IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. IV (July – Aug. 2015), PP 46-51
www.iosrjournals.org

Data Hiding Inside the Image Using Uniform Embedding Techniques

J. S. Harini, Student[1],
[1](*Computer Science and Engineering, Sitams College / JNTUA, INDIA)*

I. Introduction

The main aim of steganography is to hide data in the text media such as image, text, audio and video so that it cannot be identified by others. One of the advantages of steganography is that it can be used to transmit the secret messages without knowing the fact of transmission being discovered.
In existing there are three effective methods applied to image steganography are

1. Least Significant Bit (LSB) substitution
2. Blocking
3. Palette Modification.

The process of checking the bit of pixels into carrier image is known as LSB substitution.LSB is the most powerful steganographic method which lends itself.

To maintain the confidentiality and integrity of data to prevent them from unauthorized persons. Transmitting the military data and data related to economic, industrial organization towards the information pertaining the institutions of finance and business must be confidential for transferring of data. As a result there is a need of information hiding which explains the general methods and techniques used in the area of security and confidentiality of information security for transferring them from one end to other this is one kind of problem emerged by the various means of communication.

Encryption is the most important method used for transferring confidential data from one format to another format using certain was by the sender and the recipient restores it to the original form. The term steganography was derived from Greek terminology. The term stegano means hiding or restricting and the term graphy means text, drawing or writing. This method was existing from the Greeks age which was later developed on the advancement of communication. With the advancement of communication security has become an important issue. Steganography is used to hide the secret data inside other objects such as text images audio and video to protect the confidential data. After hiding the image it should be seen as singular object and as well as materialistic. The intruder will feel difficult to discover the stego object upon its transferring among the internet until it reaches extraction of secret data.

Problem Definition:

The art and science of hiding information by embedding messages with in other terminology harmless messages. Steganography works by replacing bits of useless or unused data in regular computer file (such as graphics, format, text, and html) with bits of different invisible information. There is a need for an algorithm to embed the message. This algorithm uses simple or complex LSB embedding in the spatial domain. The hiding process starts with embedding bits of the message in to the image. In LSB insertion technique we use the least significant bit to embed the message. To improve the embedding capacity, two or more bits in a pixel are used to embed messages by changing the LSB of pixel in a sequential order.

The techniques that are available today are invisible to a human senses and most of it takes a gray color images as a special case. In order to embed a text message using a color image as a cover, two or more aspects must be considered:

1. Choose the pixel to embed.
2. Using a randomization technique by changing the LSB pixels to embed messages.

Objectives:

The main objectives are:

1. To select the pixel for an embedding a new technique is developed and designed.
2. Reduce the size for embedding the text.
3. To resist extraction process a high degree of confidentiality is given.

Significance of the problem:

A special kind of problem is categorized through the digital image steganography problem, till now, there is no proper technique used to solve this problem, but many suggested algorithms give us good results. The LSB of the pixels in a BMP image mainly focuses on hiding the text message.

In order to get some results about its ability to make the message store in a random way the study will mainly focus on choosing a pixel to embed a part of the text message under a conditional value.

Since ancient times the term steganography exists and many of general assumptions apply till now. In the area of invisible digital watermarking motivated by the desire for copyright protection of multimedia through internet is the most of recent work undergone through steganography.

To signify origin or ownership of the digital cover signal within a signature embedded is the objective of the digital watermarking. To embed a amount of data signified more than that of a serial number or signature within the cover signal is the objective of steganography.

II. Literature Survey

1. Minimizing additive distortion in steganography using syndrome-trellis codes

This paper proposes a complete practical methodology for minimizing additive distortion in steganography with general (nonbinary) embedding operation. Let every possible value of every stego element be assigned a scalar expressing the distortion of an 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. Without any loss of performance, the nonbinary case is decomposed into several binary cases by replacing individual bits in cover elements. The binary case is approached using 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 the number of covers elements. We report extensive experimental results for a large set of relative payloads and for different distortion profiles, including the wet paper channel. 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.

2. Modified matrix encoding technique for minimal distortion steganography

It is well known that all information hiding methods that modify the least significant bits introduce distortions into the cover objects. Those distortions have been utilized by steganalysis algorithms to detect that the objects had been modified. It has been proposed that only coefficients whose modification does not introduce large distortions should be used for embedding. In this paper we propose an efficient algorithm for information hiding in the LSBs of JPEG coefficients. Our algorithm uses modified matrix encoding to choose the coefficients whose modifications introduce minimal embedding distortion. We derive the expected value of the embedding distortion as a function of the message length and the probability distribution of the JPEG quantization errors of cover images. Our experiments show close agreement between the theoretical prediction and the actual embedding distortion. Our algorithm can be used for both steganography and fragile watermarking as well as in other applications in which it is necessary to keep the distortion as low as possible.

3. Design of adaptive steganographic schemes for digital image

Most steganographic schemes for real digital media embed messages by minimizing a suitably defined distortion function. In practice, this is often realized by syndrome codes which offer near-optimal rate-distortion performance. However, the distortion functions are designed heuristically and the resulting steganographic algorithms are thus suboptimal. In this paper, we present a practical framework for optimizing the parameters of additive distortion functions to minimize statistical detectability. We apply the framework to digital images in both spatial and DCT domain by first defining a rich parametric model which assigns a cost of making a change at every cover element based on its neighbourhood. Then, we present a practical method for optimizing the parameters with respect to a chosen detection metric and feature space. We show that the size of the margin between support vectors in soft-margin SVMs leads to a fast detection metric and that methods minimizing the margin tend to be more secure blind steganalysis. The parameters obtained by the Nelder--Mead simplex-reflection algorithm for spatial and DCT-domain images are presented and the new embedding methods are tested by blind steganalyzers utilizing various feature sets. Experimental results show that as few as 80 images are sufficient for obtaining good candidates for parameters of the cost model, which allows us to speed up the parameter search.

4. Digital image steganography using universal distortion

Currently, the most secure practical steganographic schemes for empirical cover sources embed their payload while minimizing a distortion function designed to capture statistical detectability. Since there exists a general framework for this embedding paradigm with established payload-distortion bounds as well as near-optimal practical coding schemes, building an embedding scheme has been essentially reduced to the distortion design. This is not an easy task as relating distortion to statistical detectability is a hard and open problem. In this article, we propose an innovative idea to measure the embedding distortion in one fixed domain independently of the domain where the embedding changes (and coding) are carried out. The proposed universal distortion is additive and evaluates the cost of changing an image element (e.g., pixel or DCT coefficient) from directional residuals obtained using a Daubechies wavelet filter bank. The intuition is to limit the embedding changes only to those parts of the cover that are difficult to model in multiple directions while avoiding smooth regions and clean edges. The utility of the universal distortion is demonstrated by constructing steganographic schemes in the spatial; JPEG, and side-informed JPEG domains, and comparing their security to current state-of-the-art methods using classifiers trained with rich media models.

5. Reversible Data Embedding Using a Difference Expansion

In this paper, we present a novel reversible data embedding method for digital images. We explore the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low.

6. On Compressing Encrypted Data

In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. Although counter-intuitive, we show surprisingly that, through the use of coding with side information principles, this reversal of order is indeed possible in some settings of interest without loss of either optimal coding efficiency or perfect secrecy.

III. Indentations and Equations

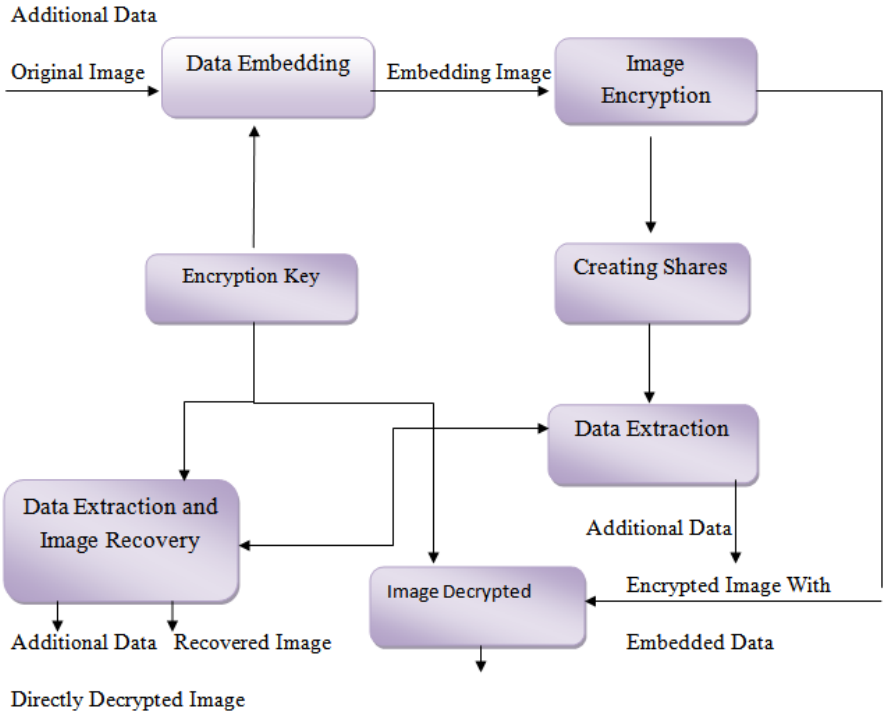
Steganography Terminology

Steganography system is divided into two operations as detailed below:

1- Embedding process: from which it can choose the cover then put secret messages included using the stego key that contains the secret message Stego Cover.

2- Extraction process: From which to extract the secret message using the secret key, and can be watched through the lid are moving between the sender and the recipient by the attackers who have no right to extract the secret message.

System Architecture



Reversible Data Hiding:

Reversible Data hiding Images is a technique, by which the original cover can be loss lessly recovered after the embedded message is extracted. In theoretical aspect, Kalker and Willems established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memory less covers and proposed a recursive code construction which, however, does not approach the bound. Improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers.

Images encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few RDH techniques in encrypted images have been published yet, there are some promising applications if RDH can be applied to encrypted images. In advocated a reputation-based trust management scheme enhanced with data coloring (a way of embedding data into covers) and software watermarking, in which data encryption and coloring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted data. Thus, a reversible data coloring technique based on encrypted data is preferred. Suppose a medical image database is stored in a data center, and a server in the data center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage the image or verify its integrity without having the knowledge of the original content, and thus the patient's privacy is protected. On the other hand, a doctor, having the cryptographic key, can decrypt and restore the image in a reversible manner for the purpose of further diagnosing.

Extracting Data from Encrypted Images:

To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of our work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

Extracting Data from Decrypted Images:

In Case, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the images' owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images. Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decrypted images, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case. Next, we describe how to generate a marked decrypted image.

Image Partition:

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition is to construct a smoother area , on which standard RDH algorithms such as can achieve better performance. To do that, without loss of generality, assume the original image is an 8 bits gray-scale image with its size and pixels.

Image Encryption:

After rearranged self-embedded image, denoted by , is generated, we can encrypts to construct the encrypted image, denoted by .With a stream cipher, the encryption version of is easily obtained. For example, a gray value ranging from 0 to 255 can be represented by 8 bits, , such that The encrypted bits can be calculated through exclusive- or operation where is generated via a standard stream cipher determined by the encryption key. Finally, we embed 10 bits information into LSBs of first 10 pixels in encrypted version of to tell data hider the number of rows and the number of bit-planes he can embed information into. Note that after image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

Data Hiding in Encrypted Image:

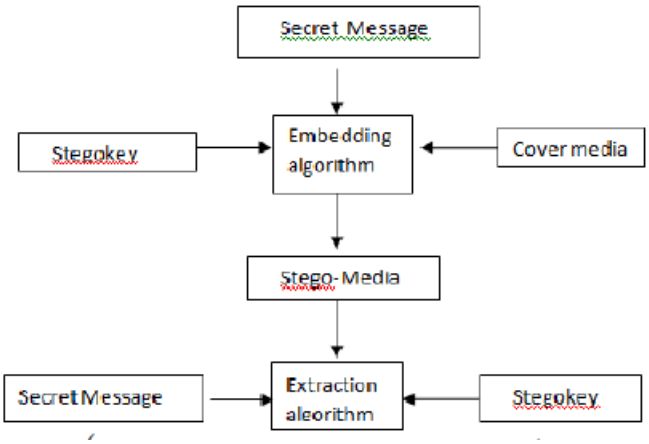
Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of , denoted by . Since has been rearranged to the top of , it is effortless for the data hider to read 10 bits information in LSBs of first 10 encrypted pixels. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following to point out the end position of embedding process and further encrypts according to the data hiding key to formulate marked encrypted image denoted by. Anyone who does not possess the data hiding key could not extract the additional data.

LSB: least significant bits

The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000).

Least significant bits are frequently employed in pseudorandom number generators, hash functions and checksums. LSB, in all capitals, can also stand for "Least Significant Byte". The meaning is parallel to the above: it is the byte (or octet) in that position of a multi-byte number which has the least potential value in Steganography a message might be hidden or encrypt with in in an image by changing least significant bit to be the message bits then the image can be transmitted through network.lsb based Steganography is perhaps the most simple and straight forward approach . in this will only affect each pixel by +\-1, if at all ,it is generally assumed with good reason that degradation caused by this embedding process would perceptually transparent. hence there are number of lsb based Steganography techniques in the passive warden model as it difficult to differentiate cover-image from stego images ,given the small changes that have been made.

There are many methods for steganography ,to hide the secret message into the image.LSB is the well known method for data hiding. The approaches for steganography that are based on LSB can be found .The another is PVD Method i.e. pixel-value differencing method divides the cover image into blocks and modifies the pixel difference in each block for data embedding. Gray-level modification Steganography is a technique to map data by modifying the gray level values of the image pixels. It uses the odd and even numbers to map data within an image.



A Novel Steganographic Technique for Hiding Text behind Image

There are two major steps. First one is embedding the secret message in cover media using stegokey the second one is extracting the secret message from the cover media using stegokey.For extraction the secret message from the stego-media the recipient must have the stego-key.

Color histogram Techniques

In image processing and photography, a color histogram is a representation of the distribution of colors in an image. For digital images, a color histogram represents the number of pixels that have colors in each of a fixed list of color ranges, that span the image's colour, the set of all possible colors. The color histogram can be built for any kind of color space, although the term is more often used for three-dimensional spaces like RGB or HSV. For monochromatic images, the term intensity histogram may be used instead. For multi-spectral images, where each pixel is represented by an arbitrary number of measurements (for example, beyond the three measurements in RGB), the color histogram is *N*-dimensional, with N being the number of

measurements taken. Each measurement has its own wavelength range of the light spectrum, some of which may be outside the visible spectrum. If the set of possible color values is sufficiently small, each of those colors may be placed on a range by itself; then the histogram is merely the count of pixels that have each possible color. Most often, the space is divided into an appropriate number of ranges, often arranged as a regular grid, each containing many similar color values. The color histogram may also be represented and displayed as a smooth function defined over the color space that approximates the pixel counts.

IV. Conclusion

The effectiveness of the proposed scheme is verified with evidence obtained from exhaustive experiments using popular steganalyzers with various feature sets on the BOSSbase database. Compared with prior arts, the proposed scheme gains favourable performance in terms of secure embedding capacity against steganalysis.

Acknowledgements

The authors would like to thank the anonymous reviewers and associate editor for their comments that greatly improved the manuscript.

I express my heartful thanks to my project guide **Dr. P. NEELAKANTAN,** for his guidance and support at each and every stage of the project.

References

Theses

[1]. (Piyush Goel),Data Hiding in Digital Images: A Steganographic Paradigm

[2]. (Dr. Oleg Victorov), Enhancement of A Steganographic algorithm for Hiding Text Messages in Images

Websites

WWW.google.com

[3]. T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion insteganography using syndrome-trellis codes," IEEE Trans. Inf. ForensicsSecurity, vol. 6, no. 3, pp. 920–935, Sep. 2011.(Ref no.1.)