NON – UNIFORM SEGMENTATION WITH BRANCH SITUATION MECHANISM BASED STEGANOGRAPHY ALGORITHM TOWARDS DATA HIDING

T. Gomathi[1], *B.L. Shivakumar*[2]

Abstract

Image hiding is shortly termed as steganography. The research work carried out that has been presented in this paper provides steganography algorithm consists of three phases (comprehensive image segmentation, data hiding at the sender side and data extracting at the receiver side). These phases are implemented in order to reduce the chances of statistical detection and to provide robustness against a variety of image manipulation attacks. After hiding the data, a stego image is produced that does not have any distortion artefacts. Furthermore, the proposed steganography algorithm did not sacrifice the embedding capacity to decrease the perceptibility of data hiding.

Keywords : RGB image, comprehensive image segmentation, data hiding, steganography, distortion.

I. Introduction

Steganography refers to the science of invisible communication. It hides information in such a way that the existence of the message is unknown. Steganographic techniques strive to hide the very presence of the message itself from an observer. It can be used in a large amount of data formats in the digital world of today. This technology is a very important part of the future of internet security and privacy on open systems such as the internet. If any suspicion about the secret communication is raised, then the goal is not achieved. The embedding process on an object, while being perceptually transparent, leaves statistical artifacts that can be used to distinguish stego and cover-objects. The argument that data hiding methods leave telltale effects is common to all stegaanalysis methods [19]. Information hiding has strong applications in military and intelligence agencies that require unobtrusive communications, criminals, law enforcement and counter intelligence agencies and schemas or digital elections and digital cash. Generally, secret information is stored into the specific position of LSB of a cover image which is the carrier to embed messages [20].

A good LSB based image steganography is presented in [21] and they proposed an approach for LSB that enhances the existing LSB substitution techniques to improve the security level of hidden information. Here hidden information is stored into different positions of the LSB of image depending on the secret key. As a result, it is difficult to extract the hidden information without knowing the retrieval methods. Another LSB based image steganography is presented in [22], and they introduced an algorithm that uses the LSB and those inhomogeneous areas of the cover image to hide a message. In this algorithm, an error correction code is used to increase the

[1] Research Scholar, Department of Computer Science, Karpagam University, Coimbatore – 21.

[2] Director, Department of Computer Applications, Sri Ramakrishna Engineering College, Coimbatore – 22.

probability of retrieving the message, as well as the receiver being able to detect if there are any alterations in the cover media; in this case the receiver informs the sender about these alterations based on grayscale image. However, we use RGB color images in our algorithm implementation. A grayscale image is simply one in which the only colors are shades of gray. Often grayscale intensity is stored as an 8 bit integer, giving 256 possible different shades of gray from black to white.

II. Related Works

High capacity data hiding has been proposed by many researchers, but they did not present the effect of the security level against new attackers if the payload capacity has been increased. Al-Qershi and Khoo [1] presented a scheme based on difference expansion (DE) to increase the hiding capacity for medical images. Hiding high payload by employing the LSB substitution technique as a fundamental stage and taking advantage of the edge detection technique was proposed by Chen et al. [2]. Ioannidou et al. [3] applied image steganography by taking advantage of sharp areas in images to hide a large amount of data; this approach is based on a hybrid edge detector. Qu et al. [4] proposed a quantum steganography protocol with a large payload based on quantum secure direct communication using entanglement swapping and building up a hidden channel within the improved ping-pong protocol to transmit secret messages. Lee et al. [5] presented an adaptive, reversible data scheme based on the prediction of difference expansion. Yang et al. [6] constructed a reversible data hiding (RDH) algorithm based on a gradient-based edge direction prediction (GEDP) scheme. Chang et al. [7] presented an index compression and reversible data hiding scheme based on side-match vector quantization (SMVQ) and search order coding (SOC).

A framework in lossless and reversible data hiding research based on the histogram difference shift was proposed by Feng and Fan [8]. Lin et al. [9] introduced reversible data hiding to fully recover the original host image after extracting the secret message. A reversible image steganographic scheme based on predictive coding was proposed by Wu et al. [10] to embed secret data into compression codes during the lossless image compression to provide a lossless hiding mechanism in the compression domain. Zeng et al. [11] presented a lossless data hiding scheme; the proposed scheme was based on pixel difference histogram shifting to spare space for data hiding. Pixel differences are generated between a reference pixel and its neighbours in a pre-assigned block.

A reversible data hiding method for natural images created by constructing a multilevel histogram based on differences between pairs of adjacent pixels was presented by Zhaoa et al. [12]. Lee and Chen [13] applied an adaptive reversible data scheme based on the prediction of difference expansion. Eslami and Ahmadabadi [14] proposed a polynomial-based secret image sharing scheme with two achievements, the first was the proposal of embedding according to the size of the hidden data, and the second was the introduction of an authentication chaining method. An embedding scheme with minimal distortion was proposed by Lin [15], for which the message to be embedded was divided into sub-messages, each of which was embedded into a pixel vector with three pixels instead of one pixel.

Sajedi and Jamzad [16] introduced a boosted steganography scheme (BSS) that uses a pre-processing stage before applying the steganography methods, where the goal of the BSS is increasing the un-detectability of stego images. Liu et al. [17] proposed an image hiding scheme based on the scrambling process composed of the rotation of the squared sub-image in the gyrator transform domains. Yu et al. [18] constructed a distortion free data hiding algorithm that can embed secret messages into high dynamic range (HDR) images to satisfy three significant benefits. First, the algorithm can convey secret messages to produce a stego image. Second, adaptive message embedding is used to conceal different amounts of secret messages based on their homogeneous representations, and third, efficient time required for message embedding or extraction is efficient.

III. Proposed Work

The new steganography algorithm has three parts (comprehensive image segmentation, data hiding at the sender side and data extracting at the receiver side). These parts are constructed and implemented to reduce the chances of statistical detection and to provide robustness against a variety of image manipulation attacks. After hiding the data, a stego image is produced that does not have any distortion artefacts. Moreover, the proposed steganography algorithm must not sacrifice the embedding capacity to decrease the perceptibility of data hiding.

3.1. COMPREHENSIVE IMAGE SEGMENTATION ALGORITHM (CIS)

A new comprehensive image segmentation algorithm (CIS) is used in the third layer of security; this layer embeds data randomly rather than sequentially, and the use of non-uniform segments is an effective approach to make detection segment edges by stego analysis difficult and to fight against attacks. The CIS algorithm is based on non-uniform segmentation using a left or right diagonal splitting technique. The following steps represent the CIS algorithm:

Algorithm 1 (CIS algorithm)

Step1: Let L be the length of cipher key (ck), where L is equal to the number of symbols at the cipher key, see Eq. (1).

$$L = |CK| \tag{1}$$

Step2: Calculate the size of each segment for both the vertical (v) and horizontal (h) directions

(Γ^V, Γ^H); using the proposal formulas, see Eq. (2) and (3).

$$\Gamma_i^V = \left[\frac{\Im(CK_i) * h_c}{\sum_{m=1}^{L} \Im(CK_m)} \right] \forall I = 1,....., L \tag{2}$$

$$\Gamma_i^h = \left[\frac{\Im(ck_i) * w_c}{\sum_{m=1}^{L} \Im(ck_m)} \right] \forall i = 1,...., L \tag{3}$$

where $\Im(ck_i)$ represents the decimal value of the ith character of the ck (h_c) and (w_c) are the height and the width of the cover image C, respectively.

Step 3 : Call procedure Segment Edges (.); where Sub-Algorithm1-1 is used to find the X_{edge}, Y_{edge} of non-uniform segments on the cover image C, where the same segments' edges procedure is applied on three colors. Step4: Apply row-wise scanning for non-uniform segments at C.

Step 4-1 : Add a right or left diagonal to each segment according to the following conditions; If $\Im(ck_i)$ is odd then

Add left diagonal to segment (i);

Else

Add right diagonal to segment (i);

Step 5 : Apply a γ function defined by the map $\gamma:\Gamma_i^V \rightarrow \Phi, \forall i=1,.....,L$ to remove all vertical boundaries from each segment to generate the new segment's shape (Φ);

Step 6 : Save the coordinates x and y for each edge e_j^s (x, y)$\forall$j = 1, . . . , N edges at each segment (S), where N edges is the number of edges at the segment S.

Step 7 : End;

3.2. The Proposed Data Hiding Algorithm

In this section, we define the new concepts of the proposed hiding algorithm.

The principle situation PS is an integer value used to categorize images into 32 levels of priority to achieve hiding in a bitmap cover-image, and the value of PS is calculated by Eq. (4): where HB_8 is the extended high nibble HB_4 of a color byte to eight bits using the following steps:

$$PS^{color} = \frac{HB_8}{8} \qquad (4)$$

Algorithm 2 (Extended high nibble)

Step 1 : Find $\Im$ (CK), the sum of integer values of each element in ck, using Eq. (5); see Eq. (1).

$$\Im(CK)=\sum_{l=1}^{L}\Im(CK_l)\times 10^{L-1} \qquad (5)$$

Step 2 : Find the weight of ck, ω (CK), using Eq. (6).

$$\omega(CK)=\frac{\Im(CK)}{10^L} \qquad (6)$$

Step3: Find the extended high nibble HB_8 using Eq. (7).

$$HB_8=\left\lceil \alpha+(\beta-\alpha)\times\frac{HB_4}{15\times\omega(CK)} \right\rceil \qquad (7)$$

Where α and β are the upper and the lower bounds of HB_8, respectively, and the value of α is equal to 0, whereas the value of β is equal to 255.

End;

When hiding a large amount of data, all three colors of one pixel are checked by the proposed steganography algorithm to perform data hiding; this hiding is achieved using a new concept based on the branch situation (BS).

The branch situation BS of the corresponding principle situation PS uses the following conditions, see Eq. (8) :

$$BS^{PS}=\left\{\begin{array}{llll} BS_1^{PS^{color}} \Leftrightarrow PS^{CP^{color}} < PS^{RC_1} \wedge & PS^{CP^{color}} & < PS^{RC_2} \\ BS_2^{PS^{color}} \Leftrightarrow PS^{CP^{color}} < PS^{RC_1} \wedge & PS^{CP^{color}} & = PS^{RC_2} \\ BS_3^{PS^{color}} \Leftrightarrow PS^{CP^{color}} = PS^{RC_1} & \wedge \quad PS^{CP^{color}} & = PS^{RC_2} \\ BS_4^{PS^{color}} \Leftrightarrow PS^{CP^{color}} > PS^{RC_1} \wedge & PS^{CP^{color}} & < PS^{RC_2} \\ BS_5^{PS^{color}} \Leftrightarrow PS^{CP^{color}} > PS^{RC_1} \wedge & PS^{CP^{color}} & = PS^{RC_2} \\ BS_6^{PS^{color}} \Leftrightarrow PS^{CP^{color}} > PS^{RC_1} \wedge & PS^{CP^{color}} & > PS^{RC_2} \end{array}\right\} \quad (8)$$

where RC_1 and RC_2 are the rest colors of the selected pixel, and CP^{color} is the current color of the current pixel.

Let (AP^{Φ}) denotes all pixels at the specific segment (Φ) in the cover image C. Then, for each pixel in Φ, it is a necessary to define the current pixel denoted by CP, and the surrounding pixel denoted by $SP_i \; \forall i = 1, \ldots, 4$ around the CP, see Eqs. (9) and (10) :

$$CP = \bigcup_{color \in \{R,G,B\}} CP^{color} \qquad (9)$$

$$SP_i^{CP} = \bigcup_{i=1}^{4} SP_i^{CP^{color}}, \quad color \in \{R,G,B\} \qquad (10)$$

Let the type DataBits be used to define the properties of the secret message (Smsg), which includes the length of Smsg with its contents.

3.3. The Extracting Function of the Proposed Steganography Algorithm

The extracting function has been used to define a number of bits to be extracted (NBE) from the stego image for each color at each pixel.

Algorithm 3 (Extracting: {pseudo code}).

```
Function Extracting (var S: Image; var $\Phi$ : Segment): DataBit;

{Where Extracting has been defined by the map Extracting: S × $\Phi$ → Smsg, where S is stego-image and Smsg is an encryption and a compression of secret message}

Begin

    For i: = 1 to q do begin {q = 32 levels of priority to definePrinciple SituationPSi}

      for each Segment $\Phi$ of X and Y coordinate do begin {where $\Phi \subset S$}

      for each Pixel CP of C do begin {CP $\in \Phi$ and number of pixels np, is

defined in np = $h_c$ x $w_c$ }

        for each Color c of RGB do begin {c = 3, we have three colors $\in$ CP.}

$BS_X^{PS^{color}}$ : = g(PS[i]); {Use function g to define the script x to determine which branch situation should be implemented in the learning $LS_{ANNAGAUpAR\,i}$ machine, see using Eq.(8).}

          end {Color}

      if $\left|\frac{\sigma^2(AP^{\Phi}) - \sigma^2(CP, SPCP|i|}{\sigma^2(AP^{\Phi})}\right| < 1$ then

begin ;

$\mathrm{NBE}_{CP} : -LS_{ANN\_AGAUPAR}(BS_i^{PS}, SP^{CP}, \sigma^2(CP, SP^{CP}|i|.))$

where $LS_{ANN\_AGAUPAR1}$ has been defined by the map

$LS_{ANN\_AGAUPAR1}(BS_i^{PS^C}, SP^{CP}, \sigma^2(CP, SP^{CP}|i|) \rightarrow NBE_{CP}$ ;.}

$\mathrm{Smsg}_{\mathrm{NBE}_{CP}} := \lambda(\mathrm{S}, \mathrm{NBE}_{CP})$;
```

```
{where $\lambda$ is the extracting function on the CP and has been defined by the map : $\lambda : S \times NBE_{CP} \rightarrow Smsg_{NBE_{CP}}$,
where $NBE_{CP}$ is the number of bits to be extracted at the CP, $Smsg_{NBE\ CP}$ ,is the portion from Smsg that has been extracted from the CP.}
End
Else
    $Smsg_{NBE_{CP}} : = \lambda$ (varS : image; Z : integer);
{where Z means that we need to extract zero byte from CP.} Smsg : = Smsg + $Smsg_{NBE\ CP}$ ; {gathering the secret message from each byte.}
end {Pixel.}
end {Segment.}
end {Principle Situation.}
Secret message := $F_{AES,SPIHT}$ (Smsg);
{Apply decryption and decompression on Smsg to find The secret message.}
end;
```

where the time complexity measures for the embedding and extracting algorithms have been applied.

IV. Experimental Results

The proposed algorithm is tested on a number of RGB color images. Our proposed model makes use of Human Vision System (HVS) properties and here HVS is unable to detect any changes in digital media after embedding the secret messages (text or image) into the cover image. Here a standard RGB (true color) image is used as the cover image. Small size image is used as the hidden information.

(a) Baboon (b) Lena

Figure 1 : Cover Images

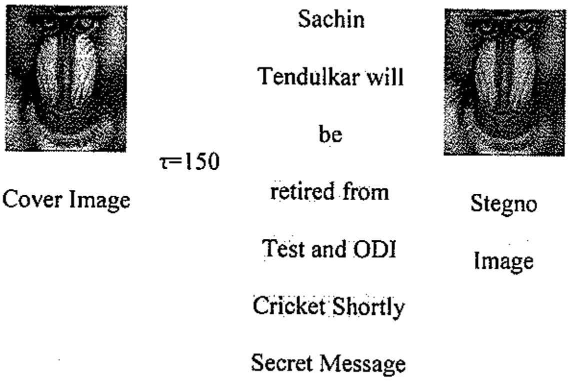
Cover Image
τ=150
Sachin Tendulkar will be retired from Test and ODI Cricket Shortly
Secret Message
Stegno Image

Figure 2 : Stegno Image Technique for Baboon Image

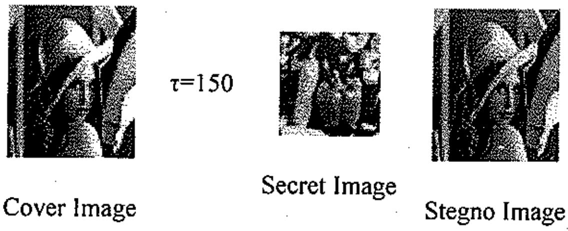

Figure 3 : Stegno Image Technique for Lena Image

Two standard RGB (true color) images, named Lena and Baboon, are used as cover images. These images are shown in Figure 1. A secret message is inserted into the cover image with a stego key. The resulting image is called a stego image. The procedure to get a stego image from the cover image is shown in Figure 2 and Figure 3.

Here in Baboon image, the secret message is text whereas in (b) Lena image, the secret message is an image.

The Peak Signal to Noise Rate (PSNR) is used to evaluate the image quality. The PSNR of an image is defined as :

$$PSNR = 10\log 10\frac{255^2}{MSE}dB \quad (11)$$

The Mean Square Error (MSE) for an M x N RGB color image is defined as follows :

$$\mathrm{MSE} = \left(\frac{1}{3\mathrm{xMxN}}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(\mathrm{X}_{ij} - \mathrm{Y}_{ij}) \quad (12)$$

where X_{ij} is the cover pixel value and Y_{ij} is the corresponding stego cover pixel value. Table 1 shows the PSNR of the four images after embedding the message in text and image respectively. In steganography, image quality is a very important issue. Due to the better quality of image, the stego image has the more secure steganography.

Table 1 : PSNR Value Comparison

Image	PSNR
Baboon	75.432
Lena	73.546

The proposed method has been tested on a number of RGB color images. Table 2 below shows the two main images (Lena and Baboon) used in the tests and their full capacity in bits to embed message bits using different threshold values. We can note that the proposed model suggests hiding three copies of the same message in Red, Green and Blue components at the same row position in order to increase the probability of retrieving the original message to recover from simple attacks. So the actual embedding capacity is three times the values listed in Table 2.

Table 2 : Maximum Capacity of RGB Cover Image to Embed Message in Bits using Different Threshold Values

Image	Threshold		
	50	100	150
Baboon (256 X 256)	65528	64888	62272
Lena (512 X 512)	262144	261320	251912

The proposed model was also tested on a number of Gray Scale images. Table 3 below shows the two images (Lena and Baboon) used in the tests and their full capacity in bits using different threshold values. Finally we found that the message capacity of an RGB image was much larger than a gray scale image of the same size.

Table 3 : Maximum Capacity of Gray scale Image to Embed Message in Bits using Different Threshold Values

Image	Method proposed in [16]	Method proposed in [17]	Method proposed in [18]	Our proposed method
Baboon	30.143	38.563	54.785	75.432
Lena	35.837	42.856	59.548	73.546

The experimental results of PSNR values by applying this proposed method on different standard images were compared with other methods in Table 2. From the results it is evident that the proposed method is better than that of the existing methods.

V. Conclusion

In this paper steganography algorithm is proposed that consists of three phases (comprehensive image segmentation, data hiding at the sender side and data extracting at the receiver side). These phases are implemented in order to reduce the chances of statistical detection and to provide robustness against a variety of image manipulation attacks. After hiding the data, a stego image is produced that does not have any distortion artefacts. Furthermore, the proposed steganography algorithm did not sacrifice the embedding capacity to decrease the perceptibility of data hiding. The proposed algorithm is implemented in MATLAB ® 2012 and the results shows that the proposed algorithm outperforms than the existing methods taken for comparison.

Reference

[1] O. Al-Qershi, B. Khoo, High capacity data hiding schemes for medical images based on difference expansion, J. Syst. Softw. 84 (1) (2011) 105–112.

[2] W. Chen, C. Chang, T. Le, High payload steganography mechanism using hybrid edge detector, Expert Syst. Appl. 37 (4) (2010) 3292–3301.

[3] A. Ioannidou, S. Halkidis, G. Stephanides, A noveltechnique for image steganography based on a high payload method and edge detection, Expert Syst. Appl. 39 (14) (2012) 11517–11524.

[4] Z. Qu, X. Chen, X. Zhou, X. Niu, Y. Yang, Novel quantum steganography with large payload, Opt. Commun. 283 (23) (2010) 4782–4786.

[5] C. Lee, H. Chen, H. Tso, Embedding capacity raising in reversible data hiding based on prediction of difference expansion, J. Syst. Softw. 83 (10) (2010) 1864–1872.

[6] W. Yang, K. Chung, H. Liao, W. Yu, Efficient reversible data hiding algorithm based on gradient based edge direction prediction, J. Syst. Softw. 86 (2) (2013) 567–580, http://dx.doi.org/10.1016/j.jss.2012.09.041.

[7] C. Chang, T. Nguyen, C. Lin, A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies, J. Syst. Softw. 86 (2) (2013) 389–402.

[8] G. Feng, L. Fan, Reversible data hiding of high payload using local edge sensing prediction, J. Syst. Softw. 85 (2) (2012) 392–399.

[9] C. Lin, D. Buehrera, C. Chang, T. Lu, Using quad smoothness to efficiently control capacity–distortion of reversible data hiding, J. Syst. Softw. 83 (10) (2010) 1805–1812.

[10] H. Wu, H. Wang, C. Tsai, C. Wang, Reversible image steganographic scheme via predictive coding, Displays 31 (1) (2010) 35–43.

[11] X. Zeng, Z. Li, L. Ping, Reversible data hiding scheme using reference pixel and multilayer embedding, Int. J. Electron. Commun. (AEU) 66 (7) (2012) 532–539.

[12] Z. Zhaoa, H. Luo, Z. Luc, J. Pand, Reversible data hiding based on multilevel histogram modification and sequential recovery, Int. J. Electron. Commun. (AEU) 65 (10) (2011) 814–826.

[13] C. Lee, H. Chen, A novel data hiding scheme based on modulus function, J. Syst. Softw. 83 (5) (2010) 832–843.

[14] Z. Eslami, Z. Ahmadabadi, Secret image sharing with authentication chaining and dynamic embedding, J. Syst. Softw. 84 (5) (2011) 803–809.

[15] C. Lin, An information hiding scheme with minimal image distortion, Comput. Stand. Interfaces 33 (5) (2011) 477–484.

[16] H. Sajedi, M. Jamzad, Boosted steganography scheme with cover image preprocessing, Expert Syst. Appl. 37 (12) (2010) 7703–7710.

[17] Z. Liu, S. Li, W. Liu, W. Liu, S. Liu, Image hiding scheme by use of rotating squared sub-image in the gyrator transform domains, Opt. Laser Technol. 45 (1) (2013) 198–203.

[18] C. Yu, K. Wu, C. Wang, A distortion data hiding scheme for high dynamic range images, Displays 32 (5) (2011) 225–236.

[19] S. Lyu and H. Farid, *"Detecting hidden messages using higher-order statistics and support vector machines"*, In 5th Information Hiding International Workshop, F. A. P. Petitcolas, Ed. vol. 2578, Lecture Notes in Computer Science, pp. 340–354, Springer-Verlag, New York, 2002.

[20] J. I. Avcýbas,, M. Kharrazi, N. Memon and B. Sankur, *"Image steganalysis with binary similarity measures,"* EURASIP J. Appl. Signal Process. 17, pp. 2749–2757, 2005.

[21] S. M. M. Karim, M. S. Rahman, and M. I. Hossain, *"A New Approach for LSB Based Image Steganography using Secret Key"*, Proceedings of 14th InternationalConference on Computer and Information Technology 2011, Bangladesh.

[22] A. Al-Jaber and I. Aloqily, *"High Quality Steganography Model with Attacks Detection"*, Pakistan Journal of Information and Technology, 2 (2): 116-127, 2003.

Author's Biography

I, **T.Gomathi,** Research Scholar, Karpagam University. I am doing Ph.D (P.T) Computer Science in Karpagam University. I was working as an Assistant Professor for 9 years. I had also published papers in international Journals and also in Scopus Index. My area of Interest is Digital Image Processing and Data Mining.

Dr.B.L.Shivakumar holds a Ph.D. in Computer Science from Bharathiar University, Coimbatore. He has more than 20 years of academic experience in various positions in reputed colleges. He has 12 years of research experience and has 47 research publications to his credit in reputed journals and conferences. He has successfully guided four research Scholars from leading Universities and presently 6 students are pursuing PhD, under his guidance. He has written 38 articles related to Computer in Tamil daily "Dina Thanthi" in Computer Jallam. He is recipient of Bharat Jyoti award conferred by The India International Friendship Society, New Delhi and NSS Best Programme Officer award by Bharathiar University. His interest includes Computer Forensic Science, Network Security and Cloud computing. He is a member in a number of Academic Bodies and Professional Societies.