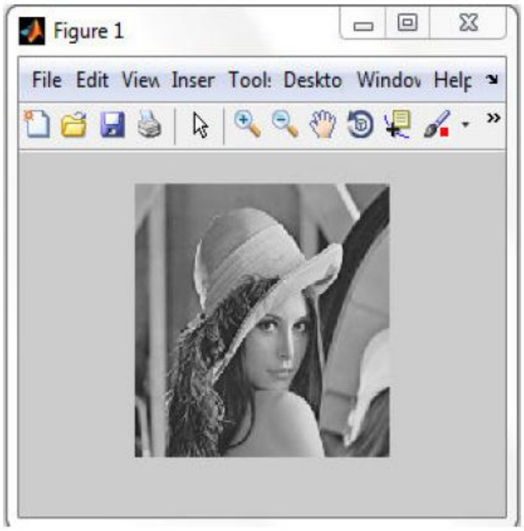
SOFTWARE

- MATLAB
- SIMULINK
- XILINX PLATFORM STUDIO
- SPARTAN 6
- VHDL

APPLICATIONS

Copyright Protection: -Digital watermarks can be used to identify and protect copyright ownership.
Tracking: -Digital watermarks can be used to track the usage of digital content
Tamper Proofing: -Digital watermarks, which are fragile in nature, can be used for tamper proofing.
Broadcast Monitoring: -Digital watermarks can be used to monitor broadcasted content like television and broadcast radio.

RESULTS



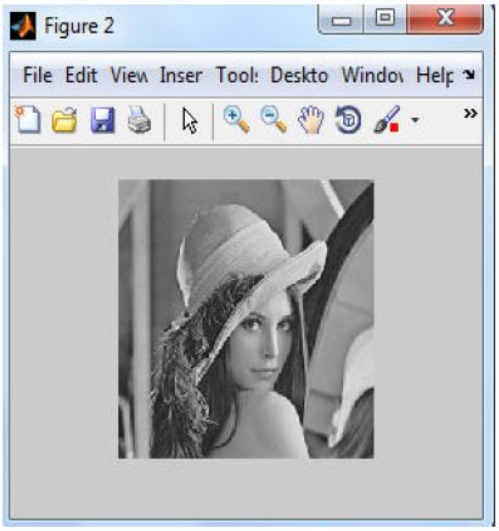


Fig.2Cover image *Fig. 3 Image after Steganography*

CONCLUSION

In this paper, we presented a new approach for data transmission in image. We initially motivated our study of raw video by examining the intended applications Here we propose a data hiding and extraction procedure for high resolution images Although embedding data in image using VLSI implementation takes more size but it can be transmitted from source to target over network after processing the source image y using these Data Hiding and Extraction procedure securely. There are two different procedures, which are used here at the sender's end and receiver's end respectively. The procedures are used here as the key of Data Hiding and Extraction. Achieving the purpose of information hiding with the secret bits of information to replacethe randomnoise, using the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy to enhance the sound embedded in the way nature to be addressed.

According to Matlab results, the LSB algorithm provides a higher PSNR and NCC value, this shows that embedding process is highly imperceptible and provides high quality stego image. Finally LSB algorithm and interpolation technique have been successfully implemented in FPGA. Experimental results show that the power consumption and area used in LSB is better than the Interpolation technique.

REFERENCES

[1] R. Gonzales, and R. Woods(1993), Digital Image Processing, Addison Wesley Publishing Co.,3^{rd} Edition 1993 (Chapt.7,Page No. 107,108,212,213,214).

[2] Silman, J.(2001), "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[3] Wang, H & Wang, S (2004), "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM,47:10, October 2004

[4] Simmons, G (1983)., "The prisoners problem and the subliminal channel", CRYPTO, 1983

[5] Chandramouli, R., Kharrazi, M. & Memon, N.(2003), "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[6] Ahsan, K. & Kundur, D (2002)., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[7] Johnson, N.F. & Jajodia, S (1998)., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[8] W. Sweldens (1996), Building Your Own Wavelets at Home, Wavelets in Computer Graphics, ACM SIGRAPH Course Notes, 1996.

[9] A. Calderbank, I. Daubechies, W. Sweldens, and B. Yeo (1996), Wavelet Transforms that Map Integers to Integers, Mathematics Subject Classification, 42C15, 94A29, 1996.

[10] B. Weaver (2007), Now You See It, Scientific Computing 24.6 (May 2007): 18-39.

[11] I.Daubechies & W.Sweldens,(1996) Factoring Wavelet Transforms into Lifting Steps.Technical Report Bell Laboratories,Lucent Technologies ,1996.

[11] Rahman Tashakkori,Christopher D.Scholar (2010),"Message Encoding in Images Using Lifting Schemes",IEEE 2010.

[12] S. Mallat (1989), "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation," IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 11, No.7, pp. 674-693, July 1989.

[13] Marvel, L.M., Boncelet Jr., C.G. & Retter, C.(1999), "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999