ISSN No. 0976-5697

Volume 4, No. 2, Jan-Feb 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Securing Information Based on Spread-Spectrum using Watermarking

Smt Renuka.S.Mathapati
Dept. of Computer Science
JSS SMI UG & PG Studies
ren_friends@rediff.com

Abstract: Watermarking is a technique used to hide data or identifying information within digital. With the advent of internet, creation and delivery of digital data (images) has grown many fold. With this, issues like protection of rights of the current and proving ownership arises. Digital watermarking came as a technique and a tool to overcome shortcomings of current copyright laws for digital data. To prove ownership and protect right, a watermark is embedded in data but to save watermark from counterfeiters we need to find locations which are invariant to all kind of attacks (rotation, expansion, compression, cropping, filtering and blurring)

Keywords: Watermarking Algorithm, Spread Spectrum, Invisible Watermarking

I. INTRODUCTION

The notion of security in watermarking began to be considered several years ago, although the first attempt at providing a mathematical framework for assessing watermarking security was, which gave rise to other related works [1]. This paper considers the security of spread-spectrum methods for watermarking and data hiding following the same guidelines as in the aforementioned works [2, 3]. The fundamentals of this approach to security assessment can be found in, where the attacks to the security of watermarking and data-hiding methods are defined as those aimed at gaining knowledge about the secret parameters of the system [4]. The key assumptions are that the water marker owns a secret key that he or she repeatedly uses to watermark contents, and an attacker is able to gather several signals (observations) that were watermarked with the same secret key; if the attacker manages to estimate this secret key from the observations at hand, then he or she has completely "broken" the watermarking system [5].

II. OBJECTIVE

To provide security for the authorized user for their data Hackers will not easily find this method to hack. The Client registers with the server database and gets an authenticated user ID and a password to secure the operation performed. The user requests for a connection with the server to send a data securely the client is responded for his request, it shows how the authenticated user ID and the password is searched in the database. After retrieving the information from the database, the client is permitted to access the tool which helps him to send the data securely. The client connects with the other client to share information which should be much secured and no hacking or any type of attacks is possible. We investigate watermarking of digital camera raw images and blind detection of spread-spectrum watermarks in images [6]. We propose straightforward watermark embedding in sensor data combined with a novel detector.

To this end, we extend a detection approach which adaptively combines the components of the image to take advantage of the interpolated and correlated image structure within and between color channels [7].

Watermarking is the process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video for example if the signal is copied, then the information is also carried in the copy [8]. The information to be embedded is called a digital watermark, although in some contents the phrase digital watermark means the difference between the watermarked signal and the cover signal. The client receives the watermarked image and decrypts it. The authentication and security is proved here. Thus the hidden message is retrieved through spread spectrum watermarking.

This paper presents both theoretical and practical analyses of the security offered by watermarking and data hiding methods based on spread spectrum. In this context, security is understood as the difficulty of estimating the secret parameters of the embedding function based on the observation of watermarked signals. On the theoretical side, the security is quantified from an information-theoretic point of view by means of the equivocation about the secret parameters. The main result reveals fundamental limits and bounds on security and provides insight into other properties, such as the impact of the embedding parameters are proposed, and the tradeoff between robustness and security. On the practical side, workable estimators of the secret parameters are proposed and theoretically analyzed for a variety of scenarios, providing a comparison with previous approaches, and showing that the security of many schemes used in practice can be fairly low.

III. PROPOSED METHOD

A. Watermarking Algorithm:

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it is possible to detect the hidden information). An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media; Steganography is sometimes applied in digital watermarking, where two parties communicate a secret message embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file

formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself.

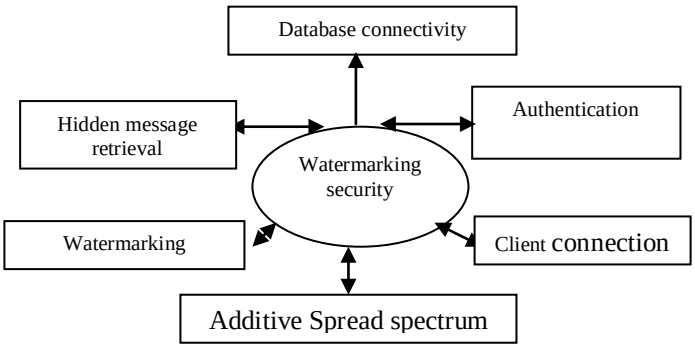


Figure. 1 Watermarking Security

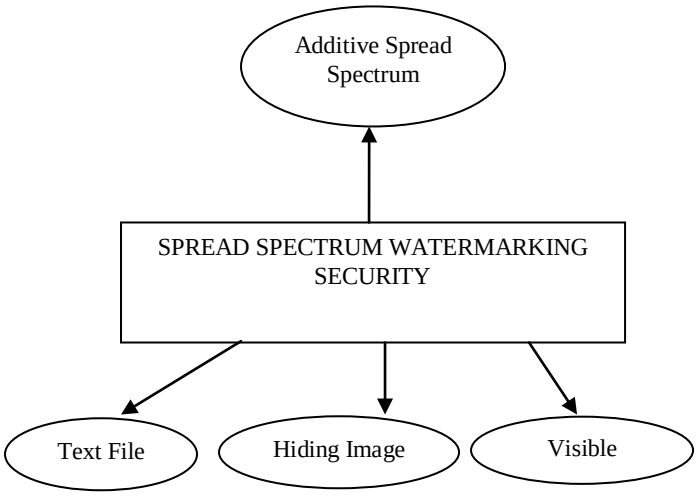
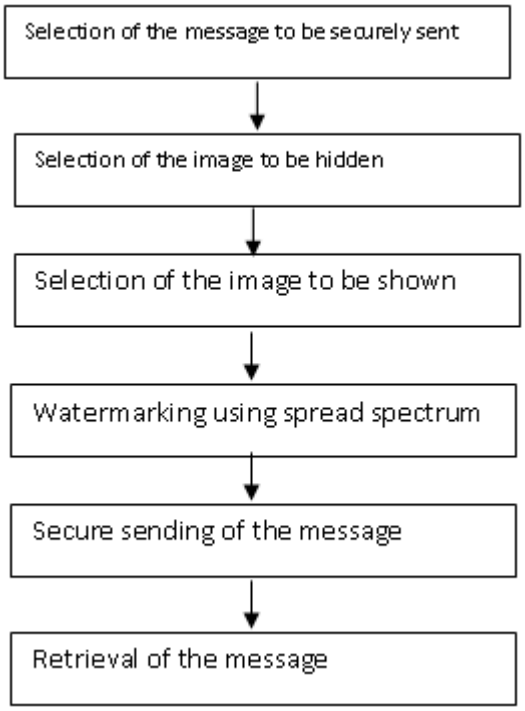


Figure. 2 Additive Spread Spectrum

Process Flow Diagram:



IV. EXISTING SYSTEM

In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

V. PROPOSED SYSTEM

Watermark detection is modeled as hidden hypothesis testing problem where the watermark detector has to decide whether the received signal has been watermarked or not. If this received signal belongs to a certain region of the space, called “acceptance region” (which is dependent on the watermarking method and a secret key), then it is spotted as watermarked.

VI. FUTURE SCOPE

Spread spectrum methods continue to be widely used, as many embedding functions existing these days are based on spreading. Thus, the analysis presented in this is expected to provide useful insights in the watermarking security.

VII. CONCLUSION

The security of spread-spectrum based data hiding methods has been investigated from theoretical and practical points of view. Among the theoretical results obtained in this paper, we would like to remark on the following

a. Under the same conditions of embedding distortion (i.e., keeping constant the power of the watermark), the decrease of the embedding rate (equivalently, the increase of) has a harmful impact on the security level. In limiting cases of zero-rate watermarking, known for being robust to blind attacks, the penalty for ignoring the embedded messages becomes negligible, representing a serious threat to the security of the system.
b. A tradeoff between security and robustness has been shown to exist in the methods that perform host rejection. For the schemes studied in this paper, which cover a wide range of the spread-spectrum schemes considered in the literature, host rejection can significantly decrease the security level of plain spread spectrum.

VIII. REFERENCES

[1] L.Perez-Freire, “Digital watermarking security,” Ph.D. dissertation, University of Vigo, Spain, 2008

[2] L.Perez-Freire, P.Moulin, and F.P ‘erez-Gonz’ alez, “Security of Spread-spectrum based data hiding” in ‘Security, Steganography, and Watermarking of Multimedia Contents IX, Edward J. Delp III and P.W.Wong.Eds,vol.6505 San Jose, California, USA: SPIE, January 2007.

[3] Y.Lee, H.Kim and Y.Park, “A new data hiding scheme for binary image authentication with small image distortion” ,Inform.Sci 2009.

[4] C.D. Vleeschouwer, J.F.Delaigle and B.Macq, "Invisibility and application functionalities in perceptual watermarking" –An overview, Proc. IEEE 90 2002 64-77.

[5] P.Moulin and A.Ivanovic, "The zero-rate spread-spectrum watermarking game," IEEE Transactions on Signal Processing, vol 51, no.4,pp.1098-1117, April 2003.

[6] H.S.Malvar and D.A.F.Florencio, "improved Spread Spectrum : a new modulation technique for ro "bust watermarking," IEEE Transactions on Signal Processing, vol.51, no.4,pp.898-905, April 2003.

[7] S.P.Maity and S.Maity, "Multistage spread spectrum watermark detection technique using fuzzy logic", IEEE Signal Proc, Letters 16 2009 245-248.

[8] A.Hyvarinen, J.Karhunen, and E. Oja, "Independent Component Analysis, ser. Adaptive and learning systems for signal processing, communications" and control., John Wiley & Sons,2001.