ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Logo Steganography Using Digital Watermarking

Kanchan [1], Krishan Kumar[2]

Student, CSE, JCDM College of Engineering, Sirsa, India[1]

Assistant Professor, CSE, JCDM College of Engineering, Sirsa, India[2]

Abstract: Logo watermarking is attaining wide popularity in today's time. Watermarking has wide range of applications such as content identification and management, content protection, forensics and piracy deterrence, document and image security and many more. This paper presents a tamper-resistant algorithm for watermarking images. With appropriate alterations to the embedding and extraction methods, we can encapsulate logo watermark in the image by the use of watermark embedder. In this paper, we systematically review proposed attacks on watermarks. We use enlightened watermark detector which can extract the watermark even in the presence of geometric attacks.

Keywords: Logos, Image files, Watermark, Pixel

I. INTRODUCTION

Logo watermarking technology is acquiring booming consideration as it presents a creditable key for prohibiting copyright in fringement of the multimedia data. Digital watermarking is a process of inlaying a cryptic stream of bits in a file. Digital Watermarking has innumerable utilizations such as supervising owner credentials, valid owner, deal tracking, content verification, copy control, upper hand on device, in medical for patients confidential reports and in fingerprinting.

With the boundless use of internet the interactive media such as image, audio, video can be replicated, mutated and refitted by anyone easily and unlimitedly. The copyright protection of the hypercritical digital information is an esteemed legal issue globally. A watermark is infused into digital images so that it is inconspicuous to a person. The watermark must also be boisterous to typical image processing operations such as JPEG compression, cropping, resizing, noising, rotation, and so on.

Logos are characterised by two types of domains - Spatial domain and Transform domain. The transform domain image is sketched in terms of its frequencies; whereas spatial domain data embedding is done by directly manipulating the pixel values, code values or bit stream of the host image signal.

Logo watermarking, consist of two processes- embedding and decoding. 'E' represents the watermarking embedding algorithm and 'D' represents the watermarking decoding algorithm. The first process is encapsulation of watermark into image.

A sequence of watermark bits we want to hide in the image is expanded by extensive factor constant, and then the amplitude of spread sequence is amplified, and regulates it with a binary pseudo-noise sequence that behaves as key. Finally, the modulated signal is added to the image, yielding a watermarked image.

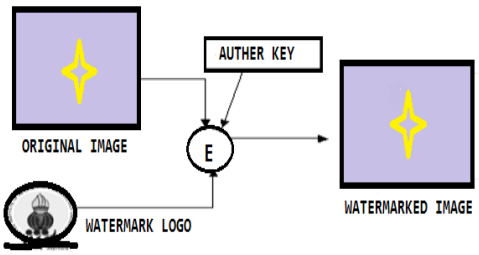

Figure 1 Embedding logo in image

The second process is detecting of watermark from a test image. This process is easily accomplished by multiplying the test image with the same key that was used in embedding and then sum all of results for each watermark bit.

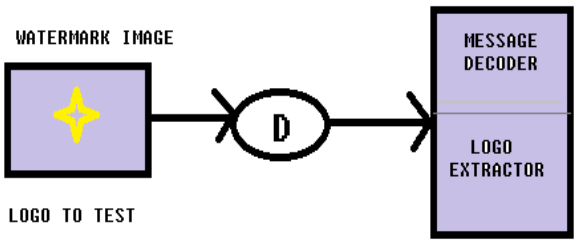

Figure 2 Decoding logo from image

II. LITERATURE REVIEW

Navneet Kumar Mandhani introduces the use of decimal sequences in watermarking to hide information for authentication. The underlying system is based on code division multiple access (CDMA), which is a form of spread spectrum communication. Different algorithms for the use of decimal sequences have been formulated for use in black and white images. The watermark is spread across the carrier image by using the d- sequences of optimal period and retrieval is made by the use of correlation. Matlab version 6.5 used to implement the algorithms discussed in this thesis. The advantage of using dsequences over PN sequences is that one can choose from

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

a variety of prime numbers which provides a more flexible system. Different methods for adding the random sequence to the image were investigated and results for random shifts and cyclic shifts have also been discussed. [2]

VIKAS SAXENA proposed that Watermarking has been invoked as a tool for the protection of Intellectual Property Rights (IPR) of multimedia contents. Because of their digital nature, multimedia documents can be duplicated, modified, transformed, and diffused very easily. In this context, it is important to develop a system for copyright protection, protection against duplication, and authentication of contents. For this, a watermark is embedded into the digital data in such a way that it is indissolubly tied to the data itself. Later on, such watermark can be extracted to prove ownership to trace the dissemination of the marked work through the network, or simply to inform users about the identity of the rights-holder or about the allowed use of data. This thesis deals the developing the watermarking schemes for digital images stored in both spatial and transformed domain. In this thesis they mainly focus on the Discrete Cosine Transform (DCT) based development. To prove its commercial usability, we take special care so that at least one attack, having huge financial implications, can be sustained due to the in-built capacity of the watermarking scheme. Apart from this, since JPEG is the most commonly used image format over WWW, we pay special attention to robustness against JPEG compression attack. Apart from developing watermarking schemes, we also discuss the selection of color channel to be used to carry the watermark data based on the attack that may occur most commonly on the watermarked images. They propose to increase the robustness against some attacks by pre-processing the images. In this thesis, they also present a correlation between the performance of the watermarking scheme against some attacks and the original image characteristics. All presented watermarking schemes are robust against common image manipulations and attacks [10]

Ingemar J. Cox, Matt L. Miller and Andrew L. McKellips examine the similarities and differences between watermarking and traditional communications. Their comparison suggests that watermarking most closely resembles communications with side information at the transmitter and or detector, a configuration originally described by Shannon. This leads to several novel characteristics and insights regarding embedded signaling. [14]. Peter Hanzlik described a steganographic system that embeds hidden data into communication channel that utilizes Reed-Solomon error-correction codes. A formal model of Reed-Solomon covert channel is proposed by stating requirements that are laid on such technique. The model was validated by experimental research methods. Findings indicate that the proposed model satisfies the primary attributes of steganography: capacity, imperceptibility and robustness. The research provides a stand base for further researches in the wide range of applications of Reed-Solomon codes [7]. Wong Hon Wah states *that* people are motivated to embed information such as owner info, date, time, camera settings, event/occasion of the image, image title, or even secret message in the digital images for value-added functionalities and possibly secret communication. Novel sample-based methods are proposed to embed some information bits in the JPEG compressed domain. The proposed method called J-Mark embeds the information bits in the DCT coefficients with significant energy in the selected blocks significant masking properties. Spread spectrum technique (SST) is widely adopted for vector-based image and video watermarking in the past few years.

Four novel techniques are proposed to embed watermarks for different purposes. The first one call Single Watermark Embedding (SWE) is use to embed a watermark bit sequence in digital images using two secret keys. The second technique called Multiple Watermark\ Embedding (MWE) extends SWE to embed multiple watermarks simultaneously in the same watermark space while minimizing the watermark energy. The third technique called Iterative Watermark Embedding (IWE) embeds watermarks in JPEG-compressed images. The proposed iterative approach can prevent largely the potential removal of watermarks in the JPEG recompression process. The fourth technique called Direct JPEG Watermark Embedding (DJWE) is an extension of the IWE. DJWE embeds the watermarks with lower computation complex then IWE and uses the Human Visual System (HVS) model to prioritize the coefficients to be altered to achieve good visual quality. Two techniques for watermarking capacity estimation are proposed. The first technique estimates the capacity for JPEG-to-JPEG image watermarking (J2J). In J2J image watermarking, the input is a JPEG image file and, after watermark embedding, the image is JPEG-compressed such that the output file is also a JPEG file. The second technique is an extension of the first technique to JPEG2000-to-JPEG2000 (J2K-2-J2K) watermarking. In J2K-2-J2K, the input is a JPEG2000 image file and, after watermark embedding, the image is JPEG2000-compressed using the same quantization factors. The Watson's Discrete Wavelet Transform (DWT) HVS model is used to estimate the JND of each Discrete Wavelet Transform (DWT) coefficients. The proposed techniques do not assume any specific watermarking method and thus would apply to any watermarking methods in the J2J and J2K-2-J2K framework.[12]

III. OBJECTIVES

To inlay the logo the first step is to embedd. Inside the encoder, one or several protocols will be implemented to embed the secret message or logo into the cover message. The type of protocol will depend on what information you are trying to embed and what you are embedding it in. For example, you will use an image protocol to embed information inside images. Our main objectives are:

1) Analyse Existing watermarking techniques

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

2) Develop a modified Algorithm to secure Digital Logos
3) Random Watermark generation for High Security
4) Impliment Modified Algorithm in MATLAB
5) Embedde and Extract features to validate working.

Existing Problems:
Some of the problems arise against the robustness and security.

1) Attacks to robustness are those whose target is to intensify the expectation of error of the data-hiding channel.
2) Attacks to security are those which are intended to accumulate knowledge about the secrets of the system
3) There are two types of attacks on security:

1. **Intentional attacks**: Attacks to security are seemingly intentional, but not all intentional attacks are threats to security. If the attacker got success in his attack, but by this intentional attack he has learned nothing about the secrets of the system.

2. **Blind attacks:** Blind attacks are those which do not attain any knowledge of the watermarking algorithm. Since attacks to security will try to expose the secret parameters of the watermarking algorithm, it is easy to realize that they cannot be blind.

3. **Non –Blind attacks**: A non-blind attack is not necessarily targeted at learning the secrets of the system.

IV. PROPOSED METHODOLOGY

Logo hiding (least significant bit method):
This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in a JPEG image for example, the following steps would need to be taken:

1) First load up both the host image and the image you need to hide.
2) Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.
3) Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

To get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.
Host Pixel: 10110011
Bits used: 4
New Image: **00110000**

V. CONCLUSION AND FUTURE WORK

We study the performances of different watermarking algorithms in terms of robustness. Algorithms are chosen to be representatives of different categories such as spatial and transform domain attacks. A new Steganography technique was presented, implemented and analyzed. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This thesis work concluded that the LSB hiding method is the worst case of the proposed method.

REFERNCES

[1] SALH EREN BALCI" ROBUST WATERMARKING OF IMAGES", 2003
[2] Navneet Kumar Mandhani" WATERMARKING USING DECIMAL SEQUENCES" 2004
[3] Mitra Abbasfard" Digital Image Watermarking Robustness: A Comparative Study".
[4] Vivek Kumar Agrawal" PERCEPTUAL WATERMARKING OF DIGITAL VIDEO USING THE VARIABLE TEMPORAL LENGTH 3D-DCT". 2007
[5] Krati vyas, B.L.Pal" A PROPOSED METHOD IN IMAGE STEGANOGRAPHY TO IMPROVE IMAGE QUALITY WITH LSB TECHNIQUE "International Journal of Advanced Research in Computer and Communication Engineering, 2014
[6] Kshetrimayum Jenita Devi" A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", 2013
[7] Peter Hanzlik" Steganography in Reed-Solomon Codes".
[8] KANG LENG CHIEW "STEGANALYSIS OF BINARY IMAGES", 2011
[9] Abbas Cheddad" Steganoflage: A New Image Steganography Algorithm", 2009
[10] VIKAS SAXENA" DIGITAL IMAGE WATERMARKING", 2008
[11] Ms. T MITA KUMARI" IMAGE ADAPTIVE WATERMARKING USING WAVELET TRANSFORM", 2007
[12] Wong Hon Wah "Image Watermarking and Data Hiding Techniques", 2003
[13] YANG, YING "Information Analysis for Steganography and Steganalysis in 3D Polygonal Meshes", 2013
[14] Ingemar J. Cox, Matt L. Miller and Andrew L. McKellips" Watermarking as communications with side information", IEEE, 1999.
[15] Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, Anand Mohan" Secure Spread-Spectrum Watermarking for Telemedicine Applications", Journal of Information Security, 2011
[16] Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey BOURENNANE" A Watermarking of Medical Image: Method Based "LSB", Journal of Emerging Trends in Computing and Information Sciences, 2011
[17] Gouenou COATRIEUX, Catherine QUANTIN, Julien MONTAGNER, Maniane FASSA, François-André ALLAERT, Christian ROUX "Watermarking Medical Images with Anonymous Patient Identification to Verify Authenticity", 2008.