Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 10, October 2013, pg.5 – 13

RESEARCH ARTICLE

A Novel Syndrome Coding Scheme for Embedding and Minimizing Distortion in Steganography

PNS Lakshmi[1], Ch NP Latha[2]

[1]M.Tech (CSE), Sri Sai Madhavi Institute of Science & Technology, Mallampudi, Near Rajahmundry, East Godavari, Andhra Pradesh, Under JNTUK University

[2]Assistant Professor, CSE, Sri Sai Madhavi Institute of Science & Technology, Mallampudi, Near Rajahmundry, East Godavari, Andhra Pradesh, Under JNTUK University

[1] lakshmi_pokanati@yahoo.in, [2] latha7891@gmail.com

Abstract— Within the field of Computer Forensics, investigators should be aware that the method steganography can be an effective means that enables concealed data to be transferred inside of seemingly innocuous carrier files. Knowing what software applications are commonly available and how they work gives forensic investigators a greater probability of detecting, recovering, and then eventually denying access to the data that mischievous individuals and programs are openly concealing. Generally speaking, steganography brings science to the art of hiding data. The purpose of steganography is to convey a secret message inside of a conduit of misrepresentation such that the existence of the message is both hidden and difficult to recover when discovered. Essentially, the information hiding process in a steganographic system starts by identifying a cover medium's redundant bits. The embedding process creates a stego medium by replacing these redundant data bits with data from the hidden message. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so attackers can detect the distortions in the resulting stego medium's statistical properties. This paper provides a general methodology for embedding while minimizing an arbitrary additive distortion function in steganography.

Keywords— Distortion; Embedding; Key; Steganography; Watermarking

I. INTRODUCTION

Internet users frequently need to store, receive or send private information. The most common way to do this is to transform the information into a different form. The resulting data can be understood only by those who know how to return it to its original content. This method of protecting information is known as encryption or encoding. A major drawback to encoding is that the existence of data is not hidden. Data that has been encoded, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. A solution to this problem is called steganography. Steganography is the art and science of hiding information; a steganographic system thus embeds hidden

content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic data. Today, computer and network technologies provide easy-to-use communication channels for steganography method. Essentially, the information- hiding process in a steganographic system starts by identifying a cover medium's redundant data bits (those that can be modified without destroying that medium's integrity) [1]. The embedding process creates a stego medium by replacing these redundant data bits with data from the hidden message.

A classical steganographic system's security relies on the encoding system's confidentiality. An example of this type of system is a "Roman" general who shaved a slave's head and tattooed a message on it. After the hair grew back, the slave was sent to deliver the now-hidden information [2]. Although such a system might work for a time, once it is known, it is simple enough to shave the heads of all the people passing by to check for the hidden messages—ultimately, such a steganographic system fails. Modern steganography attempts to be detectable only if the secret information is known—namely, a secret key [3]. This is similar to Kerckhoffs' Principle in cryptography, which holds that a cryptographic system's security should rely solely on the secret key material [4]. For steganography to remain undetected, the unmodified cover medium must be kept in secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes.

Modern steganography's goal is to keep its mere presence undetectable, but the steganographic systems— because of their invasive nature—leave behind detectable traces in the cover medium. Even if secret data is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called as statistical steganalysis [5]. Essentially, steganographic communication senders and receivers agree on a steganographic system and a shared secret key that determines how a secret message is encoded in the cover medium. To send a hidden message, for example, John creates a new image with a digital camera. John supplies the steganographic system with his shared secret and his message. The steganographic system uses the shared secret key to determine how the hidden message should be encoded in the redundant bits. The result is a stego image that John sends to David. When David receives the image, he uses the shared secret and the agreed on steganographic system to retrieve the hidden message. Figure 1 shows an overview of the encoding step.

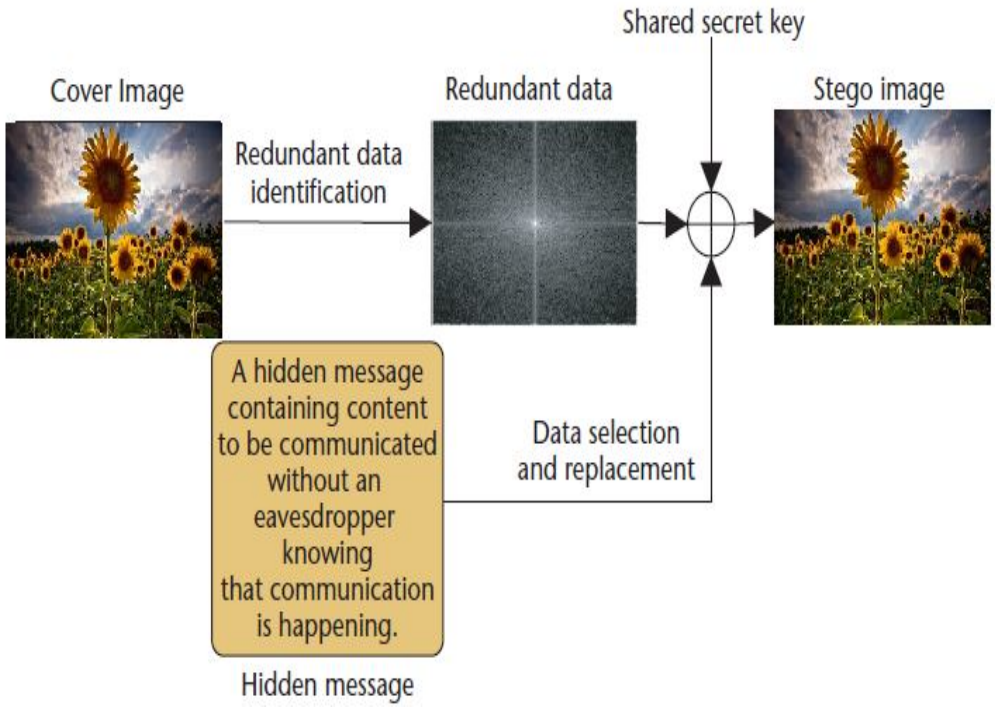

Fig 1. Steganographic communication

II. RELATED WORK

This section presents existing work regarding steganography. In [6], the authors utilize the robust watermarking scheme for steganography purposes. They embed secret data into image in the spatial domain by using a technique robust against JPEG compression. Their method provides less degradation onto the features of the DCT coefficients, and, as a result, its detectability was low against old version of the statistical steganalysis. Another way to survive against steganalysis is reducing the number of modified coefficients in the image. Traditionally, each non- zero DCT coefficient has been modified. As a result, embedding capacity is as much as the number of non- zero DCT coefficients. However, the maximum possible embedding capacity trades off the detectability. In [7], the authors has used a matrix encoding (ME) technique to lower detectability by sacrificing the embedding capacity. The encoding technique exploits the Hamming code which is designed for error correction. This scheme hides many bits by flipping at most one coefficient in each block. This approach was the first instance of using the error correcting codes for information hiding. In [8], the authors use the concept of the "minimal distortion" to enhance the security (i.e., by reducing distortion). The perturbed quantization steganography utilizes the wet paper coding technique.

Later, in [9], the authors have improved the performance of the ME by reducing the distortion impact. In fact, their modified matrix encoding (MME) method changes more number of coefficients compared to the ME. However, they show that the distortion impact after modifying one coefficient may be larger than that after modifying the two coefficients. Thus, it is obvious that modifying one coefficient or two per block may have less distortion and lower detectability against the steganalysis process. Note that matrix encoding requires the original uncompressed image for data hiding, but not for decoding. In [10], the authors have proposed a new way to hide data using more powerful error correction code. They use a structured Bose-Chaudhuri-Hochquenghem (BCH) coding technique [11]. In [12], the authors have significantly improved the original BCH-based data hiding scheme. Their improved method can easily find the flip positions and defeat the steganalysis well compared to the existing methods. Later, in [13], the authors apply a heuristic optimization technique for the data hiding scheme over the BCH coding and modify the stream of the input DCT coefficients to reduce the distortion.

III. 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 LSB method has intense affects on the statistical information of image like histogram. 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.

Limitations in Existing system

- Only the Least significant bit (LSB) is going to be effected every time
- The slight change in the cover image make the user to identify the message and this method can be easily cracked; it is more vulnerable to attacks.
- By using the histogram of the image the attacker can identify the hidden message

IV. PROPOSED SYSTEM

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:

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

c. The fourth less significant bit plane would alter (So the gray level of the pixel would increase or decrease by eight levels)

The concept of embedding in steganography that minimizes a distortion function is connected to many basic principles used for constructing embedding schemes for complex cover sources today, including the principle of minimal-embedding-impact, approximate model-preservation, or the Gibbs construction. The current work describes a complete practical framework for constructing steganographic schemes pre-processing. It consists of the following modules:

- Key Module
- Watermark embedding
- Authenticator Watermark
- Spread Spectrum
- Watermarked content

A. Key Module

The Key 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.

B. Watermark Embedding

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 (Figure 2).

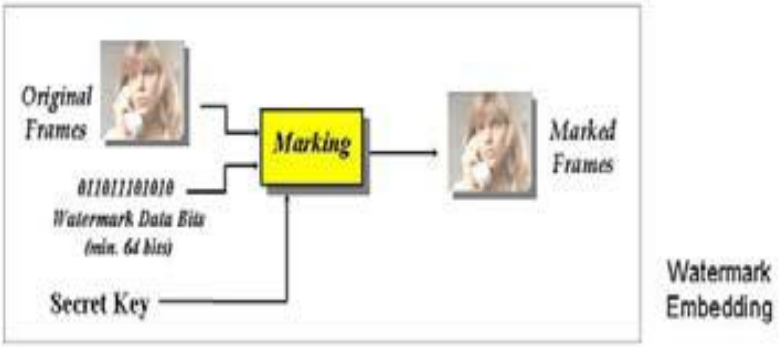

Fig 2. Watermark Embedding

C. 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.

D. 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.

E. Watermarked 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.

F. Advantages of proposed system

The advantages of our proposed system are:

- 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.

V. RESULTS

STEP1: This is a snapshot of user login page, where the user can login into the system.

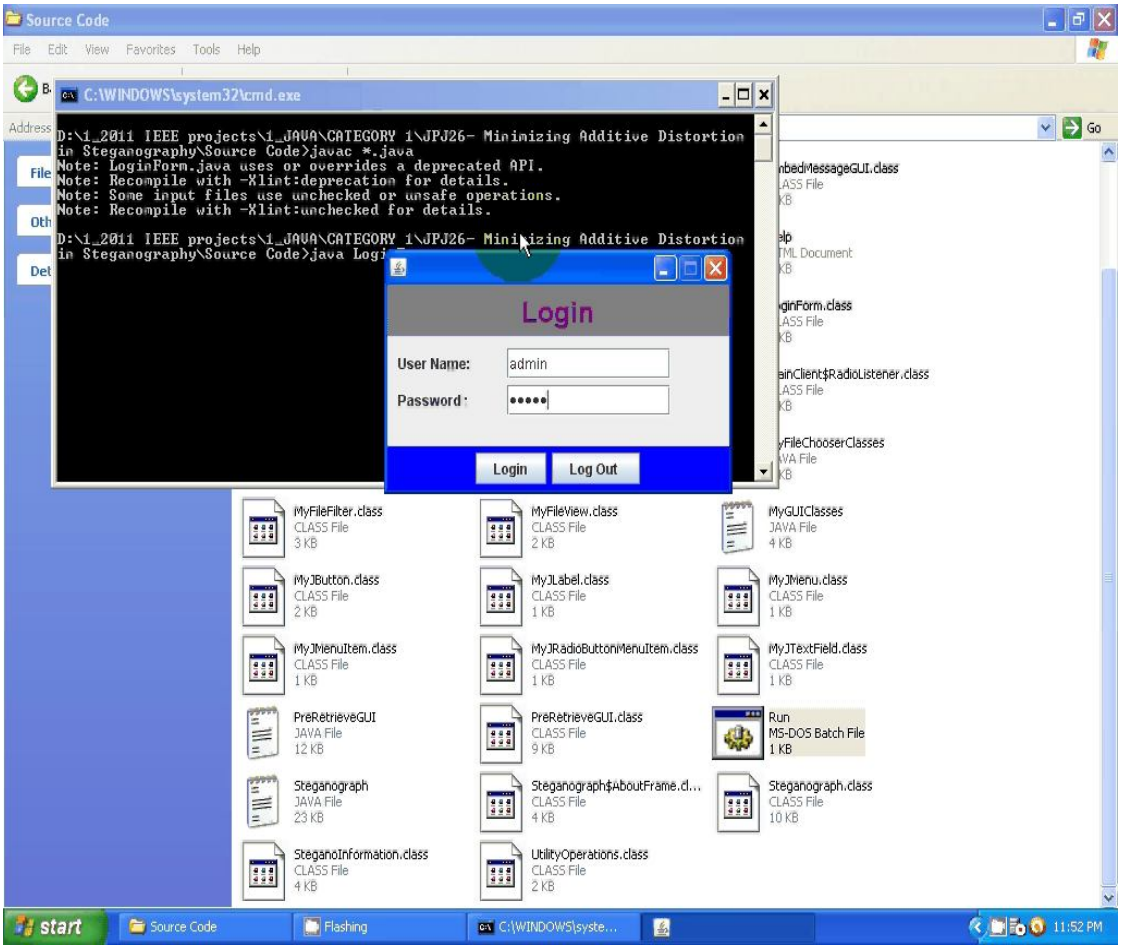

Fig 3. Login page

STEP 2: This is the Home page of the system where the user can select his option by clicking on the appropriate button

Fig 4. Home page

STEP 3: Next the user (sender) has to select a master file (here a jpeg image) to embed the secret information into it.

STEP 4: This is a snapshot in which the user is selecting the compression option to compress the master file to his required level.

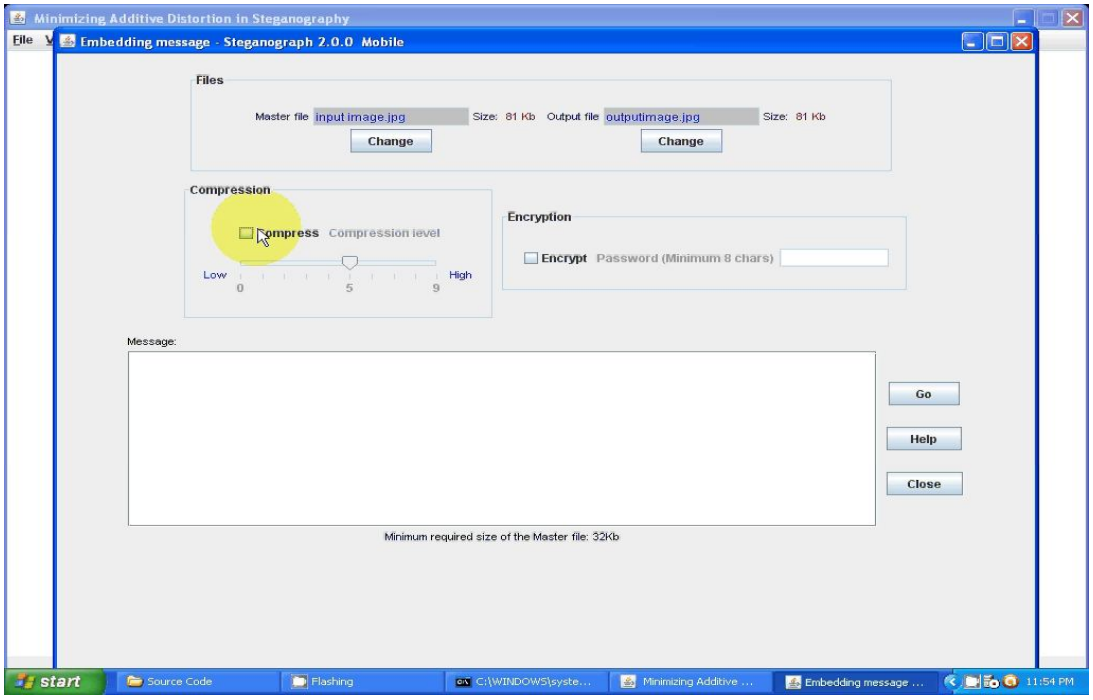

Fig 5. Compression level

STEP 5: This is a snapshot in which the user is inserting the message which he wants to hide into the file and password (secret key) to hide secret data into the image.

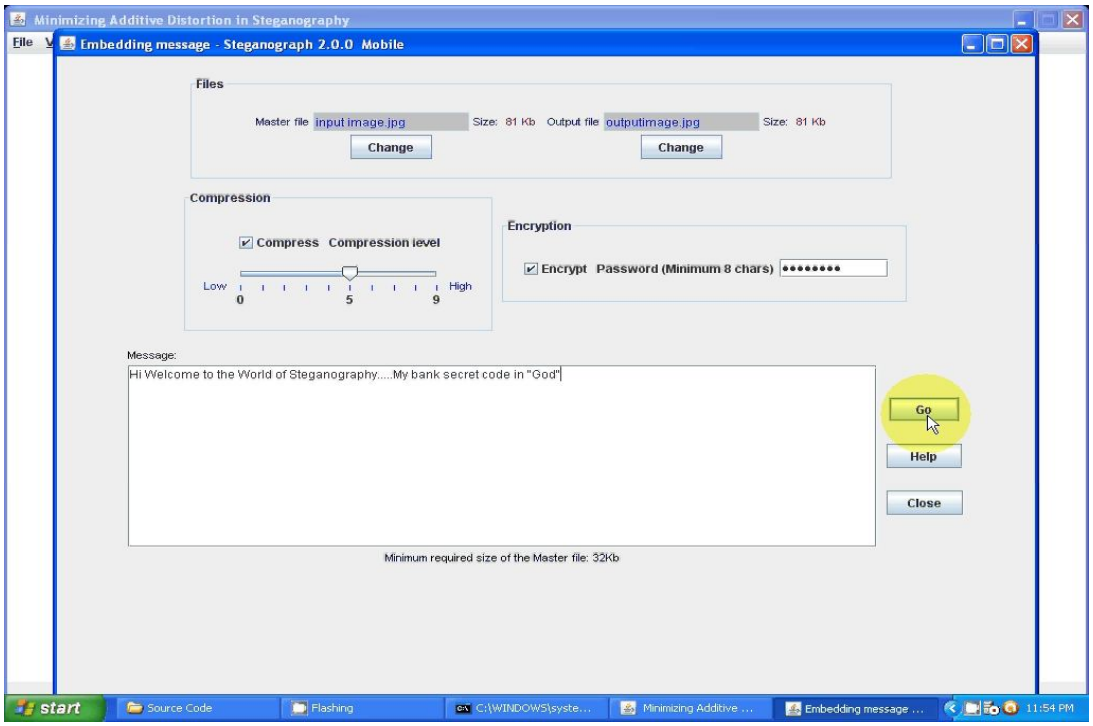

Fig 6. Entering secret message and password

Thus the secret information is embedded into the JPEG image, the result is shown below:

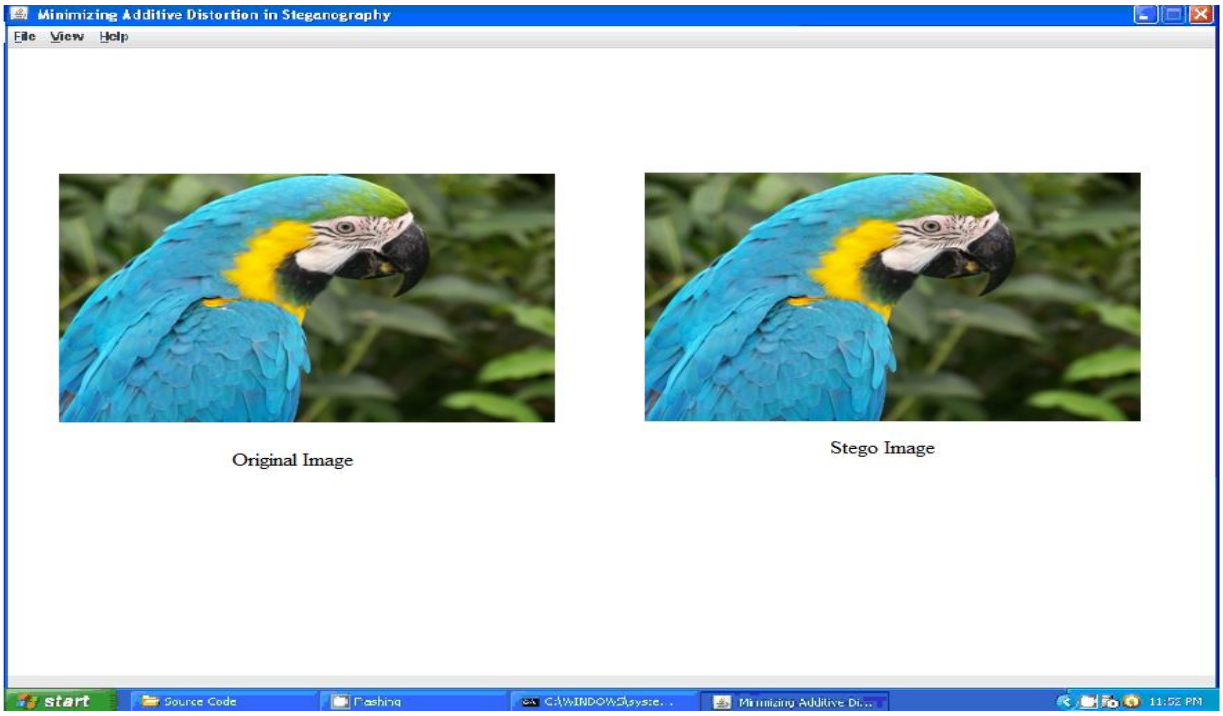

Fig 7. Original image and resultant stego image

STEP 6: This is a snapshot in which the receiver is inserting the password (key) into the encrypted zone to retrieve the file.

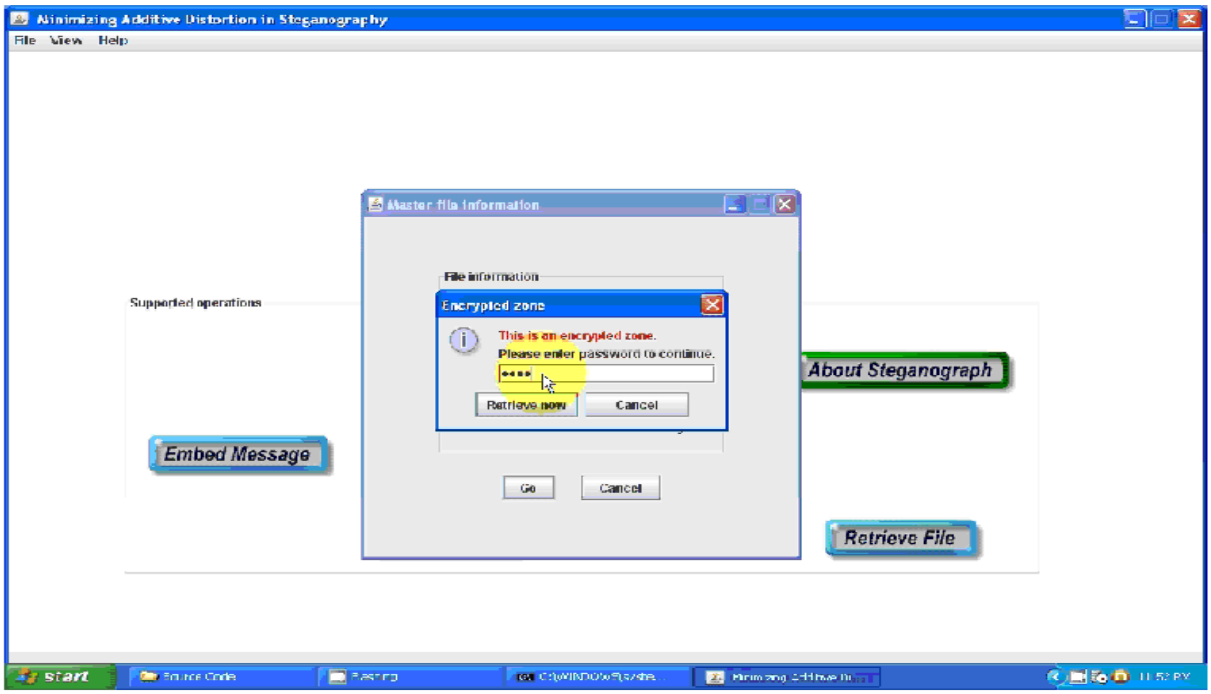

Fig 8. Decrypting message from stego image

VI. CONCLUSIONS

Steganography is the art of hiding secret information and an effort to conceal the existence of the embedded information. It serves as a better way of securing secret message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier (image or audio) such that the changes so occurred in the carrier are not observable. This paper provides a novel methodology for embedding while minimizing an arbitrary additive distortion. We present a complete methodology for solving the distortion- limited sender. The implementation described in this paper uses standard signal processing tools— such as convolutional codes with a trellis quantizer—and adapts them to our problem by working with their dual representation. These codes, which we call as syndrome-trellis codes (STCs), can directly improve the security of many existing steganographic schemes, allowing them to communicate larger payloads at the same embedding distortion or to decrease the distortion for a given payload.

REFERENCES

[1] Fridrich, J., [Steganography in Digital Media: Principles, Algorithms, and Applications], Cambridge University Press (2009).
[2] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, vol. 31, no. 2, 1998, pp. 26–34.
[3] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," Proc. IEEE, vol. 87, no. 7, 1999, pp. 1062–1078.
[4] A. Kerckhoffs, "La Cryptographie Militaire (Military Cryptography)," J. Sciences Militaires (J. Military Science, in French), Feb. 1883.
[5] R. Böhme, "Improved Statistical Steganalysis UsingModels of Heterogeneous Cover Signals," Ph.D. dissertation, Faculty of Comput. Sci., Technische Universität, Dresden, Germany, 2008.
[6] K Solanki, A Sakar, BS Manjunath, YASS: Yet another steganographic scheme that resists blind steganalysis. Lect Notes Comput Sci. 2939, 154–167 (2007).
[7] A Westfeld, High capacity despite better steganalysis (F5–a steganographic algorithm). Lect Notes Comput Sci. 2137, 289–302 (2001).
[8] J Fridrich, Minimizing the embedding impact in steganography, in Proc of ACM Multimedia and Security Workshop, Geneva, Switzerland, 2–10 (September 26–27, 2006).

[9] YH Kim, Z Duric, D Richards, Modified matrix encoding technique for minimal distortion steganography. Lect Notes Comput Sci. 4437, 314–327 (2006).
[10] D Schönfeld, A Winkler, Reducing the complexity of syndrome coding for embedding. Lect Notes Comput Sci. 4567, 145–158 (2008).
[11] J Eggers, R Bauml, B Girod, A communications approach to steganography, in Proc of EI SPIE, San Jose, CA, 4675, 26–37 (2002).
[12] R Zhang, V Sachnev, HJ Kim, Fast BCH syndrome coding for steganography. Lect Notes Comput Sci. 5806, 48–58 (2009).
[13] V Sachnev, HJ Kim, R Zhang, Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding, in Proc of ACM Workshop on Multimedia and Security, Princeton, NJ, 131–139 (September 7–8, 2009).

