Signal Processing: *Image Communication* 39 (2015) 17–25

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

journal homepage: www.elsevier.com/locate/image

# Secure spread-spectrum data embedding with PN-sequence masking

Ming Li, Yanqing Guo, Bo Wang *, Xiangwei Kong

*School of Information and Communication Engineering, Dalian University of Technology, Dalian, Liaoning 116024, PR China*

ARTICLE INFO

*Article history:*
Received 21 January 2015
Received in revised form
30 July 2015
Accepted 30 July 2015
Available online 10 August 2015

*Keywords:*
Data hiding
Information hiding
Pseudo-noise masking
Signal-to-interference-plus-noise ratio (SINR)
Spread-spectrum embedding
Steganography

ABSTRACT

Conventional additive spread-spectrum (SS) data embedding has a dangerous security flaw that unauthorized receivers can blindly extract hidden information without the knowledge of carrier(s). In this paper, pseudo-noise (PN) masking technique is adopted as an efficient security measure against illegitimate data extraction. The proposed PN-sequence masked SS embedding can offer efficient security against current SS embedding analysis without inducing any additional distortion to host nor notable recovery performance loss. To further improve recovery performance, optimal carrier design for PN-masked SS embedding is also developed. With any given host distortion budget, we aim at designing a carrier to maximize the output signal-to-interference-plus-noise ratio (SINR) of the corresponding maximum-SINR linear filter. Then, we present jointly optimal carrier and linear processor designs for PN-masked SS embedding in linearly modified transform domain host data. Finally, PN-masked multi-carrier/multi-message SS embedding is studied as well. The extensive experimental studies confirm our analytical performance predictions and illustrate the benefits of the designed PN masked optimal SS embedding.



## 1. Introduction

Information hiding, which is also called as digital data embedding, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio [1,2]. Applications may vary from annotation, copyright-marking, and watermarking to single-stream media merging (text, audio, image) and covert communication [3–8]. As a general encompassing comment, different applications of information hiding, such as the ones identified above, require different satisfactory tradeoffs between the following four basic attributes of data hiding [9]: (i) payload – information delivery rate; (ii) robustness – hidden data resistance to noise/disturbance; (iii) transparency – low host distortion for concealment purposes; and (iv) security – inability by unauthorized users to detect/access the covert communication channel.

The data hiding performance in terms of above four attributes depends directly on how the data is inserted in the host. Therefore, it is a crucial step to determine the embedding process in the design of a data hiding system. Data embedding can be performed either directly in the time (audio) or spatial (image) domain [10–14] or in a transform domain [15–26]. While direct embedding in the original host signal domain may be desirable for system complexity purposes, embedding in a transform domain may take advantage of the particular transform domain properties [27] and enables the powerful notion of spread-spectrum

* Corresponding author.
*E-mail addresses:* mli@dlut.edu.cn (M. Li), guoyq@dlut.edu.cn (Y. Guo), bowang@dlut.edu.cn (B. Wang), kongxw@dlut.edu.cn (X. Kong).

http://dx.doi.org/10.1016/j.image.2015.07.014
0923-5965/

(SS) data embedding when the secret signal is spread over a wide range of host frequencies [28–32].

In this paper, we focus our attention on additive SS embedding in transform domain host. In direct analogy to SS digital communication systems [33], conventional additive SS embedding methods use an equal-amplitude modulated carrier/signature to deposit one information symbol across a group of host data coefficients or a linearly transformed version of the host data coefficients. Recently, a dangerous security flaw of SS embedding has been alerted and investigated. Embedding a number of information symbols with a same carrier will create a strong basis/subspace of the hidden signal which can be tracked and analyzed. Therefore, even without the knowledge of carrier (s), unauthorized receivers can still blindly extract the embedded data by blind signal separation (BBS) methods [34–37] or novel iterative generalized least square (IGLS) approaches [38,39]. The illegitimate blind hidden data extraction has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context [34–37]. Thus, it raises the concerns of making SS embedding more difficult to be extracted by the illegitimate users. Two interesting SS embedding schemes were proposed in [40] which attempt to withstand SS embedding analysis by using random-like amplitudes. However, these SS embedding schemes sacrifice recovery performance to enhance the security and consequently are sensitive to noise which would lead to high recovery error rates by intended recipients. More importantly, information leakage cannot be fully prevented because information symbols are still embedded by the same carrier.

Pseudo-noise (PN) masking technique has been proven to be an effective technique against unauthorized data collection (eavesdropping) in the context of secure wireless communications. Typical examples of PN masking technique are military-grade communications and global-positioning systems (GPS). In this work, we first develop a PN-masked secure SS embedding approach in which the embedded SS single is scrambled by random-like PN masks such that no subspace of embedded signal can be found and tracked in the data-embedded host. With our proposed PN masked SS embedding scheme, the performance in terms of recovery bit-error-rate (BER) at the intended receiver is maintained at almost the same level as the conventional SS embedding (i.e. almost no performance loss), while the unauthorized users will have BER close to 0.5 (i.e. almost perfect security). Since the proposed PN masked SS embedding schemes can efficiently minimize the likelihood that embedded data are "stolen" by the unauthorized users, they are suitable for the applications with high security requirement, such as steganography and covert communications.

It should also be understood that the host, which acts as a source of interference to the secret message of interest, is known to the message embedder. Such knowledge can be exploited appropriately to facilitate the task of the blind receiver at the other end and minimize the recovery error rate for a given host distortion level, minimize host distortion for a given target recovery error rate, maximize the Shannon capacity of the covert channel, etc. By exploiting the knowledge of the second order statistics (SOS) of host, the recently presented Gkizeli–Pados–Medley eigen-design optimal carrier [29,30] can maximize the signal-to-interference-noise-ratio (SINR) at the output of the corresponding maximum-SINR linear filter. Benefiting from the legacy of [29,30], the optimal carrier design for PN-masked SS embedding is also studied.

The rest of the paper is organized as follows. Section 2 briefly reviews the prior art on additive SS embedding. PN-masked SS embedding is present in Section 3. These results are generalized to multi-carrier embedding in Section 4. Section 5 is devoted to experimental studies and comparisons. A few concluding remarks are drawn in Section 6.

The following notation is used throughout the paper. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{R}$ denotes the set of all real numbers; $()^T$ denotes matrix transpose; $\mathbf{I}_L$ is the $L \times L$ identity matrix; sgn$\{\cdot\}$ denotes zero-threshold quantization; $\mathbb{E}\{\cdot\}$ represents statistical expectation; $\|\cdot\|$ is vector norm.

## 2. Prior art of additive SS embedding

Consider a host image $\mathbf{H} \in \mathcal{M}^{N_1 \times N_2}$ where $\mathcal{M}$ is the finite image alphabet and $N_1 \times N_2$ is the image size in pixels. Without loss of generality, the image $\mathbf{H}$ is partitioned into $M$ local non-overlapping blocks of size $N_1 N_2/M$. Each block, $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_M$, is to carry one hidden information bit $b_i \in \{\pm 1\}$, $i = 1, 2, \ldots, M$, respectively. Embedding is performed in a 2-D transform domain $\mathcal{T}$ (such as the discrete cosine transform and a wavelet transform). After transform calculation and vectorization (for example by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_i) \in \mathbb{R}^{N_1 N_2/M}, i = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_i)$ we choose a fixed subset of $L \le N_1 N_2/M$ coefficients (bins) to form the final host vectors $\mathbf{x}_i \in \mathbb{R}^L$, $i = 1, 2, \ldots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

To draw a parallelism with SS communication systems, conventional SS embedding treats embedded message as the SS signal of interest transmitted through a noisy "channel" (the host). The disturbance to the SS signal of interest is the host data themselves plus potential external noise due to physical transmission of the watermarked data and/or processing/attacking. In particular, conventional additive SS embedding is carried out in the transform domain by

$$\mathbf{y}_i = A b_i \mathbf{s} + \mathbf{x}_i + \mathbf{n}_i, \quad i = 1, \ldots, M, \tag{1}$$

where information bit $b_i \in \{\pm 1\}$ is embedded in the transform domain host vector $\mathbf{x}_i \in \mathbb{R}^L$ via additive SS embedding by means of a (normalized) spreading sequence (carrier/signature) $\mathbf{s} \in \mathbb{R}^L$, $\|\mathbf{s}\| = 1$, with a corresponding embedding amplitude $A > 0$. For the sake of generality, $\mathbf{n}_i$ represents potential external white Gaussian noise[1] of mean $\mathbf{0}$ and autocorrelation matrix $\sigma_n^2 \mathbf{I}_L$, $\sigma_n^2 > 0$.

In an effort to reduce the interference effect of the host signal, the host vectors $\mathbf{x}_i$, $i = 1, \ldots, M$, can be steered away from the embedding carrier using an operator of the form

[1] Additive white Gaussian noise is frequently viewed as a suitable model for quantization errors, channel transmission disturbances, and/or image processing attacks.