Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 49 (2012) 10141-10146

ISSN: 2229-712X

# On the realization of a secure, high capacity data embedding technique using joint top-down and down- top embedding approach

Shabir A. Parah[1], Javaid A. Sheikh[1] and G.M. Bhat[2]

[1]Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India.

[2]University Science Instrumentation Center, University of Kashmir, Srinagar, India.

**ARTICLE INFO**

**Article history:**

Received: 26 June 2012;

Received in revised form:

16 August 2012;

Accepted: 25 August 2012;

**Keywords**

Steganography,

Data Hiding, Security,

Intermediate Significant Bit.

**ABSTRACT**

The rapid development of network technologies has lead to vast multimedia data being transmitted over the networks. However, the data being transmitted can be tampered or attacked by some malicious attackers during transit. To provide security to multimedia data steganography is being used as a potential tool, where the secret data to be transmitted is embedded in a cover medium (Image) in order to avert the attackers. This paper presents a secure and high capacity stegnographic technique where secret data is embedded in intermediate significant bit planes besides least significant bit plane. The embedding scheme uses alternate top-down and down-top approach to improve the quality of stego-image. The security of the embedded data is taken care of by embedding data in all locations under the control of secret key. The experimental results show that proposed scheme performs better than some existing schemes.



## I. Introduction

Digital communication has become popular due to tremendous growth of internet. This however, has resulted in serious challenges pertaining to integrity and security of data being communicated. Cryptography and steganography are well known and widely used techniques to secure information like bank transactions, corporate communication, credit card, national security issues and multimedia content copyrights. The art of keeping message secret is called stenography [1]. It is derived from Greek words that literally mean 'covered writing'. Being used for information security, steganography and cryptography are cousins in spy craft family. While cryptography scrambles the message which is unable to understand, the goal of steganography is to hide information inside a harmless cover medium in such a way that it is not possible to detect the existence of secret message [2]. The most important issue in steganography is that the very presence of a hidden message must be concealed. Such a requirement is not critical in watermarking problems.

Although steganography has been studied as part of cryptography for many decades, the focus of steganography is secret communication. In fact, the modern formulation of the problem goes by the name of the *prisoner's problem*. Here Alice and Bob are trying to hatch an escape plan while in prison. The problem is that all communication between them is examined by a warden, Wendy, who will place both of them in solitary confinement at the first hint of any suspicious communication. Hence, Alice and Bob must trade seemingly inconspicuous messages that actually contain hidden messages involving the escape plan. Further the duo ensures that the medium carrying information about their plan should pass through Wendy a less number of times so as to avert any suspicion. For this they try to put as much information in the medium (cover) as possible.

There are two versions of the problem that are usually discussed — one where the warden is passive, and only observes messages, and the other where the warden is active and modifies messages in a limited manner to guard against hidden messages.

In this paper we try to address first problem where adversary is passive. As such emphasis has been given to high hiding capacity coupled with imperceptibility besides providing adequate security. Rest of the paper is organized as follows. Section II differentiated cryptography and steganography. Section III talks about application areas of data hiding systems. In section IV literature survey regarding high capacity data hiding techniques has been presented. Section V provides complete description of proposed work. The results obtained in the proposed technique and the comparison with existing ones is presented in section VI. The paper concludes in section VII.

## II. Cryptography and Stegnography

The three important characteristics of information hiding system that contend with each other are capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego-medium can withstand before an adversary can destroy hidden information [3].

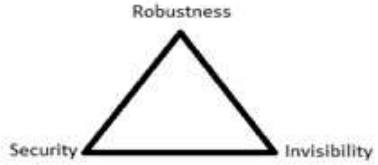



**Fig. 1: Conflict Triangle**

The data to be hidden in the cover medium can be embedded in two domains i.e spatial domain and transform domain. Two generally used transform domain techniques are Discrete Cosine Transform (DCT) and Discrete Wavelet transform (DWT). Robustness requirements of the hidden data are taken care of by selecting appropriate domain for data

Tele: 09858715541

E-mail addresses: shabireltr@gmail.com

embedding. For a more robust data hiding system transform domain is generally used. For the purpose of steganography symmetric encryption is followed. The symmetric encryption is a method of encryption that uses same key to encrypt and decrypt a message. If one person encrypts and decrypts data, that person must keep the key secret. If the data is communicated between the parties each party must agree on shared secret key and secure method to exchange the key. No encryption method is completely secure. Given knowledge of the algorithm and enough time attackers can reconstruct most encrypted data. An algorithm built on sound mathematical methods creates no predictable pattern in encrypted data and uses sufficiently long Key. In fact security of data hidden in cover image can be directly related to Kerckhoff's assumption. Kerckhoff's assumptions state that one should assume that the method used to encrypt the data is known to an unauthorized party and that the security lies in the choice of a key [4, 5]. Hence a data hiding technique is truly secure if mere knowledge of exact algorithms for embedding and extracting the data does not help an unauthorized party to detect the presence of the hidden data or remove it. Thus Key forms a pivotal part in determining the security strength of a data hiding system.

## III. Data Hiding Applications

Data hiding that encompasses both digital watermarking and steganography has been found useful in following areas:

**A. Copyright Protection**: To assert ownership of a Multimedia content.

**B. Copy control**: For copy prevention and control.

**C. Content Authentication**: To check authenticity of a multimedia content and ensure whether same piece has been received that was transmitted at transmitter or a changed version of original piece.

**D. Broadcast monitoring**: To monitor if the contracted number of commercials were broadcasted in a given time slot or not.

**E. Fingerprinting**: To discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data.

**F.Metadata binding**: Metadata information embedded in an image can serve many purposes. For example, a business can embed the Web site address for a specific product in a picture that shows an advertisement for that product.

**G. Covert communication**: For information security.

## IV. Literature review

With the development of internet and information processing techniques, as an effective solution for copyright protection and information security, data hiding techniques have been receiving much attention today. In the last decade a lot of research attention has been paid in this direction, [6] gives an idea about acceleration of research in this area.

Spatial-domain watermarking techniques for image data include [7, 8]. Some of the earliest techniques embed m-sequences in to the least significant bit (LSB) of the data to provide an effective transparent embedding technique. M-sequences are chosen due to their good correlation properties so that a correlation operation can be used for secret message detection. Furthermore, these techniques are computationally inexpensive to implement. Several spatial domain data hiding techniques for images are proposed in [9]. One technique consists of embedding a texture-based message into a portion of the image with similar texture. The idea here is that due to the similarity in texture, it will be difficult to perceive the watermark. The watermark is detected using a correlation detector. Another technique described as the patchwork method divides the image into two subsets A and B where the brightness of one subset is incremented by a small amount and the brightness of the other set is decremented by the same amount. The incremental brightness level is chosen so that the change in intensity remains imperceptible. The location of the subsets is secret and assuming certain properties for image data, the watermark is easily located by averaging the difference between the values in the two subsets. It is assumed that, on average, without the watermark, this value will go to zero for image data.

An adaptive surrounding pixel technique, which utilizes all eight adjacent neighboring pixels, for embedding secret information, so that imperceptibility grows has been developed and is presented in [10]. Pixel intensity based high capacity data embedding method is presented in [11]. The method improves the modified Kekre's algorithm which is based on LSB method. The capacity is improved by embedding the payload into the low intensity pixels and hence maximum utilization of cover image.

A stegnographic algorithm which improves security in LSB matching process has been presented in [12]. Here the distortion of one dimensional histogram is minimized based on Cachins theory. In [13] a method to find appropriate regions in cover image to embed payload has been proposed. The number of neighboring pixels is counted and only the pixel values with small difference are considered for LSB embedding method. [14] Presents a segment compression stegnographic algorithm. The input data is first compressed using Karhunen Loeve transform to achieve higher concealing capacity and then hide LSB secret data in cover medium.

In [15] development of stegnographic techniques for gray scale images has been reported. The schemes are reported to have high hiding capacity and good imperceptibility properties. [16] Reports a high capacity data embedding scheme based on average covariance. The Most significant Bit (MSB) of the payload are embedded into cover image based on average covariance of cover image. The authors have reported PSNR of 46.31% for hiding capacity of 12.50%.

A watermarking technique based on Intermediate Significant Bit (ISB) replacement has been [17]. The authors have reported that embedding information in the intermediate significant bits improves robustness compared to when data is hidden in least significant bits. [18] Reports a high capacity embedding technique based on spatial domain. The host image is partitioned into non-over lapping blocks, with each block containing three 3x3 pixels. In every block these pixels receive special treatment, with an aim to decrease the noise and deviations from the original picture values. The authors have reported an embedding capacity ranging between 20-26% when PSNR is limited between 27db to 30db range.

A high capacity data hiding method has been put forth in [19]. The proposed technique is based on Exploiting Modification Direction or (EMD) and LSB matching methods. This paper reports Peak Signal to Noise Ratio of about 47db for a range of test images when about 12.5% or 262143 bits of secret data are embedded in the cover medium.

## V. Proposed Method

The block diagram of proposed high capacity data hiding scheme is shown in Fig. 2.

Let C be the original 8-bit grey scale cover image of Mc x Nc pixels.

$$C = \{x_{ij} | 0 \leq i < M_c, 0 \leq j < N_c\} \qquad (1)$$

$x_{ij}\ \varepsilon\ \{0,1,2,3,\ldots\ldots\ldots 255\}$

Let M be the n bit secret message represented as

$$M = \{m_i | 0 \leq i < n\ ,\ m_i\ \varepsilon\ \{0,1\}\} \qquad (2)$$

The secret message M can be arranged into a vector $M'$ such that

$$M' = \{m'_{ij} | 0 \leq i < n', m'_i\ \varepsilon\ \{0,1\} \qquad (3)$$

$$where\ n' < 8 * M_c * N_c$$

The message vector is embedded into the cover image C under control of a key K given by

$$K = \left\{K_{i|}\ 1 \leq i = n', K_i\ \varepsilon\ \{1,2,3,\ldots..n\}\right\} \qquad (4)$$

Where key K is a function of seed S given by

$$S = S_k\ S_{k-1} \ldots . S_0\ such\ that\ 2^k = n$$

Prior to data embedding the cover image is broken into its constituent bit planes as shown in Fig.3. Since the perceptual quality of the covermedia *C* directly depends on the amount of data *M* embedded in the covermedia besides the significant bit plane in which the data is embedded, the proposed algorithm divides the data to be embedded in the cover media in number of blocks of varying length, equal to the bit planes in which the data is to be embedded. The embedding strategy is also depicted in Fig.3. As shown the data vector with length $n$ is divided into three variable length data vectors, viz: $L1$ $L2$ and $L3$ as shown. The data is embedded in the first LSB and two subsequent ISB planes under the control of a private key K as shown in equation 4.

The embedding key is used to thwart the adversary as data is not embedded sequentially. The key may embed first bit of data at any random location of any bit planes, and the location of second bit may vary from LSB to third ISB plane and a random location of correspondingly selected bit plane. This process is depicted in Fig. 5. The embedding process is carried out in data embedder, that outputs an image containing secret data and is generally termed as stego-image.

**Embedding Strategy:** The data to be embedded is broken down into number of blocks equal to the number of bit planes in which data is to be hidden. The lengths of data vectors can be related in several ways. In this paper the data has been broken into three blocks with lengths *L1, L2* and *L3.*

This is because data is to be embedded in three bit planes. The relation between the lengths of data blocks is *L1= n/2, L2= 3n/8 and L3=n/8;* where n is the number of bits of of secret data vector to be embedded in the cover medium. The embedder uses top –down and down–top embedding strategy alternatively as shown in Fig. 4. This is done to ensure that at most only two bit planes out of three get the information from secret message vector and as such the perceptual quality of the stego image is less affected.

**Extraction Strategy**: At the receiving end the stego-image along with same key as that used at embedder has been used to extract data from the stego-image. Since cover image is not needed for the retrieval of secret data the proposed system falls in the category of blind detection.

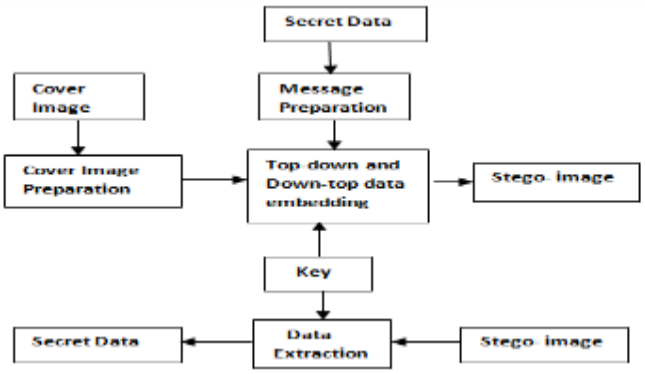



**Fig. 2: Proposed high capacity data hiding and corresponding blind extraction system**

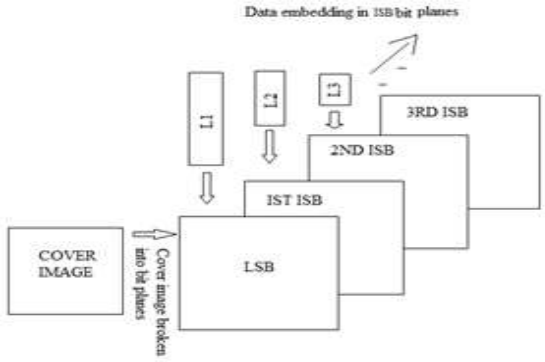



**Fig. 3: Data embedding in cover image.**

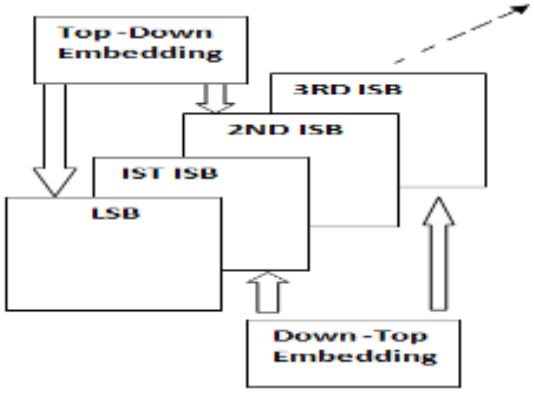



**Fig. 4: Data embedding using Top-Down and Down -Top strategy**

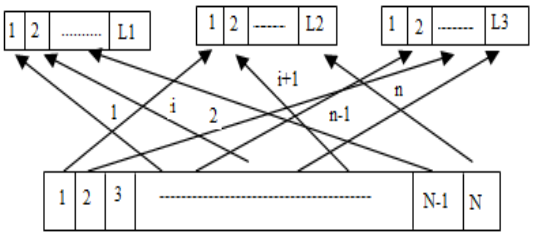



**Fig.5: Data embedding using Random Key**

## VI. Results and Analysis

In the data hiding paradigm there are two parameters of opposing nature that is to embed maximum information in an image and keeping the image degradation minimum so that it could not be perceived that something has been embedded in the host image. With this kind of motive a number of standard grayscale images (512 x512) as shown in Table 1, were used in the proposed system. Table 1 also presents stego images obtained for each gray scale test image after embedding 294906 bits of data in each of them. The implemented scheme embeds more than 14% of data in the host images compared to 12.5% in

case of [19]. Besides this the proposed system improves the Peak Signal to Noise Ratio on an average by 1.5db and by 2db at some instances like in case of test Image 'Bridge'. A comparison of the proposed data hiding scheme with that of W. Chung et.al [19] is presented in Table 2. Tables 3 and 4 respectively show a graphical comparison of the proposed scheme with [19].The proposed technique besides providing improvements in both hiding capacity and PSNR provides additional feature of high security, as data is embedded under the control of a secure key in the selected bit planes. The hiding Capacity (HC) and PSNR have been calculated as follows.

**Hiding Capacity (HC):**

Size of data in a cover image that can be modified without deteriorating integrity of the cover image gives an idea about the hiding capacity. It is also referred to as payload. Capacity is represented by bits per pixel (bpp). It is given by (total number message bits/total number of image bits) multiplied by 100. If m and N respectively denote total message bits and image bits the hiding capacity is given by

*Hiding Capacity (HC) = (m/N)*100*

**Peak Signal to Noise Ratio (PSNR):**

It is measure of quality of image. It gives an idea about how much deterioration has embedding caused to the image. It is represented as

$$PSNR = 10\log_{10}\frac{255^2}{mse}db$$

Where mse is mean square error and is given by

$$MSE = \left[\frac{1}{N*M}\right]^2 \sum_{i=1}^{N} \sum_{j=1}^{M} \left(X_{ij} - \bar{X}_{ij}\right)$$

Where N and M are image dimensions, $\mathbf{X_{ij}}$ and $\bar{\mathbf{X}}_{\mathbf{ij}}$ represent original and stego images respectively.

**VII. Conclusion**

A high capacity and secure data hiding technique is presented in this paper. The image in which the data is embedded has been broken into its constituent bit planes. The data to be embedded is divided into as many unequal blocks as the number of bit planes in which the data is to be embedded. The implemented technique embeds data in three bit planes viz. LSB and first two ISBs. The embedding is carried out using alternate top-bottom and bottom-top embedding strategy. The data is embedded under control of a key that not only embeds data pseudo randomly in various bit planes but also at various pixel locations, thus providing an adequate security to the data carried by the cover image. The technique has been implemented using MATLAB 7. The results obtained in the proposed method have been compared with [19] viz-a-viz hiding capacity and PSNR. The results clearly show that the proposed technique has a better performance.

**References:**


1. Cachin C., "An information-theoretic model for steganography," Information and Computation, **2004**. 192, 41-56.
2. Petitcolas F. P., Anderson R. J., and Kuhn N. G., "Information Hiding—A Survey" *Proceedings of The IEEE*, **1999**, 87(7), 1062-1078
3. Miller M. L., Doerr G. J and Cox I. J., "Applying Informed Coding and Embedding to Design a Robust, High capacity Watermark", *IEEE Transactions on Image Processing*, **2004**,13(6), 792-807.
4. Bhat G. M, Parah S. A. et.al, "VHDL Modelling and Simulation of Data Scrambler and Descrambler for Secure Data Communication", *Indian Journal of Science and Technology*, **2009**,Vol 2, No. 10, pp. 41-43.
5. Bhat G. M, Parah S. A. et.al, "FPGA Implementation of Novel Complex PN Code Generator based data Scrambler and Descrambler", *Maejo Int. J. Sci. Technology*. **2010**, 4(01), 125-135
6. Wah P. W. and Delp E. J., editors. "Security and Watermarking of Multimedia Contents II,". *Society of Photo-optical Instrumentation Engineers*, **2000,** volume 3971
7. Schyndel R.G., Tirkel A.Z., & Osborne C.F., "A digital watermark" .*Proceeding of IEEE International Conference on Image*", **1994**, 2, 86-90.
8. Wolfgang P., & Delp E, "A watermark for digital images." *International Conference on Image Processing Proceedings, ICIP* **1996**,96,219-222.
9. Bender W., Gruhl D., Morimoto N., & Lu A,. "Techniques for data hiding". *IBM Systems Journal*, **1996**, 35, 313-316.
10. Masoud A.and Subariah I. "Adaptive Steganography scheme using More Surrounding pixels," *International Conference on Computer Design and Applications,*. **2010**. 225-229.
11. Mehdi H. and Mureed H., "Pixel Intensity Based High Capacity Data Embedding Method," *International Conference on Information and Emerging Technologies*, **2010**,1–5
12. Lu Y., Li X. and Yang B., "A 1 –based Steganography by Minimizing the Distortion of First Order Statistics," *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, **2009,**754 – 758,
13. Huang. Q and Ouyang W., "Protect Fragile Regions in Steganography LSB Embeddeing," *International Symposium on Knowledge Acquisition and Modeling*. **2010,** 175 – 178,
14. Stanescu D., Bucur I. G. and Stratulat M., "Segment Compression Steganograhic Algorithm" *International Joint Conference on Computational Cybernetics and Technical Informatics Communications*, **2007,** 349 – 354.
15. Wu N. I. and Hwang M. S. , "Data Hiding: Current Status and Key Issues," *International Journal of Network Security*, **2010,** 4(1),1-9.
16. Sathisha N. et. al, "Embedding Information In DCT Coefficients Based On Average Covariance" *International Journal of Engineering Science and Technology (IJEST)*, **2011**,3 (4), 3184-3194.
17. Zeki A M. and Manaf A. A., "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit)" , *World academy of science Engineering and Technology* **2009**,50,989-996
18. Zeki M. A. et. al, "High watermarking capacity based on spatial domain technique" *Information technology journal*: **2011,** 10(7),1367-1373.
19. Kuo W.C. et.al, "Data Hiding Method With High Embedding Capacity Character" *International journal of image processing*, **2011** 6(3),310-317

**Table 1. Host images and their stego images**

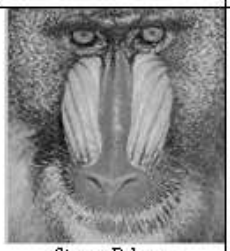
| Host image | Stego Image | Host Image | Stego Image |
|---|---|---|---|
|  Lena |  Stego- Lena |  Peppers |  Stego-Peppers |
|  Baboon |  Stego- Baboon |  Fishing Boat |  Stego-Fishing Boat |
|  Bridge |  Stego-Bridge |  Barbara |  Stego- Barbara |

**Table 2: Comparison between proposed technique and that of W. Chung et.al [19]**

| Name of Image | W. Chung et .al (Hiding Capacity in bits)[19] | Proposed (Hiding Capacity in bits) | W. Chung et.al (PSNR in db)[19] | Proposed (PSNR in db) |
|---|---|---|---|---|
| Lena | 262143 | 294906 | 47.164 | 48.663 |
| Peppers | 262143 | 294906 | 47.170 | 48.648 |
| Baboon | 262143 | 294906 | 47.171 | 48.745 |
| Boats | 262143 | 294906 | 47.074 | 48.587 |
| Bridge | 262143 | 294906 | ------ | 49.165 |
| Barbara | 262143 | 294906 | ------ | 48.637 |

**Table 3: PSNR Comparison between proposed technique and that of W. Chung et.al [19]**

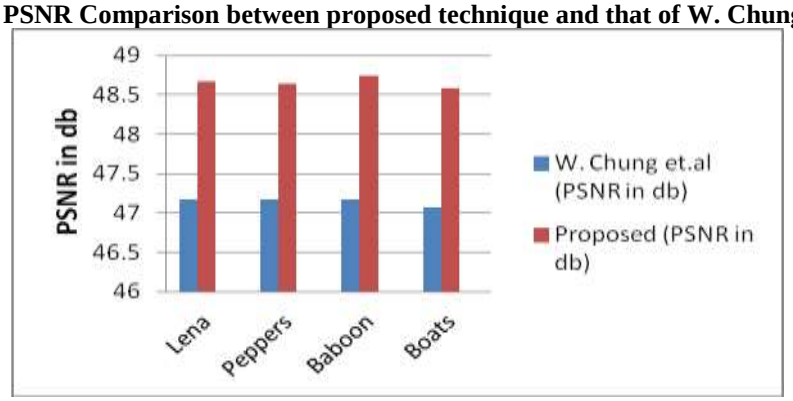



**Table 4: Hiding capacity comparison between proposed technique and that of W. Chung et. al [19]**