International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 1, Issue 12 (July 2012), PP.21-26
www.ijerd.com

A Novel method of Reducing Additive Distortion in Steganography with Embedding Operation

CH.Sairam[1], B.Lakshmi[2]
[1]*Dept of CSE, AME, Palavncha, India,*
[2]*Asst.prof, Dept of CSE, AME, Palavncha, India*

Abstract—This paper proposes a new methodology for reducing additive distortion in steganography with embedding operation. In this paper it is planned to introduce a method that embed 2 bits information in a pixel and alter one bit from one bit plane but the message does not necessarily place in the least significant bit of pixel and second less significant bit plane and fourth less significant bit plane can also host the massage. In this approach we used a novel syndrome-coding scheme based on dual convolution codes equipped with the Viterbi algorithm. This fast and very versatile solution achieves state-of-the-art results in steganographic applications while having linear time and space complexity w.r.t. the number of cover elements. Security is provided by applying DES (Data Encryption Standard) for encryption and decryption of embedded message. Practical merit of this approach is validated by constructing and testing adaptive embedding schemes for digital images in raster and transform domains. Most current coding schemes used in steganography (matrix embedding, wet paper codes, etc.) and many new ones can be implemented using this framework.

Keywords—STEGO, VITERBI, DES

I. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the Sender and intended recipient, suspects the existence of the message, a form of security through obscurity[1]. It is often thought that communications may be secured by encrypting the trac, but this has rarely been adequate in practice. Neas the Tactician, and other classical Writers, concentrated on methods for hiding messages rather than for enciphering them [2]. There exist two mainstream approaches to steganography in empirical covers, such as digital media objects steganography designed to preserve a chosen cover model and steganography minimizing a heuristically-defined embedding distortion today's least detectable steganographic schemes for digital images [3]–[6] were designed using this principle. Moreover, when the distortion is defined as a norm between feature vectors extracted from cover and stego objects, minimizing distortion becomes tightly connected with model preservation insofar the features can be considered as a low-dimensional model of covers. This line of reasoning already appeared in [6] and [7] and was further developed in [8]. With the exception of [8], steganographers work with additive distortion functions obtained as a sum of single-letter distortions. A well-known example is matrix embedding where the sender minimizes the total number of embedding changes. Near-optimal coding schemes for this problem appeared in [9] and [10], together with other clever constructions and extensions [11]–[16]. In this paper it is planned to introduce a method that embed 2 bits information in a pixel and alter one bit from one bit plane but the message does not necessarily place in the least significant bit of pixel and second less significant bit plane and fourth less significant bit plane can also host the massage. Since in our method for embedding two bits message we alter just one bit plane, fewer pixels would be manipulated during embedding message in an image and it is expected for the steganalysis algorithm to have more difficulty detecting the covert communication. It is clear that in return complexity of the system would increase. In our method there are only three ways that a pixel is allowed to be changed:

1. Its least significant Bit would alter (So the gray level of the pixel would increased or decreased by one level)
2. The second less significant bit plane would alter (So the gray level of the pixel would increase or decrease by two levels)
3. The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels).

For executing the process the code is written in JAVA language. And Simulation is done in MATLAB (for checking Histogram of Original & Stegno image). The paper is organized as fallows. In section II we described about the implementation process where in which how the data is taken and embedded and including decryption process is explained. And in section III about the experimental results showing all the pictorial view of all the results. In section IV analysis is done on this process and comparison graph is also plotted. And fallowed by conclusion section.

II. IMPLEMENTATION

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data. To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of

the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganography potential, the larger size of meaningful audio files makes them less popular to use than images. The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission
In this we have 2 modules
A) Steg module
B) UnSteg module

Steg Module:

In this module User need to write any secret information in Text area provided and need to select an Image file to which User wants to append the Secret Information Text. After Selecting the Image the processing of adding Secret Information to Image file takes place. In Steg Module only the Secret Text Information and Image to which Secret Text Information will be selected and the remaining process go on based on the pixels of image and Text given.

UnSteg Module:

In UnSteg module the Encrypted Image will be selected and Steganography Application will start decrypting it with each and every pixel of the Image and displays the output i.e. Secret Text Information. UnSteg module will be accepting only the Image which has the hidden text message in it. After decrypting the Image the Secret Text Information will be displayed from the Image by UnSteg Module.

Data flow diagram

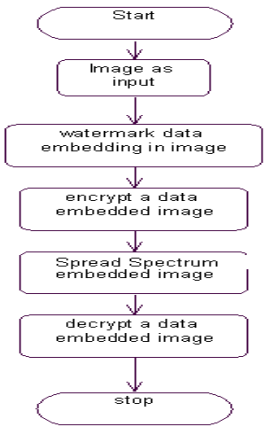


Figure 1: The overall implementation flow

Here in this process take the input image that is to be watermarked. The Input Module is designed as such a way that the proposed system must be capable of handling any type of data formats, such as if the user wishes to hide any image format then it must be compatible with all usual image formats such as jpg, gif, bmp, it must be also compatible with video formats such as avi, flv, wmf etc.And also it must be compatible with various document formats, so that the user can be able to use any formats to hide the secret data.

The next process is watermarking. Watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark. Watermarked content can prove its origin, thereby protecting the data. Next is encrypting the data. In this module we encrypt the data embedded image. The purpose of authenticator watermark of a block is invariant in the watermark embedding process; hence the watermark can be extracted without referring to the original content .The encryption and decryption techniques are used in this module. In applications, the method is required to be made robust so that embedded message can be deducted easily, even when stego images are slightly modified. In digital communications, information is transmitted bit-by-bit, i.e. as binary signaling. Larger the pulse size of the symbol higher is the probability of detection. Improvements of performance is due to the fact that for fewer symbols to hide we use more locations per symbol. Each symbol is represented by a pattern of binary bits.

Next method is we flip an edge pixel in binary images is equivalent to shifting the edge location horizontally one pixel and vertically one pixel. A horizontal edge exists if there is a transition between two neighboring pixels vertically and a vertical edge exists if there is a transition between two neighboring pixels horizontally. We use spread spectrum watermark morphological content. The watermarked content is obtained by computing the inverse for the main processing block to reconstruct its candidate pixels. Use this module we going to see the original and watermarked content

III. EXPERIMENTAL RESULTS

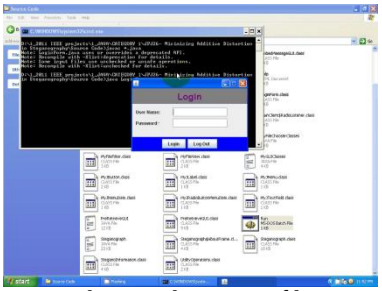
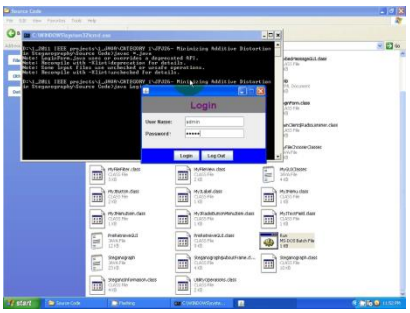


Figure1: Figure showing the screen of login page of user



Figures2: Figure showing the user entering the username and password.

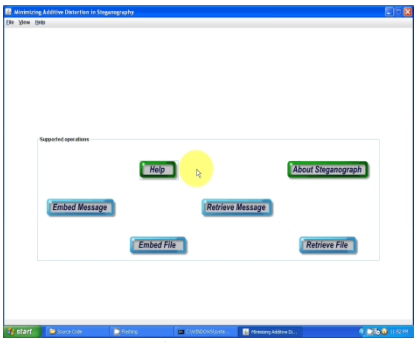


Figure 3: User interface picture showing the labels

Figure 4: Inserting an input data for embedding

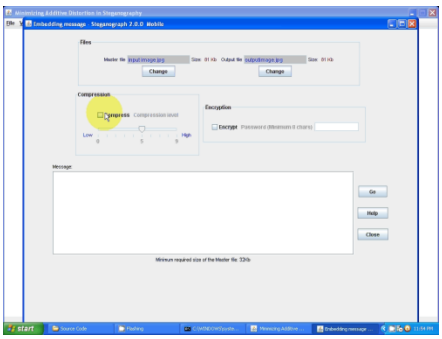


Figure 5: Entering the input message to be embedded into the input data and encrypting the final data

Figure 6: Entering the input message to be embedded into the input data and encrypting the final data

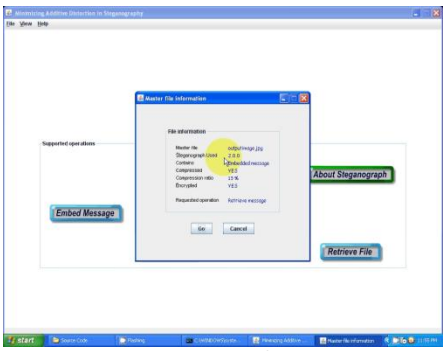


Figure 7: Final page after encryption

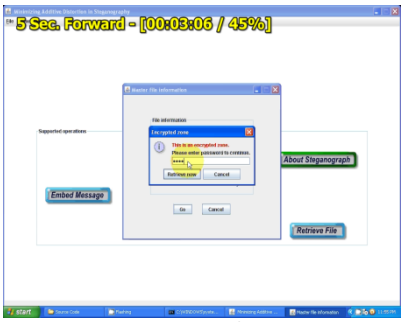


Figure8: Entering the password for decryption by receiver.

IV. SIMULATION AND STEGANALYSIS RESULTS

We will consider text-in-image embedding to demonstrate the simulation results, but the method can be used for other messages like binary images too, which was already analysized and given in IETE Technical Review. Fig 3 Output Results

Visual Precept ion

For any steganography based secure system, the perception of steganos should be as cover image itself so that one cannot differentiate them and detect the existence of embedded message. From fig 3, the cover image, processed cover image and stego images look similar and one is not able to distinguish them visually.

Difference Analysis

The "difference-images "obtained by taking the difference between cover, processed cover and stego images are not visible. For making the difference visible in "difference-images " for visual interpretation, we first increase differences by multiplication of weight factor and then revert the values to get the strengthened "difference-images". The strengthened difference-images obtained are shown in fig 4. From analysis of these "difference-images ", on could not say that the changes are either due to cover processing or message embedding and hence we can say that the method is safe from known cover-stego attack.

Distortion Analysis

Distortion analysis of stego images is carried out by studying distortion / similarity messages statistically. There are many methods for measuring distortion that can be used for distortion analysis. Distortion between two different images is measured by considering Mean Square Error (MSE), Mean Absolute Error (MAE) or Histogram Similarity (HS).

Depth Vs Distortion Analysis

Distortion occurred in different steganos is required by varying the depth of hiding for embedding information in cover image. The relation between depth of hiding used and distortion occurred in the stego images is shown in Fig 7. That depth of hiding within some LSB region is most suitable for message embedding as the distortion is very small in this region. As the depth of hiding increases beyond preferable region, the distortion becomes noticeable and unsuitable for message hiding.

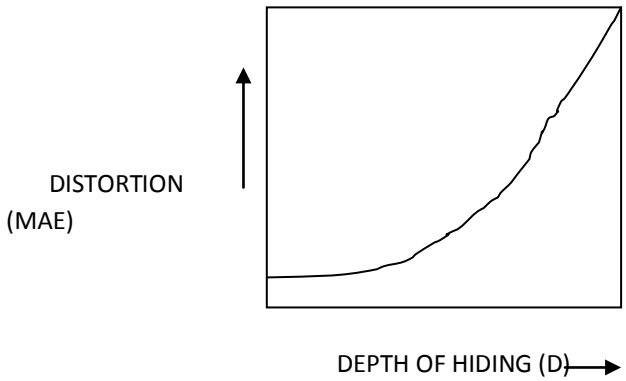


***Fig.9.*Depth Vs Distortion Analysis Security**

A method, SBIPM, for providing the security of our important information has been proposed in this paper which is based on the techniques of signal processing, cryptography, and steganography. The security of information has been strengthened by applying scanning, coding, and encryption, cover processing and embedding techniques in the method. Reshaping step of the method provides robustness for detecting message correctly in such situation when stego image is distorted. The method developed is safe from various attacks. Simulation and steganalysis results shown in this paper shows that one will not be able to distinguish between cover and stego images.

V. CONCLUSION

Thus we conclude that the strength of security achieved is very high and unauthorized receiver will not be able to get back the original message using exhaustive without the knowledge of key parameters. Digital Steganography is interesting field and growing rapidly for information hiding in the area of information security. It has a vital role in defense as well as civil applications. In future we will more of secure systems based on this technology.

REFERENCES

[1]. Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). Information hiding a survey *Proceedings of the IEEE (special issue)* **87** (7): 1062–78. . Retrieved 2008-09-02.

[2]. A. Tacticus, How to survive under siege / Aineias the Tactician, pp. 84{90, 183{193. Clarendon ancient history series,Oxford, England: Clarendon Press, 1990, ISBN 0-19-814744-9,translated with introduction and commentary by David White head

[3]. Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal istortion steganography," in Proc. 8th Int. Workshop Inf. Hiding,J.L.Camenisch,C.S.Collberg,N.F.Johnson,and P. Sallee, Eds., Alexandria, VA, Jul. 10–12, 2006, vol. 4437, Lecture Notes in Computer Science, pp. 314–327.

[4]. R. Zhang, V. Sachnev, and H. J. Kim, "Fast BCH syndrome coding forsteganography," in Proc. 11th Int. Workshop Inf. Hiding,,S.Katzen-beisser and A.-R. Sadeghi, Eds., Darmstadt, Germany, Jun. 7–10, 2009,vol. 5806, Lecture Notes in Computer Science, pp. 31–47.

[5]. V. Sachnev, H. J. Kim, and R. Zhang, "Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding," in Proc. 11th ACM Multimedia Security Workshop,J. Dittmann, S. Craver, and J. Fridrich, Eds., Princeton, NJ, Sep. 7–8,2009, pp. 131–140.

[6]. T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in Proc. 12th Int. Workshop Inf. Hiding,P.W.L.Fong,R.Böhme ,andR.Safavi-Naini,Eds., Calgary, Canada, Jun. 28–30, 2010, vol. 6387, Lecture Notes in Computer Science, pp. 161–177.

[7]. J. Kodovský and J. Fridrich, "On ompleteness of feature spaces in blind steganalysis," in Proc. 10th ACMMultimedia SecurityWorkshop,A. D. Ker, J. Dittmann, and J. Fridrich, Eds., Oxford, U.K., Sep. 22–23,2008, pp. 123–132.

[8]. T. Filler and J. Fridrich, "Gibbs construction in steganography," IEEE Trans. Inf. Forensics Security, vol. 5, pp. 705–720, Sep. 2010.

[9]. J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in Proc. SPIE, Electron. Imag., Security, Steganography, Watermark. Multimedia Contents IX,E.J.Delp and P. W. Wong, Eds., San Jose, CA, Jan. 29–Feb. 1, 2007, vol. 6505,pp. 02–03.

[10]. T. Filler and J. Fridrich, "Binary quantization using belief propagation over factor graphs of LDGM codes," presented at the 45th Annu.Allerton Conf. Commun., Control, Comput., Allerton, IL, Sep. 26–28, 2007.

[11]. X. Zhang, W. Zhang, and S. Wang, "Efficient double-layered steganographic embedding," Electron. Lett., vol. 43, pp. 482–483, Apr. 2007.

[12]. W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," IEEE Commun Lett., vol. 11, pp. 680–682, Aug. 2007.

[13]. W. Zhang, X. Zhang, and S. Wang , "Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes," in Proc. 10th Int. Workshop Inf. Hiding, ,K.Solanki,K. Sullivan, and U. Madhow, Eds., Santa Barbara, CA, Jun. 19–21, 2008,vol. 5284, Lecture Notes in Computer Science, pp. 60–71.

[14]. T. Filler and J. Fridrich, "Wet ZZW construction for steganography,"presented at the 1st IEEE Int. Workshop Inf. Forensics security,London, U.K., Dec. 6–9, 2009.

[15]. W. Zhang and X. Zhu, "Improving the embedding efficiency of wetpaper codes by paper folding," IEEE Signal Process. Lett., vol. 16, pp.794–797, Sep. 2009.

[16]. W. Zhang and X. Wang, "Generalization of the ZZW embedding construction for steganography," IEEE Trans. Inf. Forensics Security, vol 4, pp. 564–569, Sep. 2009.

Biographies

Ch.Sairam presently pursuing his M .Tech in CSE,in ADAMS Engineering college. His interested areas are networking, data mining etc.

B.Lakshmi completed her M.Tech in the Dept of CSE, Andhra University. She is presently working as Asst.prof in CSE Dept, ADAMS Engineering College. Her interested areas are Networking, Web technologies and Image processing etc.