An Enhancement in Quality of image & Anti-Steganalysis by Using Optimizing Image Steganography

Anuradha Kasande, A.A. Agarkar

Abstract— Picture quality and statistical undetectability are two main issues related to steganography techniques. In this paper, a closed-loop computing framework is proposed that iteratively searches proper modifications of pixels/coefficients to enhance a base steganographic scheme with optimized picture quality and higher anti-steganalysis capability. To achieve this goal, an anti-steganalysis tester and an embedding controller based on the optimization algorithm with a cost function are incorporated into the processing loop to conduct the convergence of searches. The cost function integrates several performance indices, namely, the mean square error, the human visual system (HVS) deviation, and the differences in statistical features, and guides a proper direction during optimization.

Index Terms— steganalysis, steganography, optimization

I. INTRODUCTION

Steganography word is of Greek origin and essentially means concealed writing. Protection of the transmitted data from being intercepted or tampered has led to the development of various steganographic techniques.

The data hiding process starts by identifying a cover image's redundant bits, i.e., those that can be modified without destroying its integrity. The embedding process then creates stego-image by replacing subset of these redundant bits with the bits of the message to be hidden. In digital image steganography, the secret message is embedded within a digital image called cover-image. Cover-image carrying embedded secret data is referred as stego-image.

In image Steganography secret message is hidden in a digital picture. Image steganography takes the advantage of limited power of human visual system (HVS).For all pixels present in an image and each pixel has basically three color numbers, there are zillions of numbers in an image. If we change a few of these color numbers the resulting picture would probably look a lot like the original image; in fact, most people probably couldn't tell that you had changed the image at all. Steganography works by changing a few pixel color values; we will use selected pixel values to represent characters instead of a color value. Of course, the resulting image will still look mostly like the original except that a few tiny 'blips' might seem a little out of place if you look very closely. We can then send the image to a buddy and they can extract the message if they know which pixels to decode.

Manuscript received February 2014.

Anuradha Kasande, Sun Paradise-II, Vadgaon, Pune (Maharashtra), India
A.A. Agarkar, Sun Paradise-II, Vadgaon, Pune (Maharashtra), India

There are several parameters to measure the performance of the steganographic system which are imperceptibility, robustness, and embedding capacity.

1. Imperceptibility is the primary parameter that is required for steganographic system to fulfill. It shows how difficult for third party to determine whether there is a hidden data in the stego-media or not. In other word it represents the ability to avoid attention of third party from detecting the stego-media. For example, people do not know there is a hidden message in image and when comparing the image with hidden message with original image, there is no difference between the two. Even though, no human eyes can detect the hidden message, there is possibility the stego-media being attacked by statistical attack. Thus, truly secure steganographic should not be undetectable either by human eyes or statistical attack.
2. Robustness here means how well the steganography systems resist the attempt of third party to extract hidden data. Some examples of distortion to hidden data that interceptors are attempting to do are image manipulation such as cropping and rotating the image, data compression and image filtering.
3. Embedding capacity is an important feature for steganography. Payload capacity or steganographic capacity shows the maximum information that can safely embedded in a stego-media without being statistically detectable. More the hidden message that are intended to embed in carrier, the more alteration should be made to the carrier which consequently turn out the stego-media to be detected by third party easily.

II. OPTIMIZATION

Optimization is a mathematical discipline that concerns the finding of minima and maxima of functions, subject to some given constraints. Optimization means finding an alternative with the most cost effective or highest achievable performance under the given constraints, by maximizing desired factors and minimizing undesired ones. The process of optimization is the process of obtaining best if it is possible to measure change and what is good or bad.

A. Different optimization Techniques

1. Hill climbing

Hill climbing is a mathematical optimization technique which belongs to the family of local search. It is an iterative algorithm that starts with an arbitrary solution to a problem, then attempts to find a better solution by incrementally changing a single element of the solution. If the change produces a better solution, an incremental change is made to the new solution, repeating until no further improvements can be found. Hill climbing is good for finding a local optimum (a solution that cannot be improved by considering a

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

neighboring configuration) but it is not guaranteed to find the best possible solution (the global optimum) out of all possible solutions (the search space).

2. Genetic Algorithm Approach [2]

Genetic Algorithms are the heuristic search and optimization techniques that imitate the process of natural evolution. Genetic algorithms generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. In a genetic algorithm, a population of candidate solutions (called individuals, creatures, or phenotypes) to an optimization problem is evolved toward better solutions. Each candidate solution has a set of properties (its chromosomes or genotype) which can be mutated and altered.

Genetic algorithm (GA) is used to iteratively modify pixel graylevels such that the difference between the statistical properties of the host image and its stego version does not exceed a certain tolerance. The process continues until a steganalytic scheme in the loop fails.

It transforms an optimization or search problem as the process of chromosome evolution. When the best individual is selected after several generations, the optimum or sub-optimum solution is found. The evolution usually starts from a population of randomly generated individuals and is an iterative process, the population in each iteration is called a generation. In each generation, the fitness of every individual in the population is evaluated; the fitness is usually the value of the objective function in the optimization problem being solved. The more fit individuals are stochastically selected from the current population, and each individual's genome is modified (recombined and possibly randomly mutated) to form a new generation. The new generation of candidate solutions is then used in the next iteration of the algorithm. Commonly, the algorithm terminates when either a maximum number of generations has been produced, or a satisfactory fitness level has been reached for the population

Problem in genetic algorithm is that it cannot guarantee a zero bit-error rate (BER) after data extraction. This scheme operates on individual 8 x 8 pixel blocks, not a full frame, implying a possible failure to resist steganalysis that considers the statistical features of more than one block. The methods construct a stego image by replacing each block of a host image with another block that has similar statistical properties.

Since altering pixel values or finding similar blocks, under the constraint of remaining statistically undetectable, is somewhat difficult, it is expected that time complexity of these methods will be large.

3. Simulated annealing (SA)[1]

Simulated Annealing (SA) is motivated by an analogy to annealing in solids. Using mappings any combinatorial optimisation problem can be converted into an annealing algorithm and is used to solve a wide range of combinatorial optimization problems. The parameters of the optimization problem will correspond to the atoms of the fluid, and an optimal solution to the problem will correspond to a low energy state of the fluid. A procedure for bringing the fluid to a low energy state will then serve as a procedure for finding an optimal solution for the optimization problem.

Starting at a given configuration, a sequence of iterations is generated, each iteration consisting of a possible transition from the current configuration to a configuration selected from the neighborhood of the current configuration. If this neighboring configuration has a lower cost, the current configuration is replaced by this neighbor; otherwise another neighbor is selected and compared for its cost value. The algorithm terminates when a configuration is obtained whose cost is no worse than any of its neighbor. Problems in simulated annealing are that it is a slow and time consuming algorithm. Only one neighbour solution is obtained by randomly altering the current solution.

III. SYSTEM ARCHITECTURE

Architecture

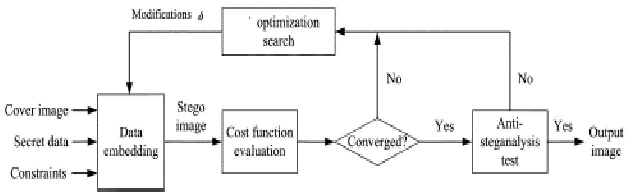

Fig.1 Proposed closed-loop architecture

Fig. 1 shows the architecture of our proposed framework for enhancing steganography systems. A completely optimal solution that minimizes all of the objective functions simultaneously does not always exist when the objectives conflict with each other.

Number of indices for performance evaluation and guidance of pixel/coefficient modifications are considered in the optimized cost function.

1) f1: Mean square error (MSE),

2) f2: HVS deviation,

3) f3: Anti-steganalysis (in terms of the differences in statistical features).

To integrate the three indices into the evaluation loop, we define a cost function E as follows:

$$E = w_1 \times f_1 + w_2 \times f_2 + w_3 \times f_3$$

where , w_1, w_2 and w_3 are predefined weights.

A search algorithm is developed to modify pixels/coefficients so that some targeted performances are optimized subject to certain constraints (e.g., capacity, robustness, or anti-steganalysis).

In the proposed architecture, we also use two performance indices MSE and HVS deviation, to measure imperceptibility. Though embedding a message of smaller size (i.e., lower embedding capacity) can make stego images nearly indistinguishable from their host images, it is less meaningful (we have to optimally increase the embedding rate without loss of statistical undetectablity). Steganalysis is often based on the statistical features of the image. That means that most steganalytic schemes determine whether an image contains confidential messages by analyzing the image's statistical properties. Then a steganographic scheme that can resist steganalysis has to consider variations in the statistical features of images.

Anti-steganalysis and optimization of the cost function in is to be achieved by modulating selected DCTcoefficients individually (i.e., the nonparametric category), in combination with an efficient search strategy.

Proposed optimization algorithm

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

The proposed algorithm is developed to overcome the drawbacks of above algorithms, by exploiting some special properties of the cost function to be optimized.
Starting at a given configuration, a sequence of iterations is generated, each iteration consisting of a possible transition from the current configuration to a configuration selected from the neighborhood of the current configuration. If this neighboring configuration has a lower cost, the current configuration is replaced by this neighbor, otherwise another neighbor is selected and compared for its cost value. The algorithm terminates when a configuration is obtained whose cost is no worse than any of its neighbor. Improving moves are always accepted while only a fraction of non-improving moves are performed with the aim to escape local optimal solutions.
The probability of accepting a worse state is given by the equation

$$P = \exp(-c/t) > r$$

Where c = the change in the evaluation function
t = the current control parameter
r = a random number between 0 and 1

Since SA is a random walk (of some type) on the solution space, the walk should go through each possible state at least once and hence the run time is very large. The idea is to partition the image into different zones and anneal these different zones at individually simultaneously. zone in the case of an optimization problem means a subset of the parameter set. If the control parameters of the zones are set right, the convergence time will be dominated by a single zone. Since the convergence time of SA is an increasing function of the number of states it can assume, proposed algorithm will indeed result in faster convergence.
Its major advantage over other methods is an ability to avoid becoming trapped in local minima. The algorithm provides mechanism to escape from local optima by allowing moves to lower quality solutions with a pre defined probability. Hill climbing suffers from problems in getting stuck at local minima (or maxima). This algorithm solves this problem by allowing worse moves (lesser quality) to be taken some of the time. That is, it allows some uphill steps so that it can escape from local minima.
Using different neighborhood selection strategies in a systematic way can significantly improve their efficiency and effectiveness. For selecting neighboring solutions, suppose we are going to find k neighboring structures. We have to decide which of the K structures to use at each step. In fact, in each step we have to solve a decision problem with K different alternatives. After choosing the neighborhood structure in the current control parameter, in each iteration, we are encountered with a two-alternative decision problem, either to continue or to stop. When we decide to stop, we may either switch to another neighborhood structure, if there is a profitable one, or decrease the control parameter and repeat the process. compute the cost of using each neighboring structure(Ck).find optimal value of each neighboring solution, and decide whether to go for this neighboring solution or not.
Stopping rule:
Stopping rule is defined for determining the optimal time for changing the value of control parameter. If the best value found for the objective function so far does not increases by at least 25% after 5 number of parameter decreases, the algorithm stops.

IV. THE BASE STEGANOGRAPHY METHOD USED

The used image steganography method requires no knowledge on data hiding positions when the data are extracted. This method offers the user the flexibility of choosing positions to hide data. It, thus, modifies the coefficients to embed data on the basis of the individual image and/or image compression technology.
Conventional methods require memorizing positions for data hiding to extract the hidden data. Moreover, since they fix the positions within the whole image, it is difficult to choose data hiding positions on an individual image basis and/or the basis of the coding scheme being applied to the images. On the other hand, methods that embed only one bit per one position are not able to embed multiple bits in any one position. Methods that are able to be extended to embed multiple bits in one position may degrade the image-quality considerably, because they have to embed L-level data using $\lfloor \log^2 L \rfloor$ bit data, e.g., four bits are hidden for data that has nine levels.
Since it hides integer data in transformed coefficients after the quantization process of image compression, the hidden data are no longer distorted by the rest of the compression process. The proposed method hides log2 L bits rather than $\lfloor \log^2 L \rfloor$ bits for L-level data into one particular area. It, thus, reduces image-degradation more than with conventional methods.

A. An embedment and extraction algorithms

Here an embedment and extraction algorithms are described using a JPEG coded image as an example.

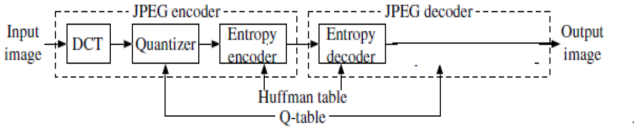

Fig. 3 Quantization based image steganography scheme

It is assumed that data sequence w is hidden in a JPEG coded image that consists of M of 8×8 pixels-sized blocks. Sequence w consists of M of elements and is represented as

$$W = \{W_m \mid m = 1, \ldots, M\}$$

Data element W_m is hidden in the m[th] block and each wm has L levels from zero to L−1. This method hides log2 L bits rather than $\lfloor \log^2 L \rfloor$ bits for W_m.

- Data Hiding in a Compressed Domain

The hiding algorithm in the proposed method is described as hiding W_m in an m[th] block after quantization of the transformed coefficients. In practice, this process is repeated M times to hide whole w.
This algorithm firstly modulates data wm to d, and this paragraph describes how it is modulated. Quantized coefficients in the m-th block are summed up by

$$S = \sum_{k=0}^{63} C_k \qquad \text{..........(1)}$$

where ck represents the quantized coefficients. Positive remainder r, then, is obtained by dividing S by L as

$$r = s \bmod L, r > 0 \qquad \text{...........(2)}$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

The difference d1 between the obtained r and data to be hidden
wm is calculated directly by

$$d_1 = |W_m - r|, \quad \text{...........(3)}$$

and another difference d2 is also given as

$$d_2 = L - d_1, \quad \text{...........(4)}$$

because of the modulus rule. Finally, the modulated value d that is actually hidden into the m-th block is given by

$$d = \min(d_1, d_2) \quad \text{............(5)}$$

Actual data hiding is achieved by modifying one or several coefficients in the m-th block so that the summation of coefficients that is represented by Sˆ satisfies

$$\hat{S} = \begin{cases} s - d, r > W_m \,\&\, d_1 < d_2 \\ s + d, r > W_m \,\&\, d_1 \le d_2 \\ s + d, r < W_m \,\&\, d_1 < d_2 \\ s - d, r < W_m \,\&\, d_1 \ge d_2 \\ s, r = W_m \end{cases} \quad \text{..........(6)}$$

It is noted again that this algorithm allows us to modify either one or several coefficients to hide data. That is, the proposed steganography allows the user the flexibility of choosing the coefficient for data hiding. The k-th stego coefficient is represented by ˆ ck hereafter, whether C_k = ˆ ck or not.

- Data Extraction in a Compressed Domain

The extraction of wm from the m-th block is described in this section, and it is repeated M times to extract the whole of w in practice. An entropy decoding process is applied to a stego JPEG codestream and, then, hidden data are extracted without using the inverse quantization process. The stego coefficients cˆks are summed up to obtain Sˆ by

$$\hat{S} = \sum_{k=0}^{63} \hat{C}_k \quad \text{...........(7)}$$

The remainder rˆ, then, is obtained by dividing Sˆ by L as

$$\hat{r} = \hat{S} \bmod L, \hat{r} > 0 \quad \text{............(8)}$$

This remainder ˆr is identical to W_m , so W_m can be extracted without decoding the whole of a stego JPEG codestream.

It is noteworthy that this extraction algorithm requires only one parameter L. No knowledge of positions for data hiding is required in this proposed steganography, whereas conventional methods require such information. Moreover, lossless processing is applied after quantization of coefficients in JPEG. Hidden data, thus, is extracted error free. Since modifying several cks to hide data does not affect the structure of the JPEG codestream, a stego JPEG codestream is decodable with a standard JPEG decoder.

It is our intent to advance this steganographic scheme by properly distributing d among non-zero coefficients so that the cost function E is optimized and the steganalytic system is broken after embedding. Expectedly, the computational complexity of finding solutions by using the exhaustive search is extremely high. Here, a more efficient manner based on the optimization algorithm is adopted instead.

V. CONCLUSION

Compared with the original embedding algorithm, a better image quality is achieved and simultaneously the anti-steganalysis capability is enhanced significantly. The proposed architecture overcomes drawbacks of genetic algorithm based framework and simulated annealing based framework in effective manner. In principle, this closed-loop architecture can be applied to most types of steganographic schemes (in either spatial or transform domain) and steganalytic systems. In future work, more constraints or performance index can be added into the cost function for optimization. Without loss of generality, this architecture is useful in enhancing steganographic schemes in terms of multi-functionalities such as embedding capacity, picture quality, HVS, anti steganalysis, BER, or more. Less computational effort at each value of control parameter because the best number of iteration in known.

REFERENCES

[1] Y.-T. Wu and F. Y. Shih, "Genetic algorithm based methodology for breaking the steganalytic systems," IEEE Trans. Syst., Man, Cybern. B, vol. 36, no. 1, pp. 25–31, Feb. 2006.
[2] A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie.
[3] Quantization-Based Image Steganography without Data Hiding Position Memorization Yusuke SEKI∗ , Hiroyuki KOBAYASHI†, Masaaki FUJIYOSHI∗ and Hitoshi KIYA Department of Electrical Engineering, Tokyo Metropolitan University, Hachioji-shi, Tokyo 192–0397, Japan
[4] Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix Xiaochuan Chen1, Yunhong Wang2, Tieniu Tan1, Lei Guo11 National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences
[5] The JPEG Still Picture Compression Standard Gregory K. Wallace Multimedia Engineering Digital Equipment Corporation Maynard, Massachusetts Submitted in December 1991 for publication in IEEE Transactions on Consumer Electronics
[6] Hudson, G.P. The development of photographic videotex in the UK. In Proceedings of the IEEE Global Telecommunications Conference, IEEE Communication Society, 1983, pp. 319-322
[7] Hudson, G.P., Yasuda, H., and Sebestyén, I. The international standardization of a still picture compression technique. In Proceedings of the IEEE Global Telecommunications Conference, IEEE Communications Society, Nov. 1988, pp. 1016-1021
[8] Image and Video Compression for Multimedia Engineering: Fundamentals By Yun Q. Shi, Huifang Sun
[9] A Secure Steganography Method based on Genetic Algorithm Shen Wang, Bian Yang and Xiamu Niu School of Computer Science and Technology Harbin Institute of Technology 150080, Harbin, China
[10] Léger, A., Omachi, T., and Wallace, G. The JPEG still picture compression algorithm. In Optical Engineering, vol. 30, no. 7
[11] Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix Xiaochuan Chen1, Yunhong Wang2, Tieniu Tan1, Lei Guo11 National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences
[12] Huffman, D.A. A method for the construction of minimum redundancy codes. In Proceedings IRE, vol. 40, 1962, pp. 1098-1101.
[13] Léger, A., Omachi, T., and Wallace, G. The JPEG still picture compression algorithm. In Optical Engineering, vol. 30, no. 7 (July 1991), pp. 947-954.
[14] Structural, Syntactic, and Statistical Pattern Recognition: Joint IAPR edited by Niels da Vitoria Lobo, Takis Kasparis, Michael Georgiopoulos, Fabio Roli, James Kwok
[15] A survey of very large-scale neighborhood search Techniques Ravindra K. Ahuja Ozlem Ergun, James B. Orlin, Abraham P. Punnen
[16] Steganographic Techniques of Data Hiding using Digital Images Babloo Saha and Shuchi Sharma Institute for Systems Studies and Analyses, Delhi – 110 054, India
[17] Mean Squared Error: Love It or Leave It? By Zhou Wang and Alan C. Bovik

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.