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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Efficient Watermarking Algorithm for Digital Images

Priyanka Arora[1], Mrs. Chandana[2]

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

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

Abstract: This paper presents a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data. We advocate that a watermark should be constructed as an independent and identically distributed Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data.
Most watermarking methods for images and video have been proposed are based on ideas from spread spectrum radio communications, namely additive embedding of a (signal adaptive or non-adaptive) pseudo-noise watermark pattern, and watermark recovery by correlation. Even methods that are not presented as spread spectrum methods often build on these principles. Recently, some scepticism about the robustness of spread spectrum watermarks has arisen, specifically with the general availability of watermark attack software which claim to render most watermarks undetectable. In fact, spread spectrum watermarks and watermark detectors in their simplest form are vulnerable to a variety of attacks. However, with appropriate modifications to the embedding and extraction methods, spread spectrum methods can be made much more resistant against such attacks. In this paper, we systematically review proposed attacks on spread spectrum watermarks. Further, modifications for watermark embedding and extraction are presented to avoid and counterattack these attacks. Important ingredients are, for example, to adapt the power spectrum of the watermark to the host signal power spectrum, and to employ an intelligent watermark detector with a block-wise multi-dimensional sliding correlator, which can recover the watermark even in the presence of geometric attacks.

Keywords: WM (Watermark), SS (spread-spectrum), DWT (Discrete Wavelet Transform).

I. INTRODUCTION

Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. Nowadays, digital watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control, and file reconstruction. The host file is called the "asset", and the bit stream is called the "message". The main specifications of a watermarking system are: Robustness (Against intentional attacks or unintentional ones such as compression), Imperceptibility, and Capacity. Importance of each depends on the application. As a matter of fact there is a trade-off between these factors. Although watermarking in some literature includes visible imprints, here we only mean the invisible embedding of the data.

The media player at the client side can detect this mark and consequently enforce a corresponding e-commerce policy. Recent introduction of a content screening system that uses asymmetric direct sequence spread-spectrum (SS) WMs has significantly increased the value of WMs because a single compromised detector (client player) in that system does not affect the security of the content. In order to compromise the security of such a system without any traces, an adversary needs to break in the excess of 100 000 players for a two-hour high-definition video.
With the widespread use of the Internet, a lot of digital media, including audio, video and image, have been duplicated, modified by anyone easily and unlimitedly.

The copyright protection of the intellectual property of the sensitive or critical digital information is an important legal issue globally. Recently, we have seen the trend of the studies in digital watermarking since the techniques provide the essential mechanism for the ownership authentication.

Background

The art of hiding messages in written text was known to the ancient Greeks as steganography. Many ingenious schemes to achieve that objective have been devised over the centuries. However, the more recent development of computer technology and the proliferation of image and graphics type data have generated the capability and the motivation for electronic watermarking as a means of copyright protection. There exist two basic classes of electronic water marks: fragile and robust. The construction of the robust type is one which is resilient to some image distortions such as pixel or bit tampering, cropping, translation, rotation and shear. At this stage, such a watermark possesses limited immunity against the first three distortions, but the intention is to improve its performance in the future. This should be contrasted with a novel technique involving a fragile watermark. where, by deliberate design, any distortions render the watermark nonrecoverable and this becomes proof of tampering. Both methods use LSB manipulation. Ingenious and effective palette manipulation technique to increase the watermark

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

effectiveness by involving the complete RGB image components. A totally different technique and its variations is reviewed. Its major advantage is its compatibility with the JPEG format, whilst its principal disadvantage is that the watermark recovery requires the presence of the unencoded image.

Use of Watermarking

In recent years image watermarking has become an important research area in data security, confidentiality and image integrity. Despite the broad literature on various application fields, little work has been done towards the exploitation of health-oriented perspectives of watermarking. While the recent advances in information and communication technologies provide new means to access, handle and move medical information, they also compromise their security against illegal access and manipulation.

Sensitive nature of patient's personal medical data necessitates measures for medical confidentiality protection against unauthorized access. Source authentication and data integrity are also important matters relating to health data management and distribution. Data hiding and watermarking techniques can play important role in the field of telemedicine by addressing a range issues relevant to health data management systems, such as medical confidentiality protection, patient and examination related information hiding, access and data integrity control, and information retrieval. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality.

Spread- Spectrum Watermarking Principle

The watermark should not be placed in insignificant regions of the image or its spectrum, since many common signal and geometric processes affect these components. The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum while preserving fidelity. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise.

This problem can be addressed by applying spread-spectrum watermarking which can be easily understood with spread-spectrum communications analogy in which frequency domain of the image is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are treated as noise that the immersed signal must be immune to. In spread-spectrum communications, one transmits a narrowband signal over a much larger bandwidth, such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into single output with high signal-to-noise ratio (SNR). However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins. Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures sufficiently small energy in any single coefficient. A watermark that is well placed in the frequency domain of an image will be practically impossible to see.

1.1 Watermarking Technologies

Audio watermarking schemes rely on the imperfections of the human auditory system (HAS). Numerous data hiding techniques explore the fact that the HAS is insensitive to small amplitude changes, either in the time or frequency domains, as well as insertion of low-amplitude time-domain echoes. Information modulation is usually carried out using: SS or quantization index modulation (QIM). The main advantage of both SS and QIM is that WM detection does not require the original recording and that it is difficult to extract the hidden data using optimal statistical analysis under certain conditions. However, it is important to review the disadvantages that both technologies exhibit. First, the marked signal and the WM have to be perfectly synchronized at WM detection. Next, to achieve a sufficiently small error probability, WM length may need to be quite large, increasing detection complexity and delay.

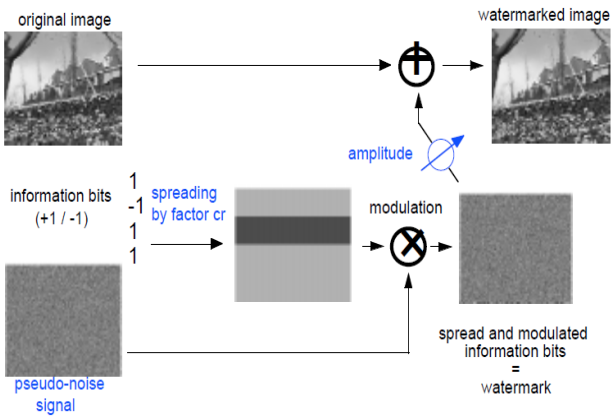

Figure 1 Spread spectrum watermark embedding

Watermarking

Watermarking is a technique used to hide data or identifying information within digital multimedia. Our discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. The digital watermarking process embeds a signal into the media without significantly degrading its visual quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work. Digital watermarking is used to

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. Digital watermarking involves embedding a structure in a host signal to "mark" its ownership. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party. While some watermarks are visible, most watermarks are invisible.

Role of communication in digital watermarking

Digital watermarking is the process of discreetly and robustly embedding information, called a watermark, in media signals to provide some form of added-value; applications include broadcast monitoring, signal tagging, and copy control. The embedding process involves imperceptibly modifying a cover media signal using a secret key and the watermark to produce a composite watermarked signal. The modifications are made such that reliable (i.e., robust) extraction of the of the embedded watermark using the secret key is possible even under a "reasonable" level of distortion applied to the watermarked signal. These distortions, whether intentional or incidental, are known as attacks.

As the research area of digital watermarking matures, one can see some general trends in its development. There was initial work in the use of basic digital signal processing (DSP) strategies for data hiding. Robustness-enhancing strategies were employed using intuition on human perception and basic communications. However, as the area has grown, some theory is emerging. This framework aims to unify much of the past work and establish technical insights for future algorithms. The new mathematical language for describing watermarking borrows tools from statistical communications and information theory.

The art of digital watermarking involves the judicious selection of technological trade-offs to develop an algorithm suitable for a particular application. There are many different factors involved in determining an appropriate compromise; these include cryptographic security, psychology of perception, robustness of extraction, statistical false extraction rates, and complexity. The communication and information theoretic approaches to analysis primarily address the interplay between watermark robustness, capacity and signal strength.

Characteristics of Watermarking

- Unobtrusive
- Perceptually invisible or presence should not interfere with work being protected
- Robust
- Difficult to remove. May be removed sufficient knowledge of the process of insertion. Available of Partial Knowledge-Result in degradation in data fidelity.
- Watermark should be robust to
- Common Signal Processing-should be retrievable even if its operations are applied to the data. For example D/A&A/D conversion, resampling, requantization.
- Common geometric distortions (image and video data) - Watermarks in image and video data should be immune from geometric image operations such as rotation, translation, cropping and scaling
- Collusion and Forgery- Watermark should be robust to collusion by multiple individuals who each posses a watermarked copy of data.
- Watermark should be robust to combining copies of same data set to destroy the watermarks
- Universal – apply same digital watermark algorithm to all three media under consideration.
- Unambiguous- Retrieval of the watermark should unambiguously identify the owner.

II. LITERATURE REVIEW

Ingemar J. Cox illustrated some basic similarities and differences between watermarking and traditional communications. Content (cover data) has historically been viewed as a form of noise and watermarks treated as transmissions with very low signal-to-noise ratios. However, as we have pointed out here, viewing knowledge of the cover data as side information at the transmitter allows the design of more powerful watermark embedding algorithms. In particular, it becomes possible to calculate the robustness of watermarked data to subsequent attacks, and to maximize robustness within a specified distortive constraint. We have further argued that an effective watermark detection region is formed by a K dimensional, two-sheet hyperboloid. But, when it is important to place tight upper bounds on false positive rates, the detection region formed by thresholding a normalized correlation is probably preferable. While these observations promise a significant performance improvement, there is still much room for future work. This might include.

- Analysing more accurate models of the distribution of distortion vectors. In particular, our analysis of the embedding process is based on a simplified model of an independent Gaussian distribution. A more accurate model might be considered in order to improve overall performance. One approach might be to make use of the side information available at the embedded to predict the likely distribution of future distortions to the watermarked data.

Analysing potential performance improvement given side information at the detector. Several existing watermarking algorithms assume knowledge of the original, unwatermarked cover data at the detector. Typically, these algorithms subtract the unwatermarked data from the (possibly) watermarked data to reconstruct the watermark. It may be that more sophisticated algorithms can be developed. [1]

Pooya Monshizadeh Naini, Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. Nowadays, digital

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control, and file reconstruction. In literature, the host file is called the "asset", and the bit stream is called the "message". The main specifications of a watermarking system are: Robustness (Against intentional attacks or unintentional ones such as compression), Imperceptibility, and Capacity. Importance of each depends on the application. As a matter of fact there is a trade-off between these factors. Although watermarking in some literature includes visible imprints, here we only mean the invisible embedding of the data. In this chapter, we will introduce how to use MATLAB to implement image watermarking algorithms. These algorithms include the most famous ones which are widely used in current literature or more complicated approaches are based upon. These are commonly divided into three categories. [2]

Basant Kumar presents a secure spread-spectrum watermarking algorithm for digital images in discrete wavelet transform (DWT) domain. The algorithm is applied for embedding watermarks like patient identification source identification or doctors signature in binary image format into host digital radiological image for potential telemedicine applications. Performance of the algorithm is analysed by varying the gain factor, subband decomposition levels, size of watermark, wavelet filters and medical image modalities. Simulation results show that the proposed method achieves higher security and robustness against various attacks.

To detect the watermark we generate the same pseudorandom matrices used during insertion of watermark by using same state key and determine its average correlation with the two detail subbands DWT coefficients. Average of n correlation coefficients corresponding to each PN matrices is obtained for both LH and HL subbands. Mean of the average correlation values are taken as threshold T for message extraction. During detection, if the average correlation exceeds T for a particular sequence a "0" is recovered; otherwise a "1". The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered.

Performance of the proposed spread-spectrum watermarking algorithm was tested for telemedicine applications. Experiments were carried-out using 8-bit grey scale CT scan image of size 512 × 512. Medical information such as telemedicine origin centre (watermark 1) and doctor's signature (watermark 2) were embedded into host CT scan image as watermarks. These watermarks are in binary image formats which add robustness by allowing recovery of the watermarks even at low correlation between original and extracted watermarks. Strength of watermarking is varied by varying the gain factor in the watermarking algorithm. Perceptual quality of the watermarked radiological image is measured by calculating PSNR between host and watermarked image. At the receiver side, watermark is extracted from the watermarked image. Extracted watermark is evaluated by measuring its correlation with the original watermark.

III.OBJECTIVES

Our proposed research work is to implement a new Method of Embedding, Extraction and Detection of Data in Digital Images. Need of Secure watermarking is to protect copyright data of different companies. It helps to prevent piracy.

Significance of this work is to have a new method of Image watermarking which will be useful for detection and secure digital image.

1. Problem Statement

In this section, some thoughts about the concept of watermarking security are expounded and some definitions are proposed. First, in order to establish a clear line between robustness and security, the following definitions are put forward for consideration:

Definition1. Attacks to robustness are those whose target is to increase the probability of error of the data-hiding channel.

Definition2. Attacks to security are those aimed at gaining knowledge about the secrets of the system (e.g. the embedding and/or detection keys).

At first glance, in the definition of attacks to robustness we could have used the concept of channel capacity instead of the probability of error, but this entails some potential difficulties: for instance, an attack consisting on a translation or a rotation of the watermarked signal is only a de-synchronization, thus the capacity of the channel is unaffected, but depending on the watermarking algorithm, the detector/decoder may be fooled. Another consideration about security, taking into account the above definitions, is the following:

About the intentionality of the attacks: attacks to security are obviously intentional, but not all intentional attacks are threats to security. For instance, an attacker may perform a JPEG compression to fool the watermark detector because he knows that, under a certain JPEG quality factor, the watermark will be effectively removed. Notice that, independently of the success of his attack, he has learned nothing about the secrets of the system. Hence, attacks to security imply intentionality, but the converse is not necessarily true.

About the blindness of the attacks: blind attacks are those which do not exploit any knowledge of the watermarking algorithm. Since attacks to security will try to disclose the secret parameters of the watermarking algorithm, it is easy to realize that they cannot be blind. On the other hand, a non-blind attack is not necessarily targeted at learning the secrets of the system; for instance, in a data-hiding scheme based on binary scalar Dither Modulation (scalar DM), if an attacker adds to each watermarked coefficient a quantity equal to a quarter of the quantization step, the communication is completely destroyed because the bit error probability will be 0.5, although the attacker has learned nothing about the secrets of the systems. Hence, security implies non-blindness, but the converse is not necessarily true.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

2. Objective

1. Study of existing Image watermarking techniques
2. Find problems and weakness in existing methods.
3. Propose a modified method of Data Embedding, Extraction and detection in Digital Images to make it more secure.
4. Develop a scheme for Watermark generation using Random Number.
5. Implement Proposed Algorithm in MATLAB and Perform experiments to validate work by Check Detection Results.

IV. PROPOSED METHODOLOGY

Embedding:

The system that used for the watermark embedding is following: the original image was undergone to the Principal Component Analysis (PCA) transform. The watermark image is mixed with eigenimages within the transform domain. After watermark insertion into eigenimages the watermarked image is reconstructed by means of the inverse PCA transform. The quality of the reconstructed watermarked image is calculated as a function of the embedding system parameters. The peak signal-to-noise ratio (PSNR) and the correlation coefficient are used for image quality calculations.

Extraction:

Watermark extraction assumes to have some original data, e.g. the original image, eigenvectors, etc. Watermark extraction is performed in two different ways – Independent Component Analysis (ICA) is applied to the bands of original and watermarked images and extraction by the backward embedding formula is done.

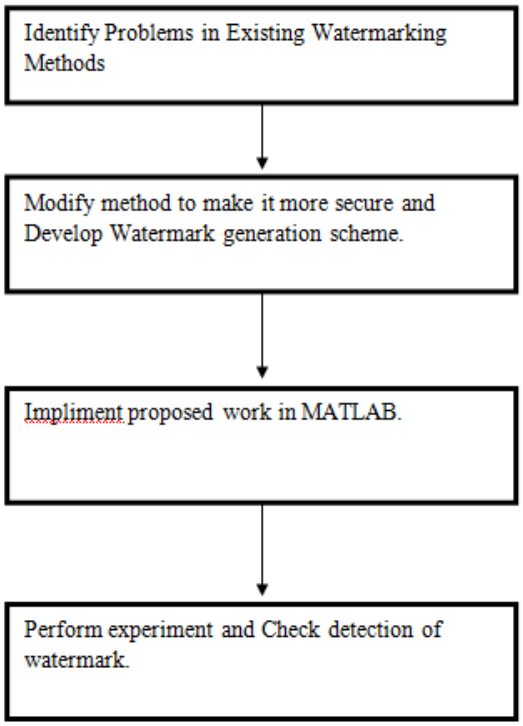

Figure2 Flow Chart

The procedures of an extraction after various attacks, by means of several various filters and the compression that was applied to the watermarked image are realized in purpose to check the watermark robustness against attacks. The quality of the extracted watermark is calculated using the correlation coefficient.

Planning of Work

- One method has been explained above. Study of Existing methods.
- Understand working of Algorithms.
- Propose a new method by modify one of them.
- Resolve issues of Image quality deteriorates.
- Embedding scheme should be good to make it more secure.
- Extraction and Detection should work according to proposed Embedding scheme.
- Understand Command and in build functions of MATLAB
- Implement proposed work in MATLAB.

V. CONCLUSION AND FUTURE WORK

A need for electronic watermarking is developing as electronic distribution of copyright material becomes more prevalent. Above, we outlined the necessary characteristics of such a watermark. These are: delity preservation, robustness to common signal and geometric processing operations, robustness to attack, and applicability to audio, image and video data. To meet these requirements, we propose a watermark whose structure consists of k i.i.d random numbers drawn from a N(0; 1) distribution. We rejected a binary watermark because it is far less robust to attacks based on collusion of several independently watermarked copies of an image. The length of the watermark is variable and can be adjusted to suit the characteristics of the data. For example, longer watermarks may be used for an image that is especially sensitive to large modifications of its spectral coefficients, thus requiring weaker scaling factors for individual components. We recommend that the watermark be placed in the perceptually most significant components of the image spectrum. This maximizes the chances of detecting the watermark even after common signal and geometric distortions. Further, modification of these spectral components results in severe image degradation long before the watermark itself is destroyed. Of course, to insert the watermark, it is necessary to alter these very same coefficients. However, each modification can be extremely small and, in a manner similar to spread spectrum communication, a strong narrowband watermark may be distributed over a much broader image (channel) spectrum. We have not performed an objective evaluation of the image quality, in part because the image quality can be adjusted to any desired quality by altering the relative power of the watermark using the scale factor term. Of course, as the watermark strength is reduced to improve the image quality, the robustness of the method is also reduced. It will ultimately be up to content owners to decide what image degradation and what level of

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

robustness is acceptable. This will vary considerably from application to application.

REFERENCES

[1] Ingemar J. Cox, Matt L. Miller and Andrew L. McKellips, "Watermarking as communications with side information", IEEE
[2] Pooya Monshizadeh Naini," Digital Watermarking Using MATLAB"
[3] Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, Anand Mohan, "Secure Spread-Spectrum Watermarking for Telemedicine Applications"
[4] Mohamed Ali HAJJAJI, "A Watermarking of Medical Image: Method Based LSB"
[5] Gouenou COATRIEUX, "Watermarking Medical Images with Anonymous Patient Identification to Verify Authenticity"
[6] Frank Hartung, "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks"
[7] Luis P´erez-Freire, "Spread Spectrum Watermarking Security", IEEE
[8] Darko Kirovski, "Spread-Spectrum Watermarking of Audio Signals", IEEE
[9] Rinaldi Munir, "Secure Spread Spectrum Watermarking Algorithm Based on Chaotic Map for Still Images"
[10] Gurpreet Kaur, "Image Watermarking Using LSB"
[11] Adrian Sequeira and Deepa Kundur, "Communication and Information Theory in Watermarking: A Survey"
[12] Anatol.Z.Tirkel, "IMAGE WATERMARKING - A SPREAD SPECTRUM APPLICATION"
[13] Pedro Comesa˜na, "Fundamentals of Data Hiding Security and their Application to Spread-Spectrum Analysis"
[14] Zhicheng Wei, "IMAGE WATERMARKING BASED ON GENETIC ALGORITHM"
[15] Benjamin Mathon, "Optimal Transport for Secure Spread-Spectrum Watermarking of Still Images", IEEE