Extracting Spread-Spectrum Hidden Data from Digital Media

S. Anil Kumar[1], N. Sowmya Srivalli[2], M.Lavanya[3], V.Sureka[4], P. Revanth Kumar[5]

[1]*Asst.Profeesor, CSE, Tirumala Enginering College, NRT, AP, India,* ***sakmba.k@gmail.com***
[2]*B.Tech, CSE, Tirumala Enginering College, NRT, AP, India,* ***sowmyasrivalli2564@gmail.com***
[3]*B.Tech, CSE, Tirumala Enginering College, NRT, AP, India,* ***lavanya71.miriyala@gmail.com***
[4]*B.Tech, CSE, Tirumala Enginering College, NRT, AP, India,* ***vankayalasurekha498@gmail.com***
[5]*B.Tech, CSE, Tirumala Enginering College, NRT, AP, India,* ***palepu.revanthkuman4896@gmail.com***

Abstract

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. Experimental studies on images show that the developed algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers and host autocorrelation matrix.

Index Terms*:* Authentication, annotation, blind detection, covert communications, data hiding, information hiding, spread-spectrum mbedding, steganalysis, steganography, watermarking..

---------- *** ----------

1. INTRODUCTION

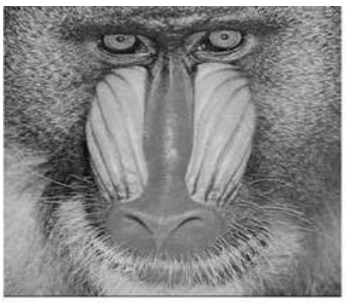
DIGITAL data embedding in digital media is an information technology field of rapidly growing commercial as well as national security interest. Applications may vary from annotation, copyright-marking, and watermarking, to single-stream media merging (text, audio, image) and covert communication. In annotation, secondary data are embedded into digital multimedia to provide a way to deliver side information for various purposes; copyright-marking may act as permanent "iron branding" to show ownership; fragile watermarking may be intended to detect future tampering; hidden low-probability-to-detect (LPD) watermarking may serve as identification for confidential data validation or digital fingerprinting for tracing purposes. 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.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.

While passive detection -only of the presence of embedded data is being intensively investigated in the past few years, active hidden data extraction is a relatively new branch of research. In blind extraction of SS embedded data, the unknown host acts as a source of interference/disturbance to the data to be recovered and, in a way, the problem parallels blind signal separation (BSS) applications as they arise in the fields of array processing, biomedical signal processing, and code - division multiple-access (CDMA) communication sys-tems. Under the assumption that the embedded secret messages are independent identically distributed (i.i.d.) random sequences and independent to the cover host, independent com-ponent analysis (ICA) may be utilized to pursue hidden data extraction. 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

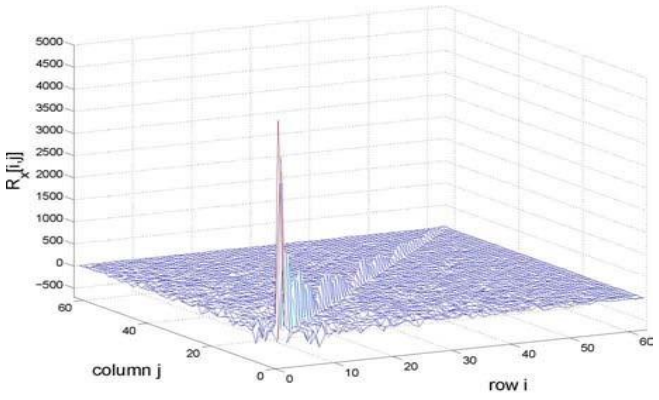
designed solely for *single-carrier* SS embedding where messages are hidden with one signature only and is not generalizable to the *multicarrier* case. Realistically, an embedder would favor *multicarrier* SS transform-domain embedding to increase security and/or payload rate.

2. MULTICARRIER SS EMBEDDING AND EXTRACTION: PROBLEM FORMULATION

Consider a host image. $\mathbf{H} \in \mathbf{M}^{n1\,X\,n2}$ Where **M** is finite image alphabet and **N1X N2** is the image size in pixels. Without loss of generality, the image H is partitioned into **M** local non overlapping blocks of size $\frac{N1XN2}{M}$.



(a)



(b)

It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

The autocorrelation matrix of the host data **X** is an important statistical quantity for our developments and is defined as

$$\mathbf{Y} = \mathbf{VB} + \mathbf{Z}$$

It is easy to verify that in general; that is, R_x is *not* constant-value diagonal or "white" in field language. For example,8 8 DCT with 63-bin host data formation (excluding only the dc coefficient) for the 256 256 gray-scale Baboon image in Fig. 1(a) gives the host autocorrelation matrix in R_x

$$\mathbf{R}_{\mathbf{x}} \triangleq \mathbb{E}\{\mathbf{x}\mathbf{x}^T\} = \frac{1}{M}\sum_{m=1}^{M} \mathbf{x}(m)\mathbf{x}(m)^T$$

3. HIDDEN DATA EXTRACTION

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

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

Where multiplication R_Z by can be interpreted as prewhitening of the compound observation data. If Gaussianity of is not to be invoked, then can be simply referred to as the joint generalized least-squares (GLS) solution2 of **V** and **B**.

$$\hat{\mathbf{B}} = \arg \min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2$$

The global GLS-optimal message matrix **B** in can be computed independently of by exhaustive search over all possible choices under the criterion function

MULTICARRIER ITERATIVE GENERALIZED LEAST-SQUARES DATA EXTRACTION

1) $d := 0$; initialize $\hat{\mathbf{B}}^{(0)} \in \{\pm 1\}^{K \times M}$ arbitrarily.
2) $d := d + 1$;
$\hat{\mathbf{V}}^{(d)} := \mathbf{Y}(\hat{\mathbf{B}}^{(d-1)})^T \left[(\hat{\mathbf{B}}^{(d-1)})(\hat{\mathbf{B}}^{(d-1)})^T\right]^{-1}$;
$\hat{\mathbf{B}}^{(d)} := \text{sgn}\left\{\left((\hat{\mathbf{V}}^{(d)})^T \hat{\mathbf{R}}_{\mathbf{y}}^{-1}(\hat{\mathbf{V}}^{(d)})\right)^{-1}(\hat{\mathbf{V}}^{(d)})^T \hat{\mathbf{R}}_{\mathbf{y}}^{-1}\mathbf{Y}\right\}$.
3) Repeat Step 2 until $\hat{\mathbf{B}}^{(d)} = \hat{\mathbf{B}}^{(d-1)}$.

complexity exponential in (total size of hidden messages in bits).We consider this cost unacceptable and attempt to reach a quality approximation of the solution of to that respect by alternating generalized least-squares estimates of and , iteratively, as described below

$$\hat{\mathbf{V}}_{\text{GLS}} = \arg \min_{\mathbf{V} \in \mathbb{R}^{L \times K}} \|\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{VB})\|_F^2 = \mathbf{YB}^T(\mathbf{BB}^T)^{-1}.$$

The multicarrier iterative generalized least-squares (M-IGLS) procedure suggested by the two equations (11) and (15) is now straightforward. Initialize arbitrarily and alternate iteratively between (11) and (15) to obtain at each step conditionally generalized least squares estimates of one matrix parameter given the other. Stop when convergence is observed.

$$\hat{\mathbf{B}}_{\text{GLS}}^{\text{binary}} = \arg \min_{\mathbf{B} \in \{\pm 1\}^{K \times M}} \|\mathbf{R}_{\mathbf{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{VB})\|_F^2 \simeq \text{sgn}\{(\mathbf{V}^T\mathbf{R}_{\mathbf{y}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathbf{y}}^{-1}\mathbf{Y}\}.$$

For the sake of mathematical accuracy, we recall that in least squares there is always a symbol sign (phase in complex domains) ambiguity when joint data extraction and carrier estimation is pursued. Moreover, in a multicarrier least-squares scenario as the one that we face herein, the index association remains unresolved (i.e., given a recovered (message, carrier) pair (S,K), the corresponding index in (1) cannot be obtained). To the extend that the application of the work Where k belong to {1,2,3,…….m}presented in this paper is to simply extract blindly the embedded bits with the least possible errors, the carrier indexing problem is not dealt with any further.

Returning to the proposed data extraction algorithm, we understand that with M = 4 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 (Kbits or more.

4. EXPERIMENTAL STUDIES

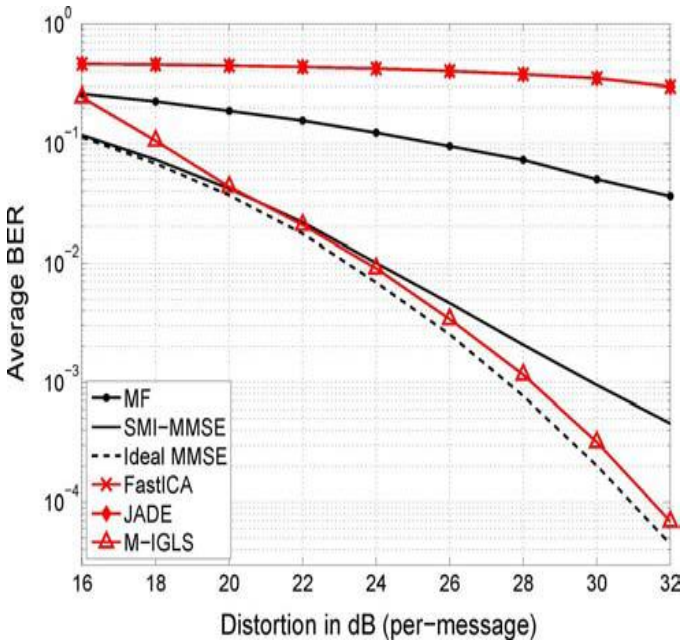
A technically firm and keen measure of quality of a hidden message extraction solution is the difference in bit-error-rate (BER) experienced by the intended recipient and the analyst. The intended recipient in our studies may be using any of the following three message recovery methods: (*i*) Standard carrier matched-filtering (MF) with the known carriers; (*ii*) sample-matrix-inversion MMSE (SMI-MMSE) filtering with known carriers and estimated host autocorrelation matrix (see (3)); and (*iii*) ideal MMSE filtering with known carriers and known true host autocorrelation matrix , which serves as the ultimate performance bound reference for all methods. In terms of blind extraction (neither nor known), we will examine: (*iv*) The developed M-IGLS algorithm in Table I with reinitializations and, for comparison purposes, the performance of two typical independent component analysis (ICA) based blind signal separation (BSS) algorithms (*v*) FastICA , and (*vi*) JADE .

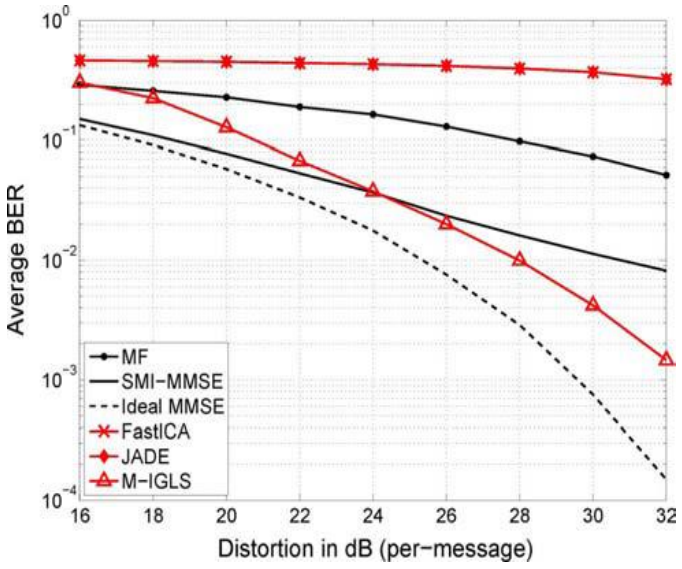
We first consider as a host example the gray-scale 512 512 “Baboon” image. We perform 8 8 block DCT embedding by (1) over all bins except the dc coefficient with K=4. The hidden message embedded by each carrier is bits long. The per-message block mean square distortion due to each embedded message is set to be the same for all messages, i.e., . With per-message 8 8-block MSE distortion, the peak signal-to-noise ratio (PSNR) of the image due to embedding can be calculated by. Another metric that reflects the relationship between host and embedding distortion is the block document-to-watermark power ratio (DWR)

defined as where is the (total) host block variance. The value of 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.

512 X 512 gray-scale Boat image

While two independent/principal-component methods (FastICA and JADE) are failing to carry out effective hidden data extraction, to our satisfaction MIGLS analysis is very close in BER performance to the ideal MMSE detector bound in which both the embedding carriers and the clean host autocorrelation matrix are treated as perfectly known. To examine the behavior of M-IGLS under increasing-density small-message hiding, we consider the **256 X 256** gray-scale "F-16 Aircraft" image with **K=4** and **K=8** hidden messages of length 1 Kbit each. The recovery performance plots for **K=4** and **K=8** are given in. 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.





While our blind data extraction algorithmic development was based on the most common SS embedding form (1) for convenience in presentation, the developed algorithm can also be applied to more advanced SS embedding

schemes such as improved spread-spectrum (ISS) [13] and correlation-aware improved spread-spectrum (CAISS) [43]. In Fig. 12, we go again over the whole [46], [47] databases under ISS embedding and in under CAISS embedding

256 X 256 gray-scale Aircraft image.

5. CONCLUSION

We considered the problem of blindly extracting unknown messages hidden in image hosts via multicarrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. We developed a low complexity multicarrier iterative generalized least-squares (MIGLS) 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/hiding

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for a wealth of comments and suggestions that helped improve significantly the presentation and content of this manuscript.

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, no. 7, pp. 1062–1078, Jul. 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA, USA: 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, Jul. 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 Process. Mag.*, vol. 17, no. 5, pp. 20–46, Sep. 2000.

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

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

[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Int. Workshop on Information Hiding*, Portland, OR, USA, 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, USA, 1984, pp. 51–67, Plenum.

[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2706–2722, Jun. 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 Syst., Special Issue on Multimedia Watermarking*, vol. 9, pp. 303–311, Sep. 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, no. 4, 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 Process.*, vol. 6, no. 12, 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 Process.*, vol. 9, no. 1, pp. 55–68, Jan. 2000.