ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 7, September 2012

A New Way to Implement Stegnography by Minimizing Distortion

K.Kiran Kumar[1], Y.Prabhu Suresh Babu[2], A.Sudhir[3], P.Ravi Prakash[4]
[1] Lecturer, IT Department, Bapatla Engineering College, Bapatla, A.P.
[2] IT Department, Bapatla Engineering College, Bapatla, A.P
[3] IT Department, Bapatla Engineering College, Bapatla, A.P.
[4] Asst.Professor, IT Department, PVP Siddhartha Institute of Technology, Vijayawada, A.P

***Abstract*— In this paper we are going to learn about the minimization of distortion in steganography. For this purpose we use a general nonbinary embedding operation and discuss various system requirements. We assume every possible value of stego element by assigning a scalar which expresses the distortion of a embedding change done by replacing the cover element by this value. The total distortion is assumed to be a sum of per-element distortions. Both the payload-limited sender (minimizing the total distortion while embedding a fixed payload) and the distortion-limited sender (maximizing the payload while introducing a fixed total distortion) are considered. Nonbinary case is decomposed into several binary cases by replacing individual bits in cover elements, but there is no loss of performance. Using a novel syndrome-coding scheme, the binary case is approached and these are 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 with respect to the number of cover elements. Practical merit of this approach is validated by constructing and testing adaptive embedding schemes for digital images. In this paper what we've obtained is to implement steganography by using general non-binary embedding operation. This gives the new technique to implement steganography effectively and easily.**

I. Introduction

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.The disadvantage is that an adversary can usually rather easily identify statistical quantities that go beyond the chosen model that allow reliable detection of embedding changes. The latter strategy is more pragmatic—it abandons modeling the cover source and instead tells the steganographer to embed payload while minimizing a distortion function. In fact, today's least detectable steganographic schemes for digital images [2]–[5] 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 paper provides a general methodology for embedding while minimizing an arbitrary additive distortion function with a performance near the theoretical bound. We present a complete methodology for solving both the payload-limited and the distortion-limited sender.

This paper is organized as follows. In the next section, we introduce the modules of the system. By pointing out the limitations of previous approaches, we motivate our contribution. In Section III, we explain the software methodology that we have used to develop this paper. The existing and proposed methods for steganographic communication is reviewed in Section IV. Both the binary and nonbinary versions of payload and distortion-limited senders are tested by blind steganalysis. Finally, the paper is concluded in Section V. This paper unifies these methods into a complete and self-contained framework.

II. MODULE DESCRIPTION

2.1 Input Module :

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 user any formats to hide the secret data.

2.2 Watermark embedding :

Watermarking is a technology for embedding[6] 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.

2.3 Authenticator Watermark :

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 used in this module.

2.4 Spread Spectrum :

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[7].

2.5 Watermarked content

The watermarked content is obtained by computing the inverse for the main processing block to reconstruct its candidate pixels.[8] Use this module we going to see the original and watermarked content.

2.6 Module I/O:

2.6.1 Module Input:

We give original content as input with watermark data embedding. We view flipping an edge pixel in binary images as shifting the edge location one pixel horizontally and vertically.

2.6.2 Module Output:

The output of the project is we reconstruct the pixel horizontally and vertically .we can see the original watermarked data and embedding content.

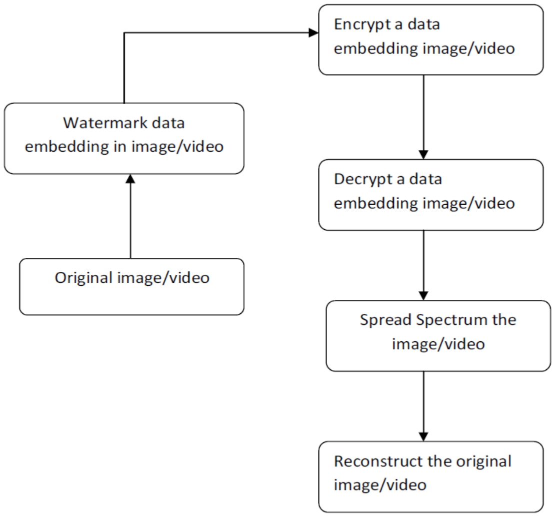
Encrypt a data embedding image/video
Watermark data embedding in image/video
Decrypt a data embedding image/video
Original image/video
Spread Spectrum the image/video
Reconstruct the original image/video

Fig. 1 Module Description

III. SOFTWARE ENVIRONMENT

The Java Programming Language

The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called *Java byte codes* —the platform-independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed. You can think of Java byte codes as the machine code instructions for the *Java Virtual Machine* (Java VM). Every Java interpreter, whether it's a development tool or a Web browser that can run applets, is an implementation of the Java VM. Java byte codes help make "write once, run anywhere" possible. You can compile your program into byte codes on any platform that has a Java compiler. The byte codes can then be run on any implementation of the Java VM. That means that as long as a computer has a Java VM, the same program written in the Java programming language can run on Windows 2000, a Solaris workstation, or on an iMac.

IV.SYSTEM ANALYSIS

4.1 EXISTING SYSTEM:

- In special domain, the hiding process such as least significant bit(LSB) replacement, is done in special domain, while transform domain methods hide data in another domain such as wavelet domain.
- Least significant bit (LSB) is the simplest form of Steganography. LSB is based on inserting data in the least significant bit of pixels, which lead to a

slight change on the cover image that is not noticeable to human eye. Since this method can be easily cracked, it is more vulnerable to attacks.

- LSB method has intense affects on the statistical information of image like histogram[1]. Attackers could be aware of a hidden communication by just checking the Histogram of an image. A good solution to eliminate this defect was LSB matching. LSB-Matching was a great step forward in Steganography methods and many others get ideas from it.

4.2 PROPOSED SYSTEM:

- Our system 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. The fourth less significant bit plane can also host the message.
- 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:
  - Its least significant Bit would alter (So the gray level of the pixel would increased or decreased by one level)
  - The second less significant bit plane would alter (So the gray level of the pixel would increase or decrease by two levels)
  - The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels)
- Data hiding in video sequences is performed in two major ways: bit stream-level and data-level.
- In this paper, we propose a new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding[15][16] (FZDH).
- By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks.

ADVANTAGES

- User cannot find the original data.
- It is not easily cracked.
- To increase the Security .
- To increase the size of stored data.
- We can hide more than one bit.

4.3 FEASIBILITY ANALYSIS

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out[9-11]. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ♦ ECONOMICAL FEASIBILITY
- ♦ TECHNICAL FEASIBILITY
- ♦ SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

V.CONCLUSION

The video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH are proposed in this paper. we found that the method is robust. , we compare FZDH and QIM as the data hiding method of the proposed framework then observe that FZDH is superior to QIM, especially for low embedding distortion levels. Tested with the MPEG-2, H.264 compression, scaling and frame-rate conversion attacks. The typical system parameters reported for error decoding results represent them successfully. We also compared the proposed framework against the canonical watermarking method, JAWS, and a more recent quantization based method.

REFERENCES

[1] Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes Tomáš Filler, Member, IEEE, Jan Judas, Member, IEEE, and Jessica Fridrich, Member, IEEE page 920 IEEE transactions on Information forensics & security, sep 2011.

[2] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *Proc. 8th Int. WorkshopInf. 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.

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

[4] 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.

[5] 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, and R. Safavi-Naini, Eds., Calgary, Canada, Jun. 28–30, 2010, vol. 6387, Lecture Notes in Computer Science, pp. 161–177.

[6] J. Kodovský and J. Fridrich, "On completeness 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.

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

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities," in *Proc. 9th ACM Multimedia Security Workshop*, J. Dittmann and J. Fridrich, Eds., Dallas, TX, Sep. 20–21, 2007, pp. 3–14.