Volume 6, Issue 12, December 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Practical Approach of Image Watermarking Implemented in MATLAB

Aruna
M.Tech (CSE), JCDM College of Engineering, Sirsa, Haryana, India

Rai Singh
Assistant Professor (CSE), JCDM College of Engineering, Sirsa, Haryana, India

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: Audio watermarking, attack, embedding and extraction, Least significant bits, spread –spectrum.

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. With the growth of the Internet, unauthorized copying and distribution of digital media has never been easier. As a result, the music industry claims a multibillion dollar annual revenue loss due to piracy, which is likely to increase due to peer-to-peer file sharing Web communities. One source of hope for copyrighted content distribution on the Internet lies in technological advances that would provide ways of enforcing copyright in client-server scenarios. Traditional data protection methods such as scrambling or encryption cannot be used since the content must be played back in the original form, at which point, it can always be rerecorded and then freely distributed. A promising solution to this problem is marking the media signal with a secret, robust, and imperceptible watermark (WM). 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.

II. AUDIO WATERMARKING

Audio watermarking is defined as a technique in which the owner specific information or the cover audio tracking information etc. is embedded on to the cover audio signal in such a way that there is no perceptual difference between the original and the resultant audio. The embedded information is referred as the watermark and the resultant

audio is referred as the watermarked audio signal. The embedded information should be extracted/ detected from the watermarked audio whenever required even if the watermarked audio is manipulated to give the feel like Original. The different audio watermarking schemes exploits the deficiency of HAS. Audio watermarking mainly involves the use of two separate algorithms. First is the embedding algorithm and the second is the extraction/detection algorithm. The typical embedding and extraction modules of audio watermarking can be pictorially represented using the following figures.

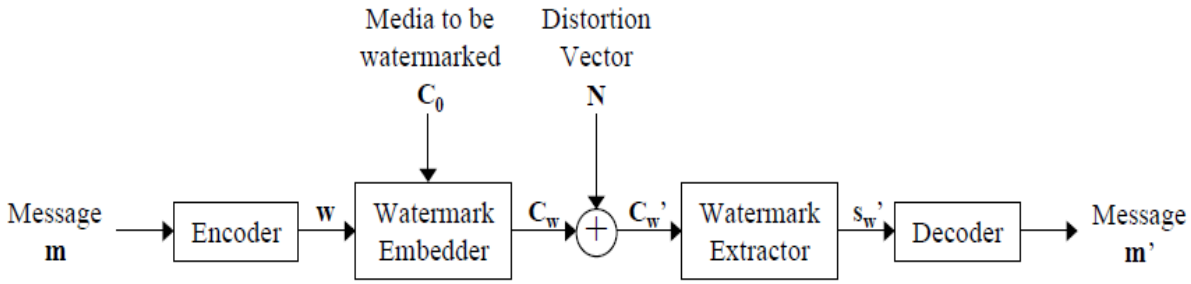

Figure 1: Watermarking as communications

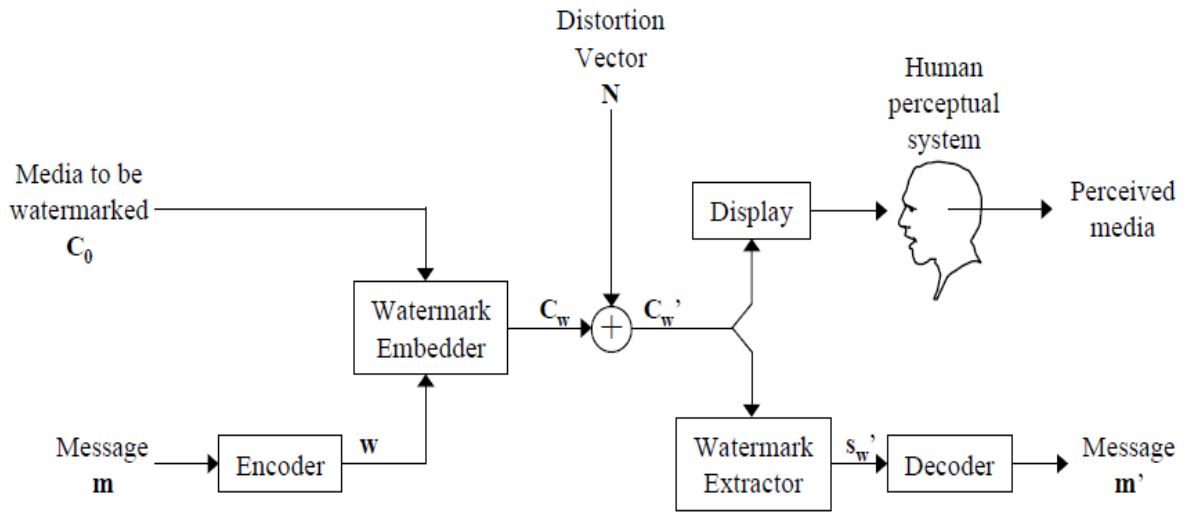

Figure 2: Complete model of watermarking

Depending upon the requirement of original audio and tracing of the copyright information (like ownership protection applications) at the time of authentication /investigation /detection/ extraction, audio watermarking can be mainly categorized into the informed source or uninformed source watermarking. When the destination watermark information (like fingerprinting applications) is to be traced the watermarking schemes are categorized as informed destination or uninformed destination schemes. In principle, whether the original audio information is required or not at the time of extraction/detection of the watermark makes the watermarking schemes as informed or uninformed.

III. LITERATURE REVIEW

[1] Ingmar J. Cox, Matt L. Miller and Andrew L. McKellips, "Watermarking as communications with side information", IEEE. Several authors have drawn comparison between embedded signaling or watermarking and communications, especially spread spectrum communications. We examine the similarities and differences between watermarking and traditional communications. Our 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 which are discussed in detail.

[2] Pooya Monshizadeh Naini," Digital Watermarking Using MATLAB". 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. 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).

[3] Basant Kumar, Harsh Vikram Singh, Surya Pal Singh, Anand Mohan, "Secure Spread-Spectrum Watermarking for Telemedicine Applications". This paper 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 doctor's signature in binary image format into host digital radiological image for potential telemedicine applications. Performance of the algorithm is analyzed by varying the gain factor, sub

band 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.

[4] Mohamed Ali HAJJAJI, "A Watermarking of Medical Image: Method Based LSB". In this paper, they present a new approach for watermarking of medical image that we are trying to adapt to telemedicine. This approach is intended to insert a set of data in a medical image. These data should be imperceptible and robust to various attacks. It's containing the signature of the original image, the data specific to the patient and his diagnostic. The purpose of the watermarking method is to check the integrity and preservation of the confidentiality of patient data in a network sharing. This approach is based on the use the LSB (least significant bits) of the image and tools borrowed from cryptography.

IV. OBJECTIVES & PROPOSED METHODOLOGY

Based on the literature review done and the issues identified along with the main issue of watermarking, the thesis objective is oriented towards improvement of the uninformed source and destination based watermarking schemes with respect to imperceptibility, robustness, security.

Study the existing method.

1. Identify the discrete cosines transform and fast Fourier transform.
2. To solve this problem, the frequency domain of the image or sound at hand 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 thus treated as noise that the immersed signal must be immune to. While we use this methodology to hide watermarks in data, the same rationale can be applied to sending any type of message through media data.
3. We originally conceived our approach by analogy to spread spectrum communications. 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.
4. Similarly, the watermark is spread over very 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 a single output with high signal-to-noise ratio.
5. The result will be generated and display the watermarking image.

V. RESULTS

Embed watermark in Original Image:

Figure 3: Original Image without watermarking

A random watermark sequence has been generated and embedded into above image. A new image will be generated as shown in figure, which is similar to figure, but contains watermark data.

Matlab Command to embed data: SpreadSpectrumEmbed ('1.jpg', '2.jpg', 'wm.seq', 1000, 2)

102 101 98 96 96 99 100 100 103 100 99 97 98 100 98 100 100 101 102 102 102 103 107 110 98
103 101 95 97 99 100 100 102 99 95 95 100 103 98 95 98 94 102 103 101 99 104 110 95 101 101
92 98 97 99 101 100 99 93 95 99 102 102 95 97 94 98 99 97 101 106 102 91 98 100 94 96 96
95 95 100 103 100 98 103 105 101 98 100 89 98 101 93 95 102 100 92 102 104 98 95 91 92 94
93 102 112 105 107 104 102 102 103 98 101 104 101 95 96 102 98 99 93 87 88 88 94 101 90 93
107 104 102 98 98 102 105 120 102 99 109 106 102 109 95 93 95 91 89 87 89 93 98 95 97 95
95 96 96 95 101 108 99 98 103 101 101 103 88 88 91 94 95 94 100 101 97 95 95 95 95 92 92
95 97 93 101 103 103 106 99 93 96 90 91 93 95 95 97 93 95 93 99 95 95 95 96 97 100 95
101 95 95 101 102 93

Figure 4: Image after embedding watermark (1000Bits, 2 strength)

Matlab Command to embed data: SpreadSpectrumEmbed ('1.jpg', '2.jpg', 'wm.seq', 2000, 5)

Figure 5: Image after embedding watermark (2000Bits, 5 strength)

Experiment-1: Extract watermark data from figure and compare it with Original Image:
Matlab Command to extract data:
SpreadSpectrumExtract('2.jpg', '1.jpg', 'wm.seq', 1000, 2)

Result:

Original watermark similarity appears at index(100) = 1.852191e+000

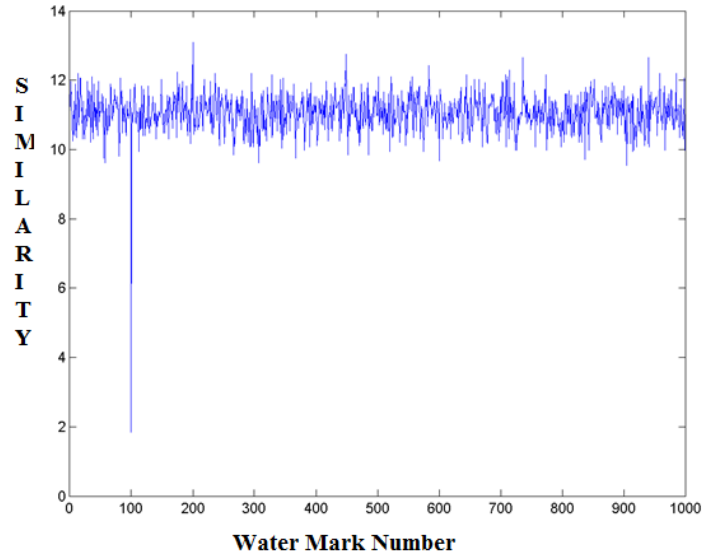

Figure 6: Comparison Result of Experiment 1

It's clear from above result that watermark is presented in suspected image. Similarity at index 100 is: 1.852191

Extracted watermark Data:

1,0,0,1,1,0,0,0,1,0,0,1,0,0,1,0,0,0,0,0,0,1,0,0,0,1,0,1,0,1,0,0,0,0,0,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,0,1,0,0,0,0,0,0,0,0,0,0,1,0,1,1,0,0,1,0,0,0,0,0,0,0,0,
1,1,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,1,1,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
,0,0,0,0,0,0,0,0,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

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

In future LSB may also use for other type of data embedding along with Gaussian Vector and watermark strength can be improved .Analyzing 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.

REFERENCE

[1] Ingmar 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".

