Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.271 – 275

RESEARCH ARTICLE

An Enhance Approach for Invisible Watermark for Digital Images to Watermark Image Text Data

Gurpreet Kaur
M.Tech student CSE department, Guru Kashi University, Talwandi Sabo
Gurpreetpreet622@gmail.com

Vinod Sharma
Assistant Professor CSE Department, Guru Kashi University, Talwandi Sabo
Ojasompreet@gmail.com

Abstract

Invisible watermarks are mainly used to hide the information in an image. It is the science of secret communication. The goal of invisible watermark is to hide the existence of the message from unauthorized party. The modern secure image invisible watermark presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier le formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. The proposed work purposed an image based invisible watermark that Least Significant Bits (LSB) techniques and pseudo random encoding technique on images to enhance the security of the communication. In the L-SB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and water-object if few LSB bits of the cover object are replaced. In Pseudo-Random technique, a random-key is used as seed for the Pseudo-Random Number Generator is needed in the embedding process. Both the techniques used a water-key while embedding messages inside the cover image. By using the key, the chance of getting attacked by the attacker is reduced.

Keywords: Invisible watermark, LSB, Random-key, Image, secret message, water-key, cover image, Techniques.

Introduction

Digital invisible watermark is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore,

it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of invisible watermark to be used with communication protocols, which represent unconventional but promising invisible watermark mediums. Digital image invisible watermark, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image invisible watermark. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the water image quality (imperceptibility). This chapter provides a general introduction to the research by first explaining the research background. Then, the main motivations of this study and the research problem are defined and discussed. Next, the research aim is identified based on the established definition of the research problem and motivations.

Invisible watermark and Watermarking

Invisible watermark aims to hide the very existence of communication by embedding messages within other cover objects. However, watermarking aims to protect the rights of the owners of digital media such as images, music, video and software. Even if people copy or make minor modification to the watermarked file, the owner can still prove it is his or her file. Thus, both of invisible watermark and watermarking are forms of data hiding and share some common characteristics. Nevertheless, the goal of invisible watermark is the embedded message while the goal of watermarking is the cover object itself. Watermarking is a data hiding technique that protects digital documents, files, or images against removal of copyright information. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing a distortion or destroying the original (watermarked) object. This aspect or feature of watermarking is known as "robustness". According to the kind of embedded information, two techniques of document marking can be distinguished: watermarking

and fingerprinting. Watermarking is the process of embedding a specific copyright mark into digital documents in the same way. On the other hand, in order to detect any break of licensing agreement, a serial number is embedded in every copy of this digital document. This process is known as "fingerprinting". Even if these markings are detected, it should be practically impossible to remove them.

Invisible watermark: Methods of Classification

There are two general approaches to classify steganographic systems. The first approach is based on the type of cover file while the second approach is based on the hiding method or the layout of modification used in the embedding process (Cole, 2003; Katzenbeisser and Petitcolas, 2000). These two general classification approaches of invisible watermark are explained in the next subsections.

Cover-Type Based Classification

Since many kinds of digital media can be used as cover files of invisible watermark, the first approach of classification breaks down invisible watermark according to the type of the cover file used. However, the properties of these cover files vary from one type to another and these properties control how the secret data can be hidden in these cover files. To this end, knowing the type of cover file can give us an indication or idea where the secret data might be hidden (Cole, 2003). Mostly, steganographic systems are classified according to the cover file used. Accordingly, different invisible watermark types can be distinguished such as: image, audio, video, text, and HTML invisible watermark. For example, the steganographic system that uses digital images as cover files is an image-based steganographic system.

Hiding Method-Based Classification

Regardless of the cover type used for data hiding, invisible watermark can be classified according to the method used to hide secret data. Furthermore, this approach of invisible watermark classification is the most preferred approach in the invisible watermark research community. Accordingly, there are three ways to hide secret data in cover files: insertion-based, substitution-based, and generation-based method (Cole, 2003; Kipper, 2004).

Insertion-Based Method

This method depends on finding some areas in cover files which are usually ignored by applications that read this cover file and then embedding the secret data in these areas. Since this method inserts the secret data inside the cover file, the size of the water file would be larger than the size of the cover file. As a result, the main advantage of this method is that the contents of the cover file would not be changed after the embedding process since this method relies on accumulating or adding the secret data to the cover file.

An example of such a method is using a Word document to write a secret message in the areas between the end-text and begin-text markers. Because of the configuration of Word documents, which depends on ignoring anything written in such areas, the hidden message will not appear when this document is viewed in Word (Cole, 2003; Kipper, 2004).

Substitution-Based Method

Unlike the insertion-based method, this method does not add the secret data to the cover file data. However, substitution-based method depends on finding some insignificant regions or information in cover files and replacing this information with the secret data. Therefore, the sizes of both the water file and the cover file are similar since some of the cover data is just modified or replaced without any additional data. However, the quality of the cover file can be degraded after the embedding process. Additionally, the limited amount of insignificant information in cover files restricts the size of secret data that can be hidden (Cole, 2003; Kipper, 2004).

Generation-Based Method

Unlike both methods explained above, this method does not need a cover file since it uses secret data to generate appropriate water files. One of the invisible watermark detection techniques depends on comparing cover files with their water files. Therefore, one advantage of the generation-based invisible watermark is preventing such kind of detection since only water files are available and there is no cover files used. The major limitation of this method is the limited water files which can be generated. Moreover, the generated water files might be unrealistic files for end users (e.g. an image contains different shapes and colours without any sense or a text without any meaning). Therefore, the main media for such techniques are random-looking images and English text files (Cole, 2003).

Literature Survey

Vijay Kumar Sharma,2vishal Shrivastavaa "Invisible watermark Algorithm For Hiding Image In Image By Improved Lsb Substitution By Minimize Detection"

Invisible watermark is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of invisible watermark on their lives will continue to grow. Many confidential information were leaked to a rival firm using steganographic tools that hid the information in music and picture files. The application of invisible watermark is an important motivation for feature selection. In recent years, many successful invisible watermark methods have been proposed. They challenge by steganalysis. Steganalysis (type of attack on invisible watermark Algorithm)Algorithm which detects the water-message by the statistic analysis of pixel values, To ensure the security against the steganalysis attack, a new steganographic algorithm for 8bit(grayscale) or 24 bit (colour image) is presented in this paper, based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. in this n LSB of cover image ,from a byte is replaced by n MSB of secret image. the image quality of the water-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the water-image and the cover-image is derived. Experimental results show that the water-image is visually indistinguishable from the original cover-image when n<=4, because of better PSNR which is achieved by this technique. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to cover up the very existence of the embedded data In this a data hiding method by improved LSB substitution process is proposed. The image quality of the water-image can be greatly improved with low extra computational complexity.

Gurpreet Kaur, Kamaljeet Kaur ,Image Watermarking Using LSB (Least Significant Bit) In this paper author uses Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a

smaller object may be embedded multiple times. Authors does not test the proposed system on different types of images which is concluded as the future work.

Amit Singh, Susheel Jain, Anurag Jain, Digital watermarking method using replacement of second Least significant Bit(LSB) with inverse of LSB

In this paper new algorithm proposed for digital watermarking using Least Significant Bit (LSB) .LSB already used but there is a slightly effect on the image. The above algorithm is using LSB & second LSB bit. Here they used binary value of watermark text in LSB, and in place of second LSB, the inverse of their correspond LSB bit. The proposed algorithm is flexible depending on the length of watermark text. In this paper they compare theirproposed algorithm with simple LSB method and other method, for example DCT & DWT.

Proposed Methodology

The Proposed research aims to develop an improved invisible watermark approach which is Adaptive LSB Method for color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks. Images as well as text messages can be hide within the images using sequential and random methods. It will incorporate cryptography to achieve high security and random pixel embedding to attain high immunity to attacks. It would be highly immune to any environmental disturbances like noise due to hybrid filtering.

The proposed system comprises of two components:

1. Embedding Module
2. Extracting Module.

Embedding Module

Embedding is the process of hiding the embedded message generating the water image. Hiding information may require a Water key which is additional secret information, such as password, required for embedding the information.

For example, when a secret message is hidden within a cover image, the resulting product is water image (water object).

The main algorithm for the embedded stage can be listed as follow:

1. Input the message to hide.
2. Input the image in which message is to hide
3. Generate the binary code of the message
4. Read the image into RGB message.
5. Generate the fourier series and perform MOD - 3 operation to update RGB values to hide the data
6. Update the image matrix
7. Construct the image from the matrix updated in step 6
8. Display the result.

Conclusion

There are several types of algorithms for invisible watermark. Each type of algorithms has its own advantages and limitations. No method can provide fully perfect solution. Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in this field is to make the invisible watermark algorithms resilient to geometric transformations. In case of practical application, choice of solution type actually depends on the nature of application and requirements. The proposed method uses Modified LSB Method to optimize the strength of stegnographic process. The imperceptibility and robustness of proposed method shows better performance in comparison to other approaches in practice. Accuracy of the system evaluated to be 85% which shows considerably good improvement over the existing approaches.

Future Scope

Proposed system can embed the stegnograph such as images as well as text in the image of any format. We proposed two algorithms, one for embedding the stegno image into a cover image and second for decoding the message from the encoded image. Proposed system shows good results But it has one major limitation which is system cannot embed the image message larger than the image in which message to e hide. Further the proposed system can also be extended to embed watermark in the video file.

References

1. Vijay Kumar Sharma ,vishal Shrivastavaa "Invisible watermark Algorithm For Hiding Image In Image By Improved Lsb Substitution By Minimize Detection"
2. Gurpreet Kaur, Kamaljeet Kaur ,Image Watermarking Using LSB (Least Significant Bit)
3. Amit Singh, Susheel Jain, Anurag Jain, Digital watermarking method using replacement of second Least significant Bit(LSB) with inverse of LSB
4. Nayan K. Dey ,Suman K. Mitra ,Ashish N. Jadhav , Hybrid Scheme for Robust Digital Image Watermarking Using Dirty Paper Trellis Codes ,
5. Lahouari Ghouti, Ahmed Bouridane, Mohammad K. Ibrahim, and Said Boussakta, Digital Image Watermarking Using Balanced Multiwavelets
6. Amir Houmansadr,Shahrokh Ghaemmaghami ,A Digital Image Watermarking Scheme Based on Visual Cryptography
7. Neil F. Johnson2, Zoran Duric1, and Sushil Jajodia2 "Recovery of Watermarks from Distorted Images"
8. Henri Bruno Razafindradina and Attoumani Mohamed Karim , BLIND AND ROBUST IMAGES WATERMARKING BASED ON WAVELET AND EDGE INSERTION
9. Prabhishek Singh, R S Chadha, A Survey of Digital Watermarking Techniques, Applications and Attacks
10. Vinita Gupta, Mr. Atul Barve , A Review on Image Watermarking and Its Techniques
11. Chan-Il Woo and Seung-Dae Lee , Digital Watermarking for Image Tamper Detection using Block-Wise Technique
12. Gopika V Mane, G. G. Chiddarwar ,Review Paper on Video Watermarking Techniques
13. Rajat Tiwari,Navneet Kaur, Manpreet Kaur ,An Optimization Image Watermarking Technique Using Biogeography Based Optimization
14. Yonghong Chen, Jiancong Chen , Digital Image Watermarking Based on Mixed Error Correcting Code
15. Saeed AL-Mansoori and Alavi Kunhu , Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat-1 Images against Attacks

