OPTIMIZING COST USING KNIGHT TOUR FOR CONTENT ADAPTIVE STEGANOGRAPHY

S.Monisa[1], P.Ganesh Kumar PhD[2]

[1]PG Scholar, [2]Assistant Professor, Dept of IT Anna University Coimbatore (India)

ABSTRACT

Steganography includes all the actions that must be transported out to hide and protect the secret data inside the cover image encryption. In the first step of the embedding phase, the plain text will be encrypted, there are several encryption methods that can be applied to encrypt the data, but in this situation, we need a method that does not produce a cipher text longer than the plain text. The embedding algorithm is the most prominent part of the steganographic methods. In fact, it defines which pixels of the image should be changed and also in what order they will be altered with the secret data. The embedding algorithm of the proposed steganographic method is based on the described "Knight Tour" algorithm. The "Knight tour" algorithm is a suitable technique to formulate the sequence of the secret bit stream within the image pixels. When the sequence of the target pixels is defined in the previous step, now it's the time to replace the least significant bits of the image pixels with the bit stream of the secret message.

Keywords : Stegnography, Encryption, Knight Tour, PSRM, PPM,

I. INTRODUCTION

Steganography has been an important subject since people started communicating in writing. Steganography means hiding a secret message the embedded message within a larger one source cover in such a way that an observer cannot detect the presence of contents of the hidden message. Today the growth in the information technology, especially in computer networks such as Internet, Mobile communication and Digital Multimedia applications such as Digital camera, handset video etc. has opened new opportunities in scientific and commercial applications. But this progress has also led to many serious problems such as hacking, duplications and malevolent usage of digital information. Steganography finds its role in attempt to address these growing concerns.

The basic idea is to use the values of pixel pair as a reference coordinate, and search a coordinate in the Neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information

even exists. The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as cover-object which the message is embedded and serves to hide the presence of the message.

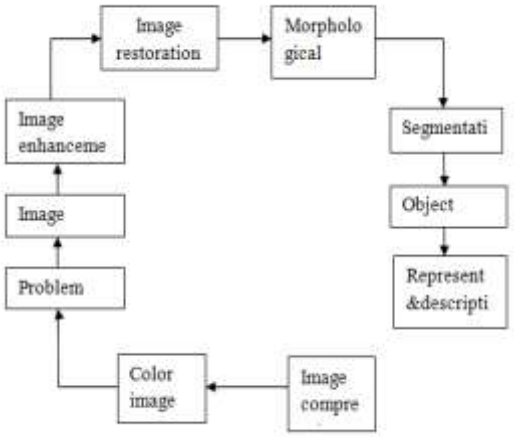

Fig 1.1 Key stages of Digital Image processing

The key stages of image processing is image acquisition, image enhancement, image restoration, morphological processing, segmentation, object recognition, and represent and description can be performed in images. These stages can be processed from color images or any other images.

Relating the embedding cost in a distortion function to statistical detectability is an open vital problem in modern steganography we propose some rules for ranking the priority profile for spatial images. Following such rules, we propose a five-step cost assignment scheme. Previous steganographic schemes, such as HUGO, WOW, S-UNIWARD, and MG, can be integrated into our scheme.

II. RELATED WORK

In an attempt to alleviate the negative impact of unavailable cover model, some stegano graphic schemes utilize the knowledge of the so-called “precover” when embedding secret data. The precover is typically a higher resolution (unquantized) representation of the cover, such as the raw sensor output before it is converted to an 8-bit per channel color image. The precover object is only available to the sender but not to the Warden, which seems to give a fundamental advantage to the sender. Provide theoretical insight for why side-informed embedding schemes for empirical covers might provide high level of security. By adopting a piece-wise polynomial model corrupted by AWGN for the content, we prove that when the cover is sufficiently non-stationary, embedding by minimizing distortion with respect to the precover is more secure than by preserving a model estimated from the cover (the so-called model-based steganography). Moreover, the side-informed embedding enjoys four times lower steganographic Fisher information than LSB matching.

A standard way to design steganalysis features for digital images is to choose a pixel predictor, use it to compute a noise residual, and then form joint statistics of neighboring residual samples (co-occurrence matrices). Proposes a general data-driven approach to optimizing predictors for steganalysis. First, a local pixel predictor is parameterized and then its parameters are determined by solving an optimization problem for a given sample of

cover and stego images and a given cover source. Our research shows that predictors optimized to detect a specific case of steganography may be vastly different than predictors optimized for the cover source only. The results indicate that optimized predictors may improve steganalysis by a rather non-negligible margin. Furthermore, we construct the predictors sequentially having optimized *k* predictors, design the *k* + 1st one with respect to the combined feature set built from all *k* predictors. In other words, given a feature space image model extend diversify the model in a selected direction functional form of the predictor in a way that maximally boosts detection accuracy.

Steganography has been an important subject since people started communicating in writing. Steganography means hiding a secret message the embedded message within a larger one source cover in such a way that an observer cannot detect the presence of contents of the hidden message. Today the growth in the information technology, especially in computer networks such as Internet, Mobile communication, and Digital Multimedia applications such as Digital camera, handset video etc. has opened new opportunities in scientific and commercial applications. But this progress has also led to many serious problems such as hacking, duplications and malevolent usage of digital information. Steganography finds its role in attempt to address these growing concerns. We know that, with the use of steganographic techniques, it is possible to hide information within digital images and video files which is perceptually and statistically undetectable. Proposes a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit.

The traditional way to represent digital images for feature based steganalysis is to compute a noise residual from the image using a pixel predictor and then form the feature as a sample joint probability distribution of neighboring quantized residual samples the so-called co-occurrence matrix. In this paper, we propose an alternative statistical representation instead of forming the co-occurrence matrix; we project neighboring residual samples onto a set of random vectors and take the first-order statistic histogram of the projections as the feature. When multiple residuals are used, this representation is called the projection spatial rich model (PSRM). On selected modern steganographic algorithms embedding in the spatial, JPEG, and side-informed JPEG domains, we demonstrate that the PSRM can achieve a more accurate detection as well as a substantially improved performance versus dimensionality trade-off than State-of-the-art feature sets .Enhancing the security of the traditional LSB matching, two improved LSB-matching methods are proposed. In the steganograhical procedure, the Markov chain distance based on the second-order statistics is chosen as the security metric to control the modification directions of ±1 embedding. The first method is based on stochastic modification, which directly determines the modification directions by the empirical Markov transition matrix of a cover image and the pseudorandom number generated by a pseudorandom number generator. The second one is based on genetic algorithm, which is used to find the optimum matching vector to make the security metric as small as possible. Experiments show the proposed algorithms outperform LSB matching and LSB replacement in a sense of the first order and second-order security metrics. And the adjacent calibrated COM-HCF steganalytical tests also show that the two algorithms are more secure than the traditional ones.

III. SYSTEM ARCHITECTURE DESIGN

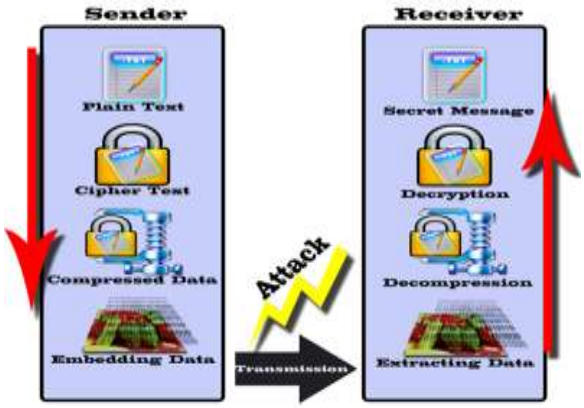

Fig 3.1. Architecture design

3.1 Module Description

- Two-phase perspective on cost assignment and Different techniques of Steganography
- New cost assignment scheme
- Experimental results using Stego images

3.2 Two-Phase Perspective On Cost Assignment

We explore a different perspective on the cost assignment scheme. We conceptually separate the assignment process into two phases. First, we sort image elements in an order where the elements after modification leading to better undetectability are ranked higher. We call the ranking order as priority profile.

In the second phase, we assign cost-values, which follow a specified distribution (called a cost - value distribution), to the corresponding image elements. In this way, the security impact of the cost assignment can be regarded as being determined by two factors — priority profile and cost-value distribution. If these two factors are independent, we may optimize them separately to enhance the security performance. In the following subsections, we will investigate their roles in steganographic security.

3.2.1 Different techniques of Steganography

A. Spatial Domain based Steganography

It includes LSB (Least Significant Bit) Steganography. The spatial methods are most frequently employed because of fine concealment, great capability of hidden information and easy realization. LSB Steganography includes two schemes:

- Sequential Embedding
- Scattered Embedding.

B. Transform Domain based Steganography

The method of transform domain Steganography is to embed secret data in the transform Coefficients.

C. Document based Steganography

This method embeds data in documents files by adding tabs or spaces to .txt or .doc files.

D. File Structure based Steganography

This method inserts secrets data in the redundant bits of cover files, such as the reserved bits in the file header or the marker segments in the file format.

3.3 NEW COST ASSIGNMENT SCHEME

First present a new cost assignment scheme. Then explain the naming syntax for different options in the proposed scheme. Then discuss how to enhance the performance of previous methods by integrating them into our scheme. Finally presenting the general method to enrich the ways of obtaining priority profile.

3.4 Experimental Results Using Stego Images

The experiments in this section are conducted on BOSS Base version 1.01 with 10000 gray scale images of size 512 × 512. The performances are evaluated by using steganalyzer with a 32671-D SRM feature set and an ensemble classifier, where Fisher linear discriminates is used as base learners. A number of 5000 randomly selected cover images and their Stego counterparts are used for training, while the rest 5000 cover images and their Stego counterparts are used for testing. The performance is evaluated by the testing error, which is the average of the false positive rate and the false negative rate, and we find that the testing error is usually slightly lower than the ensemble's "out-of-bag" error.

IV. IMPLEMENTATION

The MATLAB language supports the vector and matrix operations that are fundamental to engineering and scientific problems. It enables fast development and execution. With the MATLAB language, you can program

and develop algorithms faster than with traditional languages because you do not need to perform low-level administrative tasks, such as declaring variables, specifying data types, and allocating memory. In many cases, MATLAB eliminates the need for 'for' loops. As a result, one line of MATLAB code can often replace several lines of C or C++ code. At the same time, MATLAB provides all the features of a traditional programming language, including arithmetic operators, flow control, data structures, data types, object-oriented programming (OOP), and debugging features.

MATLAB is a wide range of applications, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational biology. Add-on toolboxes (collections of special-purpose MATLAB functions, available separately) extend the MATLAB environment to solve particular classes of problems in these application areas. MATLAB provides a number of features for documenting and sharing your work. You can integrate your MATLAB code with other languages and applications, and distribute your MATLAB algorithms and applications.

4.1. Steganographic Algorithm

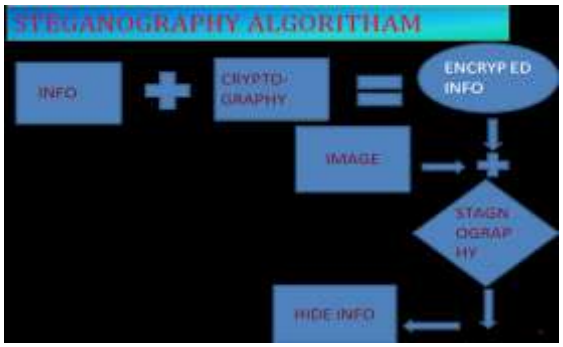

Fig 4.1 Steganography Algorithm

The information is combined with the image and it is encrypted by cryptography and then compressed these things and it changes into stenography which hides the information.

4.2 Knight Tour Algorithm

The "Knight tour" algorithm is a suitable technique to formulate the sequence of the secret bit stream within the image pixels. The advantage of the knight tour method over the PRNG technique is that, it is a self-developed algorithm based on the knight tour mathematical problem and it is almost unknown for the unintended receivers. By considering the image as an extended chessboard, we can have an algorithm, which determines the path of the knight within the image. The solution of the "Knight Tour" problem divides the chess board into the blocks with the size of 4x4 squares.

4.3 Performance Analysis

The general architecture of the proposed steganography method is designed and implemented. The whole process is composed of two main phases, which are embedded phase and Receiving phase.

- **Embedding Process** - This phase includes all the activities that must be carried out to hide and protect the secret data inside the cover image. The sender uses some algorithms to encode and compress the data and then embeds the bit stream into the image. Moreover, the secret key is defined as the first position of the bit stream within the image. This key is identified just for the sender and receiver.
- **Receiving Phase** - On the other side of the communication line, the receiver should be able to comprehend the secret data within the Stego image. Therefore, another procedure is required to recover the content of the message and restructure it. First of all, base on the stego key and the extracting algorithm (the same as sender side) the bits of the secret message are obtained to compose a compressed data. Then the unzipping algorithm will generate the encrypted data and finally the plain message will be revealed.

V. RESULT

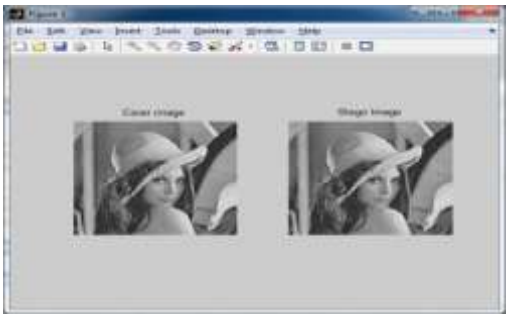

Fig 5.1 Encrypted Image

5.2 Hiding Images

Fig 5.3 Encrypted Data

VI. CONCLUSION

In this work, we decided to fix the weakness of the Simple LSB system by providing some enhancements. The Enhanced LSB method utilizes three fundamental improvements specifically embedding algorithm, encryption

and compression. The process starts with the encoding the confidential information by using encryption techniques. Both of the sender and receiver have a secret key which is used in encryption and decryption phases. Afterward, the compression technique reduces the size of encrypted data to improve the payload capacity. Clearly, as much the length of input data increases, the rate of compression surges, as well. Finally, the generated bit streams are embedded into the image in the positions which are defined by the proposed embedding algorithm. The aforesaid embedding method is an extended form of proposed algorithm and provides the maximum number of pixels to hide the secret message.

REFERENCES

[1] Böhme R. (2010) *Advanced Statistical Steganalysis. Berlin, Germany:* Springer-Verlag.

[2] Bin Li, *Member*, Shunquan Tan, *Member*, Ming Wang, and Jiwu Huang, *Senior Member*, *(*2014) 'Investigation on Cost Assignment in Spatial Image Steganography', *IEEE Transactions On Information Forensics And Security*, vol. *9*, no. *8*.

[3] Chen L. Shi Y.Q Sutthiwan P and Niu X. (2013) 'A novel mapping scheme for steganalysis', in *Digital Forensics and Watermaking* (Lecture Notes in Computer Science), vol. 7809. Berlin, Germany: Springer-Verlag, pp. 19–33.

[4] Chonev V.K and Ker A.D. (2011) 'Feature restoration and distortion metrics', *Proc. SPIE*, vol. 7880, pp. 0G01–0G14,

[5] Fridrich J. and Kodovský J. (2012) 'Rich models for steganalysis of digital images', *IEEE Trans. Inf. Forensics Security, vol. 7, no. 3,* and pp. 868–882.

[6] Fridrich J. (*2009) 'Steganography in Digital Media Principles', Algorithms, and Applications Cambridge, U.K, Cambridge Univ. Press.*

[7] Holub V. Fridrich J. and Denemark T. (2013) 'Random projections of residuals as an alternative to co-occurrences in steganalysis', *Proc. SPIE*, vol. 8665, p. 86650L.

[8] Huang F, Huang J. and Shi Y.Q. (2012) 'New channel selection rule for JPEG steganography', *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1181–1191.

[9] Ker A. D *et al., (2013) 'Moving steganography and steganalysis from the* laboratory into the real world', in *Proc. 1st ACM Workshop Inform. Hiding Multimedia Security, pp. 45–58.*

[10] Kodovský J. Fridrich J. and Holub V. (2012) 'Ensemble classifiers for steganalysis of digital media', *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444.

[11] Li B.J. He Huang J. and Shi Q.Y (2011) 'A survey on image steganography and steganalysis', J. Inform. Hiding Multimedia Signal Process vol. 2, no. 2 pp. 142–172.

[12] Mielikainen J. (2006) 'LSB matching revisited', *IEEE Signal Process. Lett.* vol. 13, no. 5, pp. 285–287.

[13] Pevný T. Bas P. and Fridrich J. (2010) 'Steganalysis by subtractive pixel adjacency matrix,' *IEEE Trans. Inf. Forensics Security, vol. 5, no. 2,* pp. 215–224.