Obtain a Hidden Data from Digital Media

Syed Abdul Wahab Bokhari, Dr.K.V.Subba Reddy Institute of Technology, syedwahabbokhari@gmail.com, Shaik. Imran Pasha, Assistant Professor in Dept of CSE

Abstract—We consider the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video). We develop a novel multicarrier/ signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. We considered the problem of blindly extracting unknown messages hidden in image hosts via multi-carrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available.

I.INTRODUCTION

Digital data embedding in digital media is an information technology field of rapidly growing commercial as bwell as national security interest. Applications may vary from bannotation, copyright-marking, and watermarking, to singlestream media merging (text, audio, image) and covert communication [1]. Covert communication or steganography, which literally means "covered writing" in Greek, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio, to establish secret communication between trusting parties and conceal the existence of embedded data [5]-[9]. 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. (*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 communication channel. In this work, we focus our attention on the blind recovery of secret data hidden in medium hosts via multi-carrier/signature direct-sequence spread-spectrum (DS-SS) transform domain embedding [13]-. Neither the original host nor the embedding carriers (signatures or spreading sequences) are assumed known (fully blind data extraction). This blind hidden data extraction problem has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context. However, ICA-based BSS algorithms are not effective in the presence of correlated signal

interference as is the case in SS multimedia embedding and degrade rapidly as the dimension of the carrier (signature) decreases relative to the message size. In , an iterative generalized least squares (IGLS) procedure was developed to blindly recover unknown messages hidden in image hosts via SS embedding. The algorithm has low complexity and strong recovery performance. However, the scheme is designed solelyfor *single-carrier* SS embedding where messages are hidden with one signature only and is not generalizable to the *multi-carrier* case. In this paper, we develop a novel multi-carrier iterative generalized least squares (M-IGLS) algorithm for SS hidden data extraction that, to the best of the authors' knowledge, appears for the first time in the broad communication theory and systems literature. The rest of the paper is organized as follows. we present the signal model for the multi-carrier SS embedding procedure and formulate the problem of active SS data extraction.

The following notation is used throughout the paper. Boldface

lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; R denotes the set of all real numbers; T denotes matrix transpose; Tr is matrix trace; IL is the L identity matrix; sgn denotes zero-threshold quantization; and E represents statistical expectation. Finally, k, and kF are the scalar magnitude, vector norm, and matrix Frobenius norm, respectively.

II.EMBEDDING AND EXTRACTION

Consider a host image H ∈ MN1×N2 where M is the finite image alphabet and N1 ∓ N2 is the image size in pixels. Without loss of generality, the image H is partitioned into M local non-overlapping blocks of size N1N2 M . Each block, H1,H2, ...,HM, is to carry K hidden information bits (KM bits total image payload). Embedding is performed in a 2-D transform domain T (such as the discrete cosine transform, a wavelet transform, etc.).

We consider K distinct message bit sequences, {bk(1), bk(2), . . . , bk(M)}, k = 1, 2, . . . ,K, bk(m) m = 1, . . . ,M, each of length M bits. The K message sequences may be to be delivered to K distinct corresponding recipients or they are just K portions of one large message sequence to be transmitted to one recipient. In particular, the mth bit from each of the K sequences, b1(m), . . . , bK(m), is simultaneously hidden in the mth transform-domain

host vector x(m) via additive SS embedding by means of K spreading sequences (carriers) sk ∈ RL, kskk = 1, k = 1, 2, . . . ,K,

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m)\mathbf{s}_k + \mathbf{x}(m) + \mathbf{n}(m),\ m = 1, 2, \ldots, M,$$

with corresponding amplitudes Ak > 0, k = 1, . . . ,K. For the sake of generality, n(m) represents potential external white Gaussian noise1 of mean 0 and autocorrelation matrix _2n IL, _2n> 0. It is assumed that bk(m) behave as equi-probable binary random variables that are independent in m (message bit sequence) and k (across messages). The contribution of each individual embedded message bit bk to the composite signal is Akbksk and the block mean-squared distortion to the original host data x due to the embedded k message alone is

$$\mathcal{D}_k = \mathbf{E}\{\|A_k\mathbf{s}_k b_k\|^2\} = A_k^2,\ k = 1, 2, \ldots, K.$$

The intended recipient of the kth message with knowledge of the kth carrier sk can perform embedded bit recovery by looking at the sign of the output of the minimum-mean-squareerror (MMSE) filter wMMSE,k = R−1 y sk,

Formulation of the Extraction Problem

To blindly extract spread-spectrum embedded data from a given host image, the analyst needs first to convert the host to observation vectors of the form of y(m), m = 1, . . . ,M, in (1). This requires knowledge of (*i*) the partition, (*ii*) transform domain, (*iii*) subset of coefficients, and (*iv*) number of carriers used by the embedder. The host image partition (and block size N1N2/M in our notation) may be estimated by neighboringpixels difference techniques as in [30]. Regarding the subset of coefficients used in embedding, the conservative approach is to assume that all coefficients are used, except maybe the dc value, and set accordingly L = N1N2/M − 1. The number of carriers K can be estimated by SS signal population identification algorithms.

Then, we can further reformulate SS embedding as

$$\begin{aligned} \mathbf{y}(m) &= \sum_{k=1}^{K} b_k(m)\mathbf{v}_k + \mathbf{z}(m) \\ &= \mathbf{V}\mathbf{b}(m) + \mathbf{z}(m),\ m = 1, \ldots, M, \end{aligned}$$

For notational simplicity, we can write the whole observation data in the form of one matrix

$$\mathbf{Y} = \mathbf{V}\mathbf{B} + \mathbf{Z}$$

HIDDEN DATA EXTRACTION

If Z were to be modeled as Gaussian distributed, the joint maximum-likelihood (ML) estimator of V and decoder of B would be

$$\hat{\mathbf{V}}, \hat{\mathbf{B}} = \arg \min_{\substack{\mathbf{B} \in \{\pm 1\}^{K \times M} \\ \mathbf{V} \in \mathbb{R}^{L \times K}}} \|\mathbf{R}_x^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2$$

The global GLS-optimal message matrix bB in (9) can be computed independently of bV by exhaustive search over all possible choices under the criterion function kR

$$\hat{\mathbf{V}}_{\text{final}}, \hat{\mathbf{B}}_{\text{final}} = \arg \min_{(\mathbf{V},\mathbf{B}) \in \left\{(\bar{\mathbf{V}}_1, \bar{\mathbf{B}}_1), \ldots, (\bar{\mathbf{V}}_P, \bar{\mathbf{B}}_P)\right\}} \|\hat{\mathbf{R}}_y^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2.$$

Returning to the proposed data extraction algorithm, we understand that with arbitrary initialization convergence of the

M-IGLS procedure described in Table I to the optimal GLS solution of (9) is not guaranteed in general. Extensive experimentation with the algorithm in Table I indicates that, for sufficiently long messages hidden by each carrier (M = 4Kbits or more, for example), satisfactory quality message decisions bB can be directly obtained. However, when the message size is small, M-IGLS may very well converge to inappropriate points/solutions. The quality (generalized-least-squares fit) of

the end convergence point depends heavily on the initialization point and arbitrary initialization -which at first sight is unavoidable for blind data extraction- offers little assurance that the iterative scheme will lead us to appropriate, "reliable" (close to minimal generalized least-squares fit) solutions. To that respect, re-initialization and re-execution of the M-IGLS procedure, say P times, is always possible. To assess which of the P returned solutions, say (bV1,bB1), . . . , (bVP ,bBP), has superior generalized-least-squares fit, we simply feed (bVi,bBi)

to (9) (using bRy in place of Rz) .

III. RESULTS

A technically firm and keen measure of quality of a hiddenmessage extraction solution is the difference in bit-error-rate (BER) experienced by the intended recipient and the analyst.The intended recipient in our studies may be using any of the following three message recovery methods: (*i*) Standard carrier matched-filtering (MF) with the known carriers sk, k = 1, ...,K; (*ii*) sample-matrix-inversion MMSE (SMI-MMSE) filtering with known carriers sk and estimated host autocorrelation matrix bRy (see (3)); and (*iii*) ideal MMSE filtering with known carriers sk and known true host autocorrelation matrix Rx, which serves as the ultimate performance bound reference for all methods. In terms of blind extraction (neither sk nor Rx known), we will examine: (*iv*) The developed MIGLS algorithm in Table I with P = 20 re-initializations and, for comparison purposes, the performance of two typical independent component analysis (ICA) based blind signal separation (BSS) algorithms (*v*) FastICA lated by PSNR , 20log10(255) − 10log10(PK k=1 Dk/64). Another metric that reflects the relationship between host and embedding distortion is the block document-to-watermark power ratio (DWR) defined as DWR , 10log10_2x−10log10(PK k=1 Dk) where _2x , Tr{Rx} is the (total) host block variance. The value of _2x depends on the nature of each host image and is provided in each experiment that we run (see figure captions) to facilitate translation by the reader between MSE and DWR if desired. For the sake of generality, in our studies we also incorporate white Gaussian noise of variance _2n= 3dB.

An encompassing conclusion over all executed experiments is that M-IGLS remains a most effective technique to blindly extract hidden messages, while extraction becomes more challenging as the length of the hidden message per used embedding carrier decreases or the number of hidden messages (number of used carriers) increases. It is also worth pointing out that, in these experimental studies, M-IGLS may outperform (in moderate to high distortion values) SMI-MMSE in which the true carriers/signatures are known. This is because SMI-MMSE suffers from performance degradation due to small-sample-support adaptation (estimation of matrix Ry). The unsatisfactory performance of the ICA-based methods is due to the interference from high-amplitude (low-frequency). host coefficients. To demonstrate this point, in Fig. 10 we repeat the exact same experiment of Fig. 2 using this time only the L = 20 highest-frequency DCT coefficients as our host vector. It can be observed that, in this moderate host interference environment, ICA-based methods can provide satisfactory

performance (not superior to M-IGLS, however). Of course, we may not expect that data are always embedded exclusively in low-amplitude coefficients alone.

We considered the problem of blindly extracting unknown messages hidden in image hosts via multi-carrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. We developed a low complexity multi-carrier iterative generalized least-squares n(M-IGLS) core algorithm. Experimental studies showed that M-IGLS can achieve probability of error rather close to what may be attained with known embedding signatures and known original host autocorrelation matrix and presents itself as an effective countermeasure to conventional SS data embedding/hiding5.

Fig. 1. 512 × 512 gray-scale Boat image.

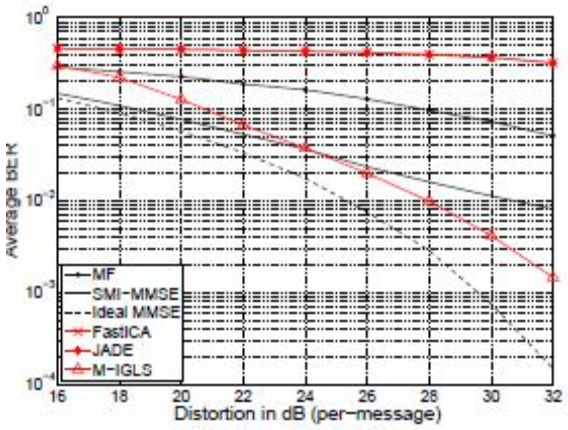

Fig. 2. Average BER versus per-message block distortion (256×256 Baboon,L = 63, K = 4 messages of 1Kbit each, σ_2= 3dB, σ_{2x}= 45.45dB).

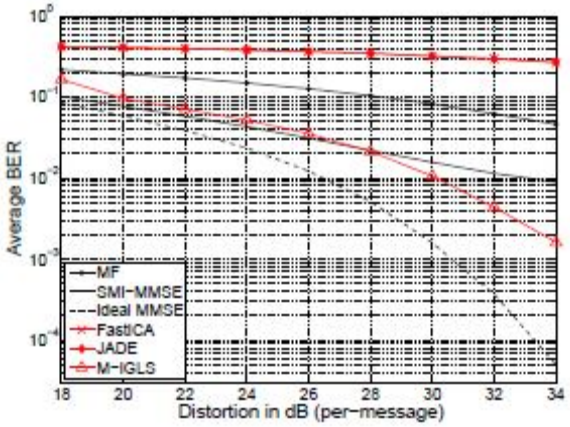

Fig. . 3 . Average BER versus per-message block distortion (256 × 256 F16 Aircraft, L = 63, K = 8 messages of 1Kbit each, σ_{2n} = 3dB, σ_{2x}=46.23dB

Fig. 4. 256 × 256 gray-scale Aircraft image.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1079-1107, July 1999.

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[6] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.

[8] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*. New York, NY: Plenum, 1984, pp. 51-67.

[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.

[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2706-2722, June 2008.

[11] *Federal plan for cyber security and information assurance research and development*, Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.

[12] R. Chandramouli, "A mathematical framework for active steganalysis," *ACM Multimedia Systems Special Issue on Multimedia Watermarking*, vol. 9, pp. 303-311, Sept. 2003.

[13] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Proc.*, vol. 51, pp. 898-905, Apr. 2003.

[14] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Proc.*, vol. 6, pp. 1673-1687, Dec. 1997.

[15] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Proc.*, vol. 9, pp. 55-68, Jan. 2000.

[16] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, pp. 273-284, Sept. 2001.