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

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

Secure Digital Images using Hidden Watermarking

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 ways for pictures and video are projected are supported ideas from unfold spectrum radio communications, specifically additive embedding of a (signal adaptative or non-adaptive) pseudo-noise watermark pattern, and watermark recovery by correlation. Even ways that don't seem to be bestowed as unfold spectrum ways typically hinge on these principles. Recently, some skepticism regarding the strength of unfold spectrum watermarks has arisen, specifically with the final availableness of watermark attack software system that claim to render most watermarks undetectable. In fact, unfold spectrum watermarks and watermark detectors in their simplest kind ar at risk of a spread of attacks. However, with applicable modifications to the embedding and extraction ways, unfold spectrum ways may be created way more resistant against such attacks. During this paper, we have a tendency to consistently review projected attacks on unfold spectrum watermarks. Further, modifications for watermark embedding and extraction ar bestowed to avoid and counterattack these attacks. Vital ingredients are, as an example, to adapt the ability spectrum of the watermark to the host signal power spectrum, ANd to use an intelligent watermark detector with a block-wise multi-dimensional slippery correlator, which might recover the watermark even within the presence of geometric attacks.

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

I. INTRODUCTION

Embedding a hidden stream of bits in an exceedingly file is termed Digital Watermarking. The file may be a picture, audio, video or text. Nowadays, digital watermarking has several applications like broadcast watching, owner identification, proof of possession, group action following, content authentication, copy management, device management, and file reconstruction. The host file is termed the "asset", and also the bit stream is termed the "message". The most specifications of a watermarking system are: lustiness (Against intentional attacks or unintentional ones like compression), physical property, and capability. Importance of every depends on the applying. As a matter of reality there's a trade-off between these factors. Though watermarking in some literature includes visible imprints, here we have a tendency to solely mean the invisible embedding of the information.

WITH the expansion of the web, unauthorized repetition and distribution of digital media has ne'er been easier. As a result, the music trade claims a multibillion dollar annual revenue loss because of piracy that is probably going to extend because of peer-to-peer file sharing net communities. One supply of hope for proprietary content distribution on the web lies in technological advances that will offer ways in which of implementing copyright in client-server eventualities. Ancient knowledge protection strategies like scrambling or coding cannot be used since the content should be compete back within the original type, at that purpose, it will perpetually be rerecorded and so freely distributed. A promising answer to the current drawback is marking the media signal with a secret, robust, and insensible watermark (WM).

The media player at the consumer facet will discover this mark and consequently enforce a corresponding e-commerce policy. Recent introduction of a content screening system that uses uneven direct sequence spread-spectrum (SS) WMs has considerably hyperbolic the worth of WMs as a result of one compromised detector (client player) in this system doesn't have an effect on the safety of the content. so as to compromise the safety of such a system with none traces, AN individual has to break within the more than one hundred 000 players for a two-hour high-definition video.

With the widespread use of the web, plenty of digital media, as well as audio, video and image, are duplicated, changed by anyone simply and unlimitedly. The copyright protection of the holding of the sensitive or crucial digital data is a vital legal issue globally. Recently, we've got seen the trend of the studies in digital watermarking since the techniques offer the essential mechanism for the possession authentication.

Recently, with the emergence of electronic network and web, several digital multimedia system knowledge square measure simply traced, hold on and transmitted over the globe, resulting in felonious copy or unauthorized use.

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

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

Digital watermarking has been used wide as a tool for shielding copyright of digital multimedia system knowledge (e.g images). A watermark is inserted into digital pictures in order that it's insensible to an individual. The watermark should even be strong to typical signal process operation like JPEG compression, cropping, resizing, noising, rotation, and so on. Several digital watermarking algorithms for still pictures are planned. Most of them square measure supported unfold spectrum watermarking technique. Unfold spectrum watermarking theme consists of 2 processes. The primary method is embedding of watermark into image. A sequence of watermark bits we would like to cover within the image is unfold by an outsized issue constant, then the amplitude of unfold sequence is amplified, and modulate it with a binary pseudo-noise sequence that behaves as watermark's key. Finally, the modulated signal is more to the image, yielding a watermarked image. The second method is sleuthing of watermark from a take a look at image. This method is well accomplished by multiplying the take a look at image with identical key that was utilized in embedding and so total all of results for every watermark bit. The watermark bits are often recovered by thresholding.

USE OF WATERMARKING

In recent years image watermarking has become a vital analysis space in information security, confidentiality and image integrity. Despite the broad literature on varied application fields, very little work has been done towards the exploitation of health-oriented views of watermarking. whereas the recent advances in data and communication technologies give new suggests that to access, handle and move medical data, they additionally compromise their security against illicit access and manipulation.
Sensitive nature of patient's personal medical information necessitates measures for medical confidentiality protection against unauthorized access. supply authentication and information integrity are necessary matters about health information management and distribution. information concealing and watermarking techniques will play necessary role within the field of telemedicine by addressing a variety problems relevant to health information management systems, like medical confidentiality protection, patient and examination connected data concealing, access and information integrity management, and data retrieval. Medical image watermarking needs extreme care once embedding extra information at intervals the medical pictures as a result of the extra data should not have an effect on the image quality.

Security necessities of medical data derived from strict ethics and legal obligations obligatory 3 obligatory characteristics: confidentiality, dependability and availableness. Confidentiality implies that solely licensed users have access to the knowledge. Dependability has 2 aspects; 1) Integrity: the knowledge has not been changed by non-authorized individuals, and 2) Authentication: a symbol that the knowledge belongs so to the proper supply. Availableness is that the ability of associate system to be employed by entitled users within the traditional scheduled conditions of access and exercise. Authentication, integration and confidentiality ar the foremost necessary problems involved with EPR (Electronic Patient Record) information exchange through open channels. of these necessities may be consummated exploitation appropriate watermarks. General watermarking methodology has to keep the 3 factors (capacity, physical property and robustness) moderately terribly high. Strength is that the ability to recover the info in spites of the attacks within the marked image, physical property is that the invisibleness of the watermark and capability is that the quantity of knowledge which will be embedded. These necessities are clogging one another.
There should be some trade off among these necessities in keeping with the applications. 2 common approaches of knowledge concealing exploitation image covers are spatial domain concealing and rework (frequency) domain concealing. Spatial domain techniques perform information embedding by directly manipulating the picture element values, code values or bit stream of the host image signal and that they ar computationally easy and easy. LSB substitution, patchwork, and unfold spectrum image steganography ar a number of the necessary spatial domain techniques.

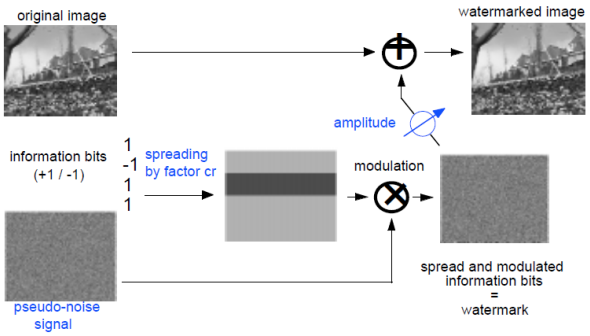

Fig. 1 Spread spectrum watermark embedding

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 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"

DOI 10.17148/IJARCCE.2015.4850

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

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

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.

II. LITERATURE REVIEW

[1] Darko Kirovski, "Spread-Spectrum Watermarking of Audio Signals", IEEE

Watermarking has become a technology of choice for a broad range of multimedia copyright protection applications. Watermarks have also been used to embed format-independent metadata in audio/video signals in a way that is robust to common editing. In this paper, we present several novel mechanisms for effective encoding and detection of direct-sequence spread-spectrum watermarks in audio signals. The developed techniques aim at i) improving detection convergence and robustness, ii) improving watermark imperceptiveness, iii) preventing desynchronization attacks, iv) alleviating estimation/removal attacks, and finally, v) establishing covert communication over a public audio channel. We explore the security implications of the developed mechanisms and review watermark robustness on a benchmark suite that includes a combination of audio processing primitives including: time- and frequency-scaling with wow-and-flutter, additive and multiplicative noise, resembling, requantization, noise reduction, and filtering.

[2] Rinaldi Munir, "Secure Spread Spectrum Watermarking Algorithm Based on Chaotic Map for Still Images"

In this paper, a chaos-based spread spectrum watermarking algorithm is developed in the DCT domain for still image. The most important feature of chaos is its sensitivity to initial conditions. This characteristic makes chaos has been used successfully for secure watermarking and encryption. In our algorithm, we use logistic map to produce pseudo-random sequence. We use the logistic map twice: one is to encrypt the embedded position and other to generate pseudo-noise sequence. The encryption to embedding position can prevent the watermark from removing ilegally, so the security can be improved better. We also use binary meaningful watermark image so that the contents of the watermark is known. The binary image is extracted without using original image. We have also tested robustness of the proposed algorithm against various attacks using common image processing (JPEG compression, cropping, resizing, and noising). Simulations have confirmed that this algorithm is robust against the typical attacks. The extracted watermarks still can be recognized visually.
In this paper a secure spread spectrum watermarking algorithm based on chaotic map for still image has been proposed. This algorithm applies DCT, based on logistic map, and embed watermark into the DCT coefficient. During watermak embedding, the chaotic sequence is used twice: one is to encrypt the embedded position and other to generate pseudo-noise sequence. We also use binary meaningful watermark image. The binary image is extracted without using original image. Simulations have confirmed that this algorithm is robust against several common images processing (JPEG compression, resizing, cropping, and adding noise). The extracted watermarks still can be recognized visually.

[3] Gurpreet Kaur, "Image Watermarking Using LSB"

With the rapid development and wide use of Internet, information transmission faces a big challenge of security. People need a safe and secured way to transmit information. Digital watermarking is a technique of data hiding, which provide security of data. This paper presents a watermarking technique which least significant bits (LSB), its steps and its process with matlab images.
There are different techniques used in watermarking for security of images. Frequency domain, Spatial domain and spread spectrum. In this paper we use spatial domain method LSB for security of images, which is easy and simple and more effective method. Process of LSB is simple when we used LSB in MATLAB. A different image in MATLAB tells different process steps and their result. In future LSB may also use for other type of data and test on different type of images.

III.PROPOSED METHODOLOGY

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

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

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

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.

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.

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. 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

IV. RESULTS

Fig 2 Image after embedding watermark (3000Bits, 4 strength)

Result:

Original watermark similarity appears at index (100) = 2.895422e+001

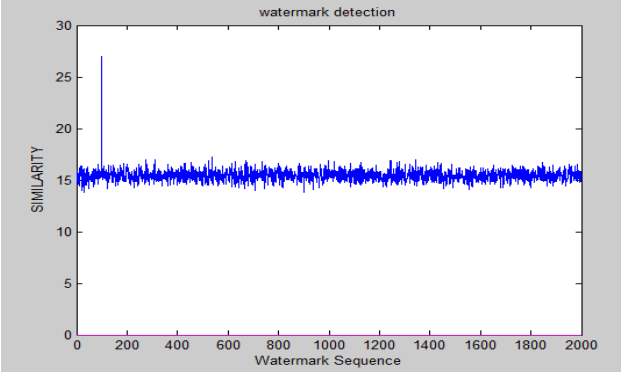

Fig 4 Data Checking

V. CONCLUSION

A need for electronic watermarking is developing as electronic distribution of copyright material becomes a lot of prevailing. Above, we tend to made public the mandatory characteristics of such a watermark. These are: delity preservation, lustiness to common signal and geometric process operations, lustiness to attack, and pertinency to audio, image and video knowledge. to fulfil these necessities, we tend to propose a watermark whose structure consists of k i.i.d random numbers drawn from a N(0; 1) distribution. we tend to rejected a binary watermark as a result of it's so much less sturdy to attacks supported collusion of many severally watermarked copies of a picture. The length of the watermark is variable and may be adjusted to suit the characteristics of the info. for instance, longer watermarks is also used for a picture that's particularly sensitive to giant modifications of its spectral coefficients, so requiring weaker scaling factors for individual parts. we tend to advocate that the watermark be placed within the perceptually most important parts of the image spectrum. This maximizes the probabilities of detection the watermark even when common signal and geometric distortions. Further, modification of those

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

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

spectral parts leads to severe image degradation long before the watermark itself is destroyed. Of course, to insert the watermark, it's necessary to change these exact same coefficients. However, every modification are often very tiny and, during a manner the same as unfold spectrum communication, a powerful narrowband watermark is also distributed over a way broader image (channel) spectrum. we've got not performed Associate in Nursing objective analysis of the image quality, partly as a result of the image quality are often adjusted to any desired quality by sterilization the relative power of the watermark exploitation the size issue term. Of course, because the watermark strength is reduced to enhance the image quality, the lustiness of the strategy is additionally reduced. It'll ultimately be up to content house owners to choose what image degradation and what level of lustiness is suitable. This may vary significantly from application to application.

REFERENCES

[1] N. F. Johnson, and S. Jajodia, "Steganography: Seeing the Unseen", 1998, IEEE Computer.
[2] Piyush Goel, "Data Hiding in Digital Images: A Steganographic Paradigm, 2008
[3] A. Ker, "Steganalysis of Embedding in Two Least-Significant Bits", 2007, IEEE Trans. on Information Forensics and Security.
[4]Kshetrimayum Jenita Devi, "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", 2013.
[5] Philip Bateman, "Image Steganography and Steganalysis", 2008
[6] Hengfu YANG, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution"
[7] Xin Liao, "Embedding in Two Least Significant Bits with Wet Paper Coding"
[8] R M Goudar, "Compression Technique Using DCT & Fractal Compression– A Survey"
[9] J. K. Mandal, "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images through Exclusion of Overflow/Underflow"
[10] Rita Chhikara, "Concealing Encrypted Messages using DCT in JPEG Images"
[11] T. Morkel, "AN OVERVIEW OF IMAGE STEGANOGRAPHY"
[12] Andrew D. Ker, "Improved Detection of LSB Steganography in Grayscale Images"