Intentional Hidden Data Extraction from Digital Media Using Spread Spectrum

A.YugandharRao, Maddala Gayatri, Kotha Vyshnavi, Buddepu Harish, Ravupalli Swarupa Rani

Abstract— **Information ambuscade is a new affectionate of secret advice technology with lot of recent user's attention. Steganography is as well a new adjustment or address of sending most valuable hidden abstracts or abstruse letters over a public channel, so that a third affair cannot detect the attendance of abstruse message. In this paper, we mainly accede the botheration of extracting blindly abstracts anchored over a wide band in a spectrum (transform) area of a digital average (image, audio and video). We develop a atypical multicarrier/ signature iterative generalized least-squares (M-IGLS) core procedure to seek alien abstracts hidden in hosts via multicarrier spread-spectrum embedding. Neither the aboriginal host nor the embedding carriers are affected available. Our experimental research plan on images appearance that the developed algorithm can accomplish accretion anticipation of error abutting to what may be accomplished with known embedding carriers and host autocorrelation matrix.**

Index Terms— **Authentication, Annotation, Blind Detection, Covert Communications, Abstracts Hiding, Information Hiding, Spread-Spectrum Embedding, Steganalysis, Steganography, Watermarking.**

I. INTRODUCTION

As there was a amazing access and improvement of the Internet and the digital information revolution, calm acquired major changes in the all-embracing culture. In the accepted market ,flexible and simple-to-use software and availability of actual low prices of agenda accessories (e.g. portable CD and mp3players, DVD players, CD and DVD recorders, laptops, PDAs) accept fabricated it achievable and easy for consumers from all over the apple to create, edit and barter multimedia data. Forth with these, with the appearance of broadband internet connections about a actual defended errorless transmission of abstracts helps humans to bear large amount of multimedia files and accomplish identical digital copies of them. In the modern communication arrangement Abstracts Hiding address is most capital for Network Security issue. Sending of admired acute letters and important files over the internet is transmitted in an apart form but anybody has got something to accumulate in secret. Data Embedding in agenda media such as audio, video, angel is an new information technology acreage ,which is rapidly growing in its interest .In comment based mechanism, secondary data are anchored into agenda multimedia content[1] to accommodate a way to bear side information for assorted purposes, forth with this copyright-marking may as well act as abiding "iron branding" apparatus to appearance ownership, fragile watermarking may as well be advised mainly to detect future tampering; hidden low-probability to- detect (LPD) watermarking may serve as new watermarking identification address for confidential abstracts validation or agenda fingerprinting for archetype purposes [2]-[4]. Covert communication method or steganography method, which literally means "covered autograph method" in Greek, is the process of ambuscade admired abstruse abstracts beneath a cover medium (also referred to as host), such as image, video, or audio, to authorize abstruse communication between dupe parties and burrow the actuality of embedded abstracts [5]-[9]. The afterward four basic attributes of abstracts ambuscade are able with digital abstracts embedding [10]:

1. Payload -This is acclimated for measuring information supply rate.
2. Robustness - This is acclimated for measuring hidden abstracts attrition to noise/disturbance.
3. Transparency- This is acclimated for measuring low host baloney for Concealment purposes.
4. Security - This is acclimated for measuring inability by crooked users to detect/access the communication channel.

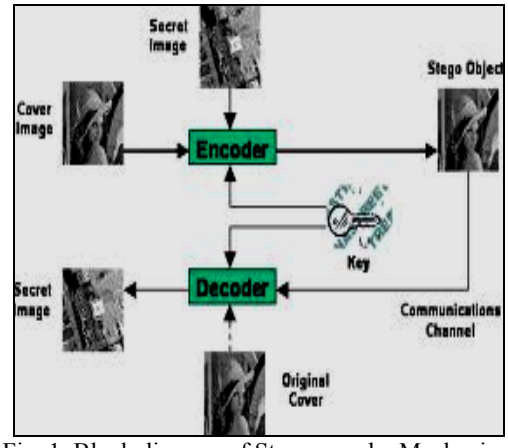


Fig. 1. Block diagram of Stegnography Mechanism

Manuscript received March 19, 2015

A.YugandharRao, Assistant Professor, Department of Information Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist, AP, India

Maddala Gayatri, Department of Information Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist, AP, India

Kotha Vyshnavi, Department of Information Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist, AP, India

Buddepu Harish, Department of Information Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist, AP, India

Ravupalli Swarupa Rani, Department of Information Technology, Lendi Institute of Engineering and Technology College, Jonnada, Denkada Mandalam, Vizianagaram Dist, AP, India

Recent assay plan on developing data embedding technologies is abundantly apparent to affectation a threat to claimed privacy, commercial, and national security interests [11], [12]. In this accepted research work, we mainly focus our complete absorption on the dark accretion of abstruse admired abstracts hidden in medium hosts via multi-carrier/signature direct sequence spread-spectrum (DS-SS) transform domain embedding [13]-[20]. This dark hidden valuable abstracts abstraction botheration has as well been referred to as "Watermarked agreeable Only Attack" (WOA) in the watermarking aegis ambience [21]- [24]. In this paper, we mainly advance a new multi-signature accepted ambiguous atomic squares (M-IGLS) SS steganalysis algorithm for hidden valuable abstracts extraction. For actual authentic and improved accretion performance, in accurate for small hidden admired belletrist that affectation the greatest challenge, we adduce a new algorithmic upgrade referred to as cross-correlation added MIGLS (CC-M-IGLS). CC-M-IGLS relies mainly on statistical assay of absolute M-IGLS executions on the host and beginning studies indicate that this apparatus can accomplish hidden data accretion with anticipation of absurdity abutting to what may be accomplished with accepted embedding signatures and accepted aboriginal host autocorrelation matrix. The afterward notations are used throughout the accomplished appear paper. Boldface lower-case belletrist in this cardboard announces column vectors and adventurous face upper-case belletrist in this paper indicate matrices. R denotes the set of all real numbers; (•) T denotes cast transpose; Tr { • } is matrix trace; IL is the L × L character matrix; sign { • } denotes zero-threshold quantization; and E { • } represents statistical expectation. Finally, | • |, ‖ • ‖, and ‖ • ‖F are the scalar magnitude, vector norm, and cast Frobenius norm, respectively.

II. EXISTING SYSTEM

In the existing system reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded in to the image by using the same encryption key. The user who knows the secret encryption key used can access the image and decrypt it after extracting or removing the data hidden in the image. After extracting the data hidden in the image then only can be the original image is retrieved.

III. DISADVANTAGES OF EXISTING SYSTEM

- Low security.
- Only image in image and message in image, encryption is possible in the existing system.
- Less reliable due to the repeating of the same process again.

IV. PROPOSED SYSTEM

We propose the information hiding concept to reduce the risk of using cryptographic algorithms alone. Data hiding techniques embed information into another medium making it imperceptible to others, except for those that are meant to receive the hidden information and are aware of it presence. It focuses on methods of hidden data in which cryptographic algorithms are combined with the information hiding techniques to increase the security of transmitted data. we focus our attention on the blind recovery of secret data hidden in medium hosts via multi-carrier/signature direct-sequence spread-spectrum transform domain embedding.

V. ADVANTAGES OF PROPOSED SYSTEM

- In our proposed system we are not following the regular encryption, decryption techniques.
- Encryption is embedded into an image, audio or video files.
- Again it will be embedded in to another media. This double embedding is increase the level of security.
- Password protections of this entire works give an additional security.

A. Multi-Carrier SS Embedding and Extraction Technique:

Consider a host angel H ∈ MN1×N2 where M is authentic with the bound angel alphabet and N1×N2 is authentic as the angel admeasurements in pixels Without a huge accident of generality in the image, the image H is initially abstracted into M altered local non-overlapping blocks of admeasurements N1N2/ M. Each divided block namely, H1, H2, ...,HM, is to backpack K hidden advice $.25 (KM $.25 absolute image payload). Embedding apparatus is performed in a 2-Dimensional transform area alleged T. Once afterwards transform adding and factorization is performed, we access a function called T (Hm) ∈ R N1N2/ M, m = 1, 2, . . . , M. From the acquired transform area vectors T (Hm) we choose a anchored subset of L ≤ N1N2/ M coefficients (bins) to anatomy the final host vectors x(m) ∈ RL, m = 1, 2, . . . ,M. It is a lot of accepted and adapted to avoid the dc accessory (if applicable) due to high perceptual acuteness in changes of the dc value. The auto alternation cast which is formed by the host abstracts x is an important statistical quantity for our developments and is defined. For example, 8×8 DCT with 63-bin host abstracts formation (excluding alone the dc coefficient) for the 256×256 gray-scale Baboon angel in Fig. 2(a) gives the host autocorrelation cast Rx in Fig. 2(b) [20].

Fig. 2. (a) Stegno Image

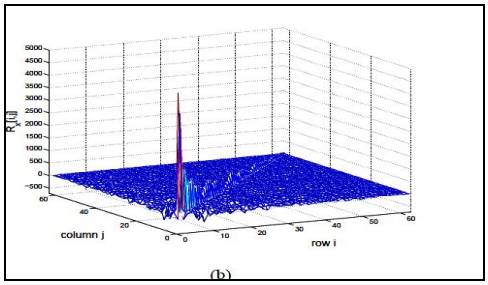


Fig. 2. (a) Represents Stegno image example H= {0, 1, 255}256×256. (b) Host data autocorrelation matrix (8 × 8 DCT, 63-bin host).

For our development we mainly require the auto correlation matrix which is finally formed by the Cover Data. For example, we take 8×8 DCT with 63-bin Cover data formation (excluding only the dc coefficient) for the 256×256 gray-scale Stegno image in Fig. 2(a) gives the host autocorrelation matrix Rx in Fig. 2(b) [11].

1. Multi-Career SS Embedding Technique

We accede initially K audible message bit sequences, {bk(1), bk(2), . . . , bk(M)}, k = 1, 2, . . . ,K, bk(m) ∈ { + 1}, m = 1, . . . ,M, anniversary of varying breadth M bits. The K bulletin sequences may be to be delivered to K audible corresponding recipients or they are just K portions of one large message arrangement to be transmitted to one recipient. In particular, the mth bit from anniversary of the K sequences, b1(m), . . . , bK(m), is simultaneously hidden in the mth transform-domain host vector x(m) via accretion SS embedding by agency of K spreading sequences (carriers) sk ∈ RL, ||sk|| = 1, k = 1, 2, . . . ,K,

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

The addition appropriate for anniversary and every alone anchored bulletin bit with notation bk to the blended arresting is authentic as Akbksk and the block mean-squared baloney to the original host abstracts x due to the anchored k message alone is authentic by characters of

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

After equation(2) is obtained, we undergo statistical ability of messages, the block mean boxlike baloney of the aboriginal angel due to the total, multimessage, admittance of abstracts is defined as follows

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

The final advised almsman of the kth message with ability of the kth carrier sk can perform anchored bit accretion by searching at the sign of the achievement of the minimum-mean-square error (MMSE) clarify wMMSE,k = R−1 y sk

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

Where Ry is authentic as the autocorrelation matrix of the host-plus-data plus- babble vectors

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

A. Formulation of the Extraction Problem

To blindly abstract spread-spectrum embedded abstracts from a accustomed host image, the analyst needs aboriginal to catechumen the host to ascertainment vectors of the anatomy of y (m), m = 1. . . M, in (1). This requires ability of
(i) The partition,
(ii) Transform domain,
(iii) Subset of coefficients, and
(iv) Number of carriers acclimated by the embedded

With the help of these four modules we are able to provide security for the hidden data over transmission channel.

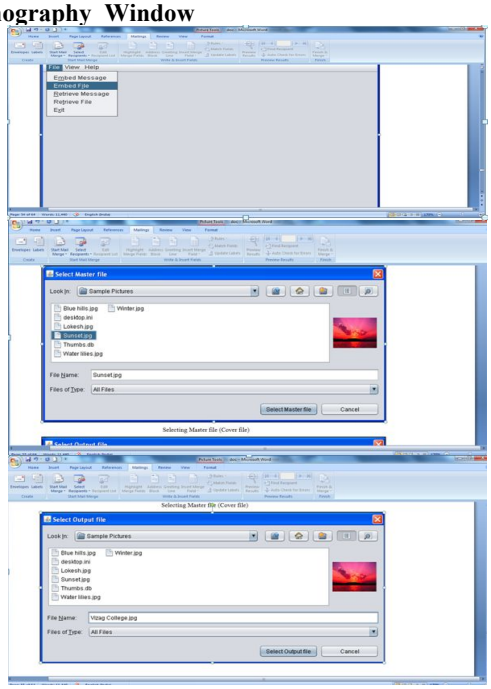
B. Experimental Results

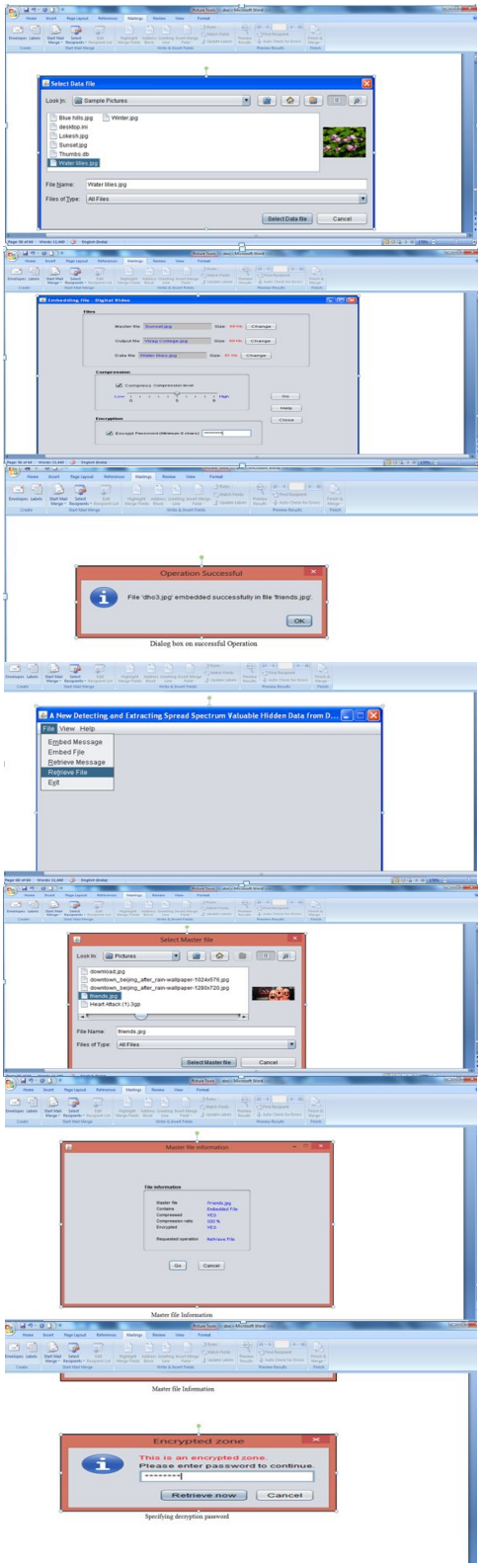
A technically close and agog admeasurements of quality of a hidden bulletin abstraction band-aid is the aberration in bit-error-rate (BER) accomplished by the advised almsman and the analyst. The intended recipient in our studies may be application any of the following three bulletin accretion methods: (i) Standard carrier matched-filtering (MF) with the known carriers sk, k =1, ...,K; (ii) sample-matrix inversion MMSE (SMI-MMSE) clarification with known carriers sk and estimated host autocorrelation matrix bRy (see (3)); and (iii) ideal MMSE filtering with accepted carriers sk and accepted accurate host autocorrelation cast Rx, which serves as the ultimate achievement apprenticed advertence for all methods. In agreement of dark abstraction (neither sk nor Rx known), we will examine: (iv) The developed MIGLS algorithm in Table I with P = 20 reinitializations and, for allegory purposes, the performance of two archetypal absolute component analysis (ICA) based dark arresting break (BSS) algorithms (v) FastICA, and (vi) JADE. The following blueprint window is the beginning results obtained by implementing the cardboard in JAVA Technology.

Main Window

Once after we click on submit button the following Stegnography window will displays in which we have facility of embedding message, embedding a file.

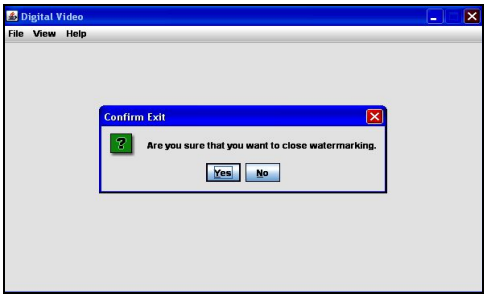
Stegnography Window





Exit Window

This window is mainly designed in order to ask confirmation whenever any user who wish to close the current process. If the user clicks on yes option then window gets closed otherwise it will be in same stegnography window.



CONCLUSION

In this paper, we advised mainly the problem of blindly extracting alien valuable messages hidden in angel hosts via multicarrier/ signature spread-spectrum embedding. Neither the aboriginal host nor the embedding carriers are affected to be available. We developed a very new adjustment of low complication multi-carrier iterative ambiguous least-squares (M-IGLS) core algorithm. Our beginning analysis studies showed that M-IGLS can accomplish top anticipation of error rather abutting to what may be accomplished with known embedding signatures and accepted original host autocorrelation cast and presents itself as an effective antitoxin to accepted SS data embedding/ hiding.

REFERENCES

[1] F. A. P. Petit colas, 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, Agenda 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 agenda angel and video data: A advanced overview," IEEE Signal Processing Magazine, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, "A analysis of steganographic techniques," in Information Hiding, S. Katzenbeisser and F. Petit colas 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. Caching, "An information-theoretic archetypal for steganography," in Proc. 2nd Intern. Workshop on Information Hiding, Portland, OR, Apr. 1998, pp. 306-318.

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

[9] J. Fredric, Steganography in Agenda Media, Principles, Algorithms, and Applications. Cambridge, UK: Cambridge University Press, 2010.

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

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