A New Detecting and Extracting Spread Spectrum Valuable Hidden Data from Digital Media

Lokesh Sirela [#1], Sk Shafiulilah [*2]

[#1]M.Tech Scholar, [*2] Assistant Professor
Department of Computer Science & Engineering,
Vizag Institute of Technology Engineering College,
Dakamarri, Visakhapatnam Dist, AP, India.

Abstract

Information hiding is a new kind of secret communication technology with lot of recent user's attention. Steganography is also a new method or technique of sending most valuable hidden data or secret messages over a public channel, so that a third party cannot detect the presence of secret message. In this paper, we mainly consider the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio and 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. Our experimental research work 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.

Keywords

Authentication, Annotation, Blind Detection, Covert Communications, Data Hiding, Information Hiding, Spread-Spectrum Embedding, Steganalysis, Steganography, Watermarking.

1. Introduction

As there was a tremendous increase and improvement of the Internet and the digital information revolution, together caused major changes in the overall culture. In the current market ,flexible and simple-to-use software and availability of very low prices of digital devices (e.g. portable CD and mp3players, DVD players, CD and DVD recorders, laptops, PDAs) have made it feasible and easy for consumers from all over the world to create, edit and exchange multimedia data. Along with these, with the advent of broadband internet connections almost a very secure errorless transmission of data helps people to distribute large amount of multimedia files and make identical digital copies of them. In the modern communication system Data Hiding technique is most essential for Network Security issue. Sending of valuable sensitive messages and important files over the internet is transmitted in an unsecured form but everyone has got something to keep in secret.

Data Embedding in digital media such as audio, video, image is an new information technology field ,which is rapidly growing in its interest .In annotation based mechanism, secondary data are embedded into digital multimedia content[1] to provide a way to deliver side information for various purposes, along with this copyright-marking may also act as permanent "iron branding" mechanism to show ownership, fragile watermarking may also be intended mainly to detect future tampering; hidden low-probability to- detect (LPD) watermarking may serve as new watermarking identification technique for confidential data validation or digital fingerprinting for tracing purposes [2]-[4]. Covert communication method or steganography method, which literally means “covered writing method” in Greek, is the process of hiding valuable secret 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]. The following four basic attributes of data hiding are accomplished with digital data embedding [10]:

1. **Payload** -This is used for measuring information delivery rate.

2. **Robustness** - This is used for measuring hidden data resistance to noise/disturbance.

3. **Transparency-** This is used for measuring low host distortion for concealment purposes.

4. **Security** - This is used for measuring inability by unauthorized users to detect/access the communication channel.

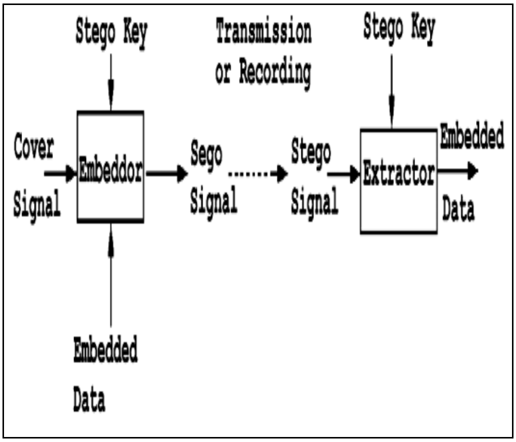


Fig. 1. Block diagram of data hiding and retrieval.

Recent research work on developing data embedding technologies is greatly seen to pose a threat to personal privacy, commercial, and national security interests [11], [12]. In this current research work, we mainly focus our complete attention on the blind recovery of secret valuable data hidden in medium hosts via multi-carrier/signature direct-sequence spread-spectrum (DS-SS) transform domain embedding [13]-[20]. This blind hidden valuable data extraction problem has also been referred to as “Watermarked content Only Attack” (WOA) in the watermarking security context [21]-[24].

In this paper, we mainly develop a new multi-signature iterative generalized least squares (M-IGLS) SS steganalysis algorithm for hidden valuable data extraction. For very accurate and improved recovery performance, in particular for small hidden valuable messages that pose the greatest challenge, we propose a new algorithmic upgrade referred to as cross-correlation enhanced M-IGLS (CC-M-IGLS). CC-M-IGLS relies mainly on statistical analysis of independent M-IGLS executions on the host and experimental studies indicate that this mechanism can achieve hidden data recovery with probability of error close to what may be attained with known embedding signatures and known original host autocorrelation matrix.

The following notations are used throughout the whole published paper. Boldface lower-case letters in this paper indicate column vectors and bold face upper-case letters in this paper indicate matrices. R denotes the set of all real numbers; $(\cdot)^T$ denotes matrix transpose; Tr $\{\cdot\}$ is matrix trace; I_L is the L × L identity matrix; sgn $\{\cdot\}$ denotes zero-threshold quantization; and E $\{\cdot\}$ represents statistical expectation. Finally, $|\cdot|$, $\|\cdot\|$, and $\|\cdot\|_F$ are the scalar magnitude, vector norm, and matrix Frobenius norm, respectively.

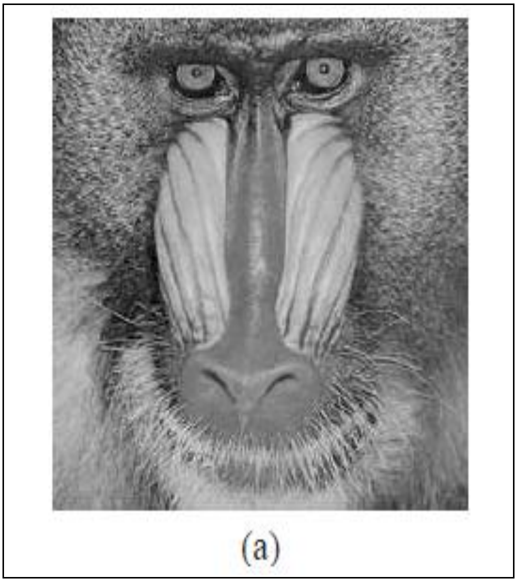
2. Multi-Carrier SS Embedding and Extraction Technique

Consider a host image $H \in M^{N1\times N2}$ where M is defined with the finite image alphabet and $N_1\times N_2$ is defined as the image size in pixels.

Without a huge loss of generality in the image, the image H is initially partitioned into M different local non-overlapping blocks of size $N_1N_2/$ M. Each divided block namely, H1, H2, ...,H_M, is to carry K hidden information bits (KM bits total image payload). Embedding mechanism is performed in a 2-Dimensional transform domain called T.

Once after transform calculation and vectorization is performed, we obtain a function called T (H_m) ∈ $R^{N1N2/ M}$, m = 1, 2, . . . , M. From the obtained transform domain vectors T (Hm) we choose a fixed subset of L ≤ $N_1N_2/$ M coefficients (bins) to form the final host vectors x(m) ∈ R^L, m = 1, 2, . . . ,M. It is most common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

The auto correlation matrix which is formed by the host data x is an important statistical quantity for our developments and is defined. 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. 2(a) gives the host autocorrelation matrix Rx in Fig. 2(b) [20].



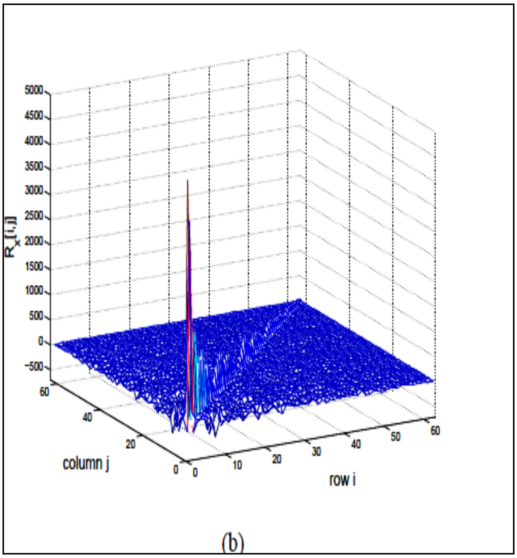


Fig. 2. (a) Baboon image example H= {0, 1, 255}256×256. (b) Host data autocorrelation matrix (8 × 8 DCT, 63-bin host) [20].

2.1 Multi-carrier SS Embedding Technique

We consider initially K distinct message bit sequences, {b_k(1), b_k(2), . . . , b_k(M)}, k = 1, 2, . . . ,K, b_k(m) ∈ {□∓_1}, m = 1, . . . ,M, each of varying 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, b_1(m), . . . , b_K(m), is simultaneously hidden in the mth transform-domain host vector x(m) via additive SS embedding by means of K spreading sequences (carriers) s_k ∈ R^L, ||s_k|| = 1, k = 1, 2, . . . ,K,

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

The contribution required for each and every individual embedded message bit with notation b_k to the composite signal is defined as $A_k b_k s_k$ and the block mean-squared distortion to the original host data x due to the embedded k message alone is defined by notation of

$$\mathcal{D}_k = \mathbb{E}\{\|A_k s_k b_k\|^2\} = A_k^2, \ \ k = 1, 2, ..., K. \tag{2}$$

After equation(2) is obtained, we undergo statistical independence of messages, the block mean squared distortion of the original image due to the total, multimessage, insertion of data is defined as follows

$$\mathcal{D} = \sum_{k=1}^{K} A_k^2.$$

The final intended recipient of the kth message with knowledge of the kth carrier s_k can perform embedded bit recovery by looking at the sign of the output of the minimum-mean-square error (MMSE) filter $w_{MMSE,k} = R^{-1}{}_y\, s_k$

$$\hat{b}_k(m) = \text{sgn}\{\mathbf{w}_{MMSE,k}^T \mathbf{y}(m)\} = \text{sgn}\{\mathbf{s}_k^T \mathbf{R}_y^{-1} \mathbf{y}(m)\} \tag{3}$$

Where Ry is defined as the autocorrelation matrix of the host-plus-data plus- noise vectors

$$\mathbf{R}_\mathbf{y} \triangleq \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{R}_\mathbf{x} + \sum_{k=1}^{K} A_k^2 \mathbf{s}_k \mathbf{s}_k^T + \sigma_n^2 \mathbf{I}_L. \tag{4}$$

2.2 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.

In this paper, we mainly focus the technical presentation purely after the point that the analyst obtains transform-domain observations in the form of y(m) in (1), upon performing appropriate image partition and transform calculation. We denote the combined "disturbance" to the hidden data (host plus noise) rewrite SS embedding by (1) as

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m) \mathbf{s}_k + \mathbf{z}(m), \ m = 1, \ldots, M, \tag{5}$$

Where z (m) is modeled as a sequence of zero-mean (without loss of generality) vectors

$$\begin{aligned} \mathbf{y}(m) &= \sum_{k=1}^{K} b_k(m) \mathbf{v}_k + \mathbf{z}(m) && (6) \\ &= \mathbf{V}\mathbf{b}(m) + \mathbf{z}(m), \ m = 1, \ldots, M, && (7) \end{aligned}$$

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

$$\mathbf{Y} = \mathbf{VB} + \mathbf{Z} \tag{8}$$

Our objective is to blindly extract the unknown hidden data B from the observation matrix Y without prior knowledge of the embedding carriers sk and amplitudes A_k, k = 1, . . . ,K,

3. Hidden Data Extraction Mechanism

In this section we mainly discuss about the hidden data extraction mechanism which was used in this paper. If **Z** were to be modeled as Gaussian distributed, the joint maximum-likelihood (ML) estimator of V and decoder of B would be

$$\hat{\mathbf{V}}, \hat{\mathbf{B}} = \arg \min_{\substack{\mathbf{B} \in \{\pm 1\}^{K \times M} \\ \mathbf{V} \in \mathbb{R}^{L \times K}}} \|\mathbf{R}_\mathbf{z}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{VB})\|_F^2 \tag{9}$$

Where multiplication by $R^{-1/2}{}_{z}$ can be interpreted as pre whitening of the compound observation data. If Gaussianity of Z is not to be invoked, then (9) can be simply referred to as the joint generalized least-squares (GLS) solution2 of V and B.

$$\hat{\mathrm{B}} = \arg\min_{\mathrm{B}\in\{\pm1\}^{K\times M}} \|\mathrm{R}_z^{-\frac{1}{2}}\mathrm{Y}\mathrm{P}_{\perp\mathrm{B}}\|_F^2 \qquad (10)$$

The generalized least-squares estimate of V is

$$\begin{aligned}\hat{\mathrm{V}}_{\mathrm{GLS}} &= \arg\min_{\mathrm{V}\in\mathbb{R}^{L\times K}} \|\mathrm{R}_z^{-\frac{1}{2}}(\mathrm{Y}-\mathrm{V}\mathrm{B})\|_F^2 \\ &= \mathrm{Y}\mathrm{B}^T(\mathrm{B}\mathrm{B}^T)^{-1}. \qquad (11)\end{aligned}$$

Pretend, in turn, that V is known. Then, the least-squares estimate of B *over the real field* is

$$\begin{aligned}\hat{\mathrm{B}}_{\mathrm{GLS}}^{\mathrm{real}} &= \arg\min_{\mathrm{B}\in\mathbb{R}^{K\times M}} \|\mathrm{R}_z^{-\frac{1}{2}}(\mathrm{Y}-\mathrm{V}\mathrm{B})\|_F^2 \\ &= (\mathrm{V}^T\mathrm{R}_z^{-1}\mathrm{V})^{-1}\mathrm{V}^T\mathrm{R}_z^{-1}\mathrm{Y}. \qquad (12)\end{aligned}$$

Observing that from above equation ,we get

$$(\mathrm{V}^T\mathrm{R}_z^{-1}\mathrm{V})^{-1}\mathrm{V}^T\mathrm{R}_z^{-1} = (\mathrm{V}^T\mathrm{R}_y^{-1}\mathrm{V})^{-1}\mathrm{V}^T\mathrm{R}_y^{-1}, \qquad (13)$$

We also rewrite the above condition as

$$\hat{\mathrm{B}}_{\mathrm{GLS}}^{\mathrm{real}} = (\mathrm{V}^T\mathrm{R}_y^{-1}\mathrm{V})^{-1}\mathrm{V}^T\mathrm{R}_y^{-1}\mathrm{Y} \qquad (14)$$

And finally suggest the approximate binary message solution of any hidden data as

$$\begin{aligned}\hat{\mathrm{B}}_{\mathrm{GLS}}^{\mathrm{binary}} &= \arg\min_{\mathrm{B}\in\{\pm1\}^{K\times M}} \|\mathrm{R}_z^{-\frac{1}{2}}(\mathrm{Y}-\mathrm{V}\mathrm{B})\|_F^2 \\ &\simeq \mathrm{sgn}\{(\mathrm{V}^T\mathrm{R}_y^{-1}\mathrm{V})^{-1}\mathrm{V}^T\mathrm{R}_y^{-1}\mathrm{Y}\}. \qquad (15)\end{aligned}$$

TABLE I
MULTI-CARRIER ITERATIVE GENERALIZED LEAST-SQUARES DATA EXTRACTION

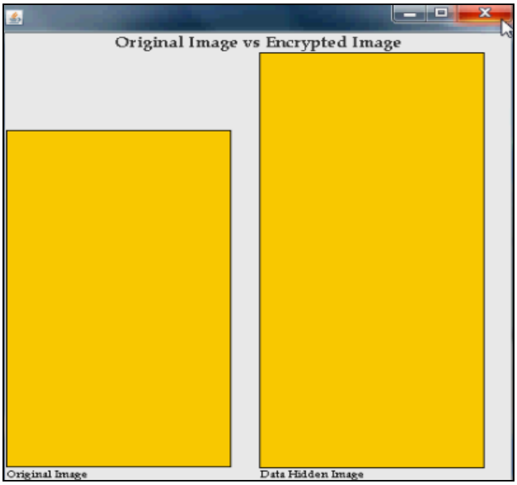
```
1) $d := 0$; initialize $\hat{\mathrm{B}}^{(0)} \in \{\pm1\}^{K\times M}$ arbitrarily.
2) $d := d+1$;
    $\hat{\mathrm{V}}^{(d)} := \mathrm{Y}(\hat{\mathrm{B}}^{(d-1)})^T\left[(\hat{\mathrm{B}}^{(d-1)})(\hat{\mathrm{B}}^{(d-1)})^T\right]^{-1}$;
    $\hat{\mathrm{B}}^{(d)} := \mathrm{sgn}\left\{\left((\hat{\mathrm{V}}^{(d)})^T\hat{\mathrm{R}}_y^{-1}(\hat{\mathrm{V}}^{(d)})\right)^{-1}(\hat{\mathrm{V}}^{(d)})^T\hat{\mathrm{R}}_y^{-1}\mathrm{Y}\right\}$.
3) Repeat Step 2 until $\hat{\mathrm{B}}^{(d)} = \hat{\mathrm{B}}^{(d-1)}$.
```

To the extend that the application of the work 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.

4. Experimental Results

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 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, and (*vi*) JADE. The following chart window is the experimental results obtained by implementing the paper in JAVA Technology.

Comparison Graph



5. Conclusion

In this paper, we considered mainly the problem of blindly extracting unknown valuable messages hidden in image hosts via multi-carrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed to be available. We developed a very new method of low complexity multi-carrier iterative generalized least-squares (M-IGLS) core algorithm. Our experimental research studies showed that M-IGLS can achieve high 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.

6. 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.

[17] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression," *IEEE Trans. Image Proc.*, vol. 13, pp. 126-144, Feb. 2004.

[18] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in *Proc. IEEE Intern. Conf. Image Proce. (ICIP)*, Singapore, Oct. 2004, pp. 1561-1564.

[19] M. Gkizeli, D. A. Pados, S. N. Batalama, and M. J. Medley, "Blind iterative recovery of spread-spectrum steganographic messages," in *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*, Genova, Italy, Sept. 2005, vol. 2, pp. 11-14.

[20] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Proc.*, vol. 16, pp. 391-405, Feb. 2007.

[21] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Proc.*, vol. 53, pp. 3976-3987, Oct.2005.

[22] L. P´erez-Freire, P. Comesana, J. R. Troncoso-Pastoriza, and F. P´erez- Gonz´alez, "Watermarking security: A survey," *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.

[23] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," *ACM Journal Signal Proc. - Special Section: Security of Data Hiding Technologies*, vol. 83, pp. 2069-2084, Oct. 2003.

[24] L. P´erez-Freire and F. P´erez-Gonz´alez, "Spread-spectrum watermarking security," *IEEE Trans. Inform. Forensics and Security*, vol. 4, pp. 2-24, Mar. 2009.

7. About the Authors

Lokesh Sirela is a student of the Department of Computer Science & Engineering of Vizag Institute of Technology, Visakhapatnam. Presently he is pursuing his M.Tech from this college. He completed his MCA Degree from JNTU Kakinada. His area of interest includes DBMS, DMDW, Networks and Web Technologies.

Sk Shafiulilah received the M.Tech degree in Computer Science & Technology from GITAM University A.P, India and B.Tech degree in Computer Science & Engineering from Al-Ameer College of Engineering, India. Currently he is working as an Assistant Professor in Vizag Institute of Technology in the department of Computer Science & Engineering. He has more than 6 years of teaching experience in various engineering colleges. His research interests include Networks and Network Security & Text Mining.