Volume 9, Special Issue No. 1, February 2018

ISBN: 978-93-5300-455-2

International Journal of Advanced Research in Computer Science
(ISSN: 0976-5697)
REVIEW ARTICLE

ICRACC 2018
(23rd–24th February 2018)

Available Online at www.ijarcs.info

Role of Soft Computing Techniques in Improving the Strength of Steganographic Systems

G.Umamaheswari
Research Scholar, Manonmaniam Sundaranar University
Asst. Professor, PG Dept. of Computer Science
SSS Jain College For Women, T-Nagar
Chennai, TamilNadu, India.
gumaganesh2011@gmail.com

Dr. C.P.Sumathi
Professor & Head, Dept. of Computer Science
SDNB Vaishnav College For Women, Chromepet,
Chennai, TamilNadu, India

ABSTRACT

In recent times steganographic systems that deal with concealing of secret data inside images have gained much attention. Robustness, capacity of embedding and imperceptibility are the major issues concerning embedding of secret data inside a cover. This paper analyses the recent advancements in this field by combining the soft computing techniques with steganographic algorithms for increasing the robustness, capacity and imperceptibility of the images used for embedding.

Keywords: Steganography, Least Significatn Bits (LSB), Soft Computing, Fuzzy Logic (FL), Neural Networks(NN), Genetic algorithm(GA), Support Vector Machines(SVM), Spatial domain, Transform Domain.

I. INTRODUCTION TO STEGANOGRAPHY

Steganography deals with secret communication of sensitive information. It deals with concealing secret data into other media like images, audio, video etc. When compared to cryptography, steganography provides an additional layer of security. Cryptography uses data scrambling with the intention of protecting it, so that it is not understood other than the intended recipient.

Steganography hides the very presence of data; in fact cryptography can be combined with steganography to increase the efficiency of steganographic systems. Although many algorithms exist for different ways of embedding secret data, the challenge in developing these kinds of systems is in protecting the secret embedded data that can withstand attacks. The combination of Soft computing techniques with steganographic algorithms helps to build a strong system that can withstand attacks. The Basic steganographic model is given in Figure 1 where the function f(x,m,k) represents the steganographic process.

The rapid growth in transmitting data through public channels has raised the bar for securing information. Steganography based information security is one such field that proposes techniques for hiding information that is being transmitted. An audio/ video/ image file can be used as a medium that is used to hide information. With regard to embedding data in images two popular techniques exist.

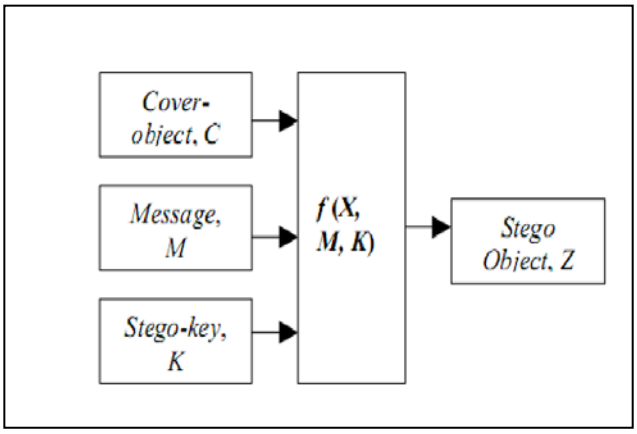

Figure 1: Basic Steganographic model [1].

1. Spatial domain secret embedding
2. Transform domain secret embedding

Spatial domain deals with embedding data straightforwardly in the spatial coordinates (i.e) the pixel values. The different techniques under the spatial domain include

- Least Significant Bit (LSB) substitution
- Pixel Value Differencing (PVD)
- Region of Interest methods [2].

The main features of spatial domain techniques are their

- Simplicity
- Less time complexity
- Ease of implementation

The main drawback of spatial domain techniques is that they cannot withstand attacks, a feature referred to as robustness.

The cover file is transformed to a different domain using any one of the transform domain techniques available and then data is hidden into the coefficients of the transformed domain.

The main highlight of these techniques is the robustness against attacks [3].

The Commonly used transform domain techniques are

- Discrete Cosine Transform (DCT)
- Discrete Fourier Transform (DFT)
- Discrete Wavelet Transform (DWT)

II. INTRODUCTION TO SOFT COMPUTING

Soft computing is a branch of computer science (sometimes referred to as computational intelligence) that is used to find approximate solutions to computationally hard tasks such as the solution of NP-complete problems, where it is found that there is no exact solution available in polynomial time. Soft computing is different from conventional (hard) computing in a sense that, it is tolerant to uncertainty, approximation, partial truth and imprecision. The main role model for Soft Computing is our Human mind.

The constituents of Soft Computing are Probabilistic Reasoning, Machine Learning, Fuzzy Logic, Evolutionary Computing etc.

Soft Computing techniques include Fuzzy logic, Genetic algorithms, Rough Sets, Neural networks and Support vector machines. These techniques intend at achieving robust, optimal, low cost and adaptive solutions for problems related to data hiding.

In recent times the combination of soft computing techniques along with the traditional ways of embedding secret data has gained much attention. In this paper we analyze several methods that propose to hide data using fuzzy logic, neural networks, genetic algorithm and support vector machines.

A. *Fuzzy Logic (FL)*

Fuzzy logic theory was introduced in 1965 by Zadeh [4]. Problems that require human like reasoning and inference are usually tacked by fuzzy logic.. Figure 2 represents the basic fuzzy logic model.

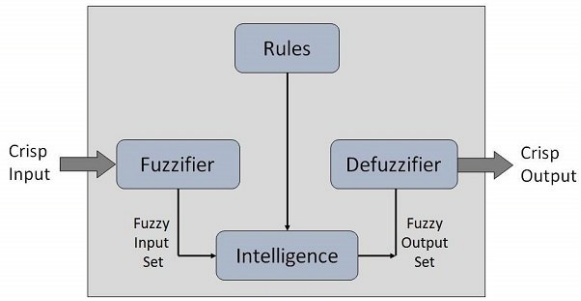

Figure 2: Basic Fuzzy Logic Model.

The process of fuzzification involves mapping of input values (mathematical) into fuzzy membership functions. To arrive at "crisp" output value they are mapped with fuzzy output membership functions by the process of de-fuzzification. The result can be used for decision and/or control purposes.

Process

1. All input values are fuzzified into fuzzy membership functions.
2. The fuzzy output functions are computed by application of all rules in the rule base.
3. The get "crisp" output values the process of De-fuzzification is done on fuzzy output functions [11].

Figure 3 shows the effect of information hiding fuzzy set.

The scheme of focus of attention is closely associated to information hiding. The collections of the elements that are hidden are viewed from the stand point of membership functions. Information hiding is achieved through normalization and is done by increasing or decreasing the level of α cut and is referred to as α information hiding. The hiding of elements about x is achieved [18].

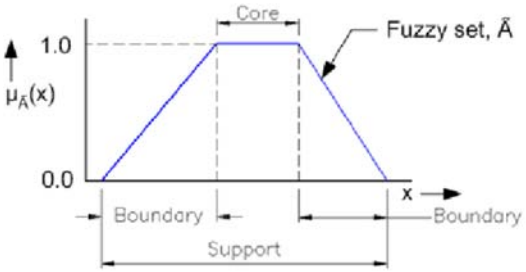

Figure 3: Effect of Information Hiding Fuzzy set.

A.saleema et.al [9] in their article suggests a hybrid fuzzy neural network model at the post processing phase that improves the quality of the stego image. The input features are subjected to fuzzy pre processing and the improved stego image is resilient to visual and statistical attacks and also the stego image is highly imperceptible

Sara sajasai et.al [10] has developed an intelligent novel adaptive steganography scheme that integrates Fuzzy Inference System (FIS) with the characteristics of Human Visual System (HVS). The scheme uses 36 rules that discover strong relationships between features and output classes.

Fatma Hassan Al-Rubbaiy in his article has proposed a system in which the cover image is divided into blocks of 10 x 10 and secret data in embedded only in the even sub images. Fuzzy Logic is used for dividing the blocks into odd and even sub images and also for encryption of secret message [12].

B. *Neural Network (NN)*

Neural Network is an optimization technique mainly used as a classifier. Neural networks are organised in layers and consists of neurons that are interconnected group of nodes. Neural networks can still continue in the event of the failure of an element, because of its parallel nature. Figure 4 shows the multi-layered perceptron model in which each node represented by a circle is a neuron and the arrows correspond to a link from the output of one neuron to the input of another neuron [6]. The working of the three layers in neural networks is as follows:

- Input Layer-> includes training set and trained target is passed as input to neural.
- Hidden Layer -> is concerned with the number of iterations at which the best result is achieved.
- Output Layer -> generates the final result.

Neural network accepts a signal as input to the neuron and is converted to a certain value using a function usually sigmoid function [7] given by equation 1 and outputs this value as output signal.

$$f(x) = \frac{1}{1+e^{-x}} \qquad (1)$$

Each synaptic link has a network weight. The network weight from unit i to unit j is represented by W_{ij}. O_i represents the output value for unit i. The Speed of the learning process normally has a value between 0 and 1 that is a constant and is referred to as Learning Rate. The main aim is to train the neural network to output a value of 1 or 0 as output signal.

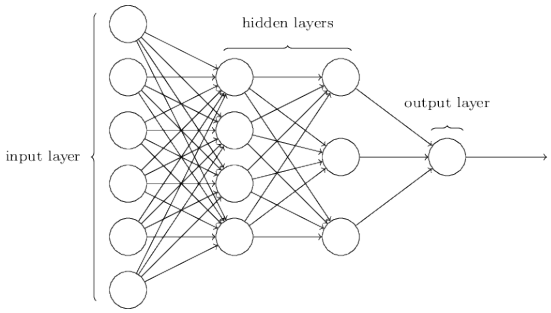

Figure 4: Multi-Layered perceptron model

In the article proposed by Anamika Sharma et.al. a new methodology in which wavelet transform is applied to both the cover image and the secret image is used. The process of fusion using neural network is used to get the stego image which is a merged image got from cover and secret image. The method is found to achieve robustness against image attacks like cropping, rotation and noising.

In Kensuke Naoe et. al's article [7] one network represents one binary digit for corresponding secret codes. The hidden layer consists of a number of neurons and the count of neurons is taken randomly as 10 neurons in this case. The proposed network uses the values that get converged from network weights and the extraction keys from coordinates of selected feature subblocks. The sender and the receiver shares the keys in order to extract proper hidden signals from the contents.

C. Genetic Algorithm (GA)

Genetic algorithms are modelled on evolutionary biology for search optimization. The natural theory of evolution which is based on the survival of the fittest approach is the basis of Genetic Algorithm. The next generation reproduces from only the fittest surviving individual.

In the field of steganography genetic algorithm is mainly used to find the best embedding position so that the image obtained after inserting secret message can withstand any type of attack.

A Component based architecture is proposed by Usha.B.A et. al. The main steps of genetic algorithm are

- [start] A random population of n chromosomes generated (suitable solution for the problem).
- [Fitness] For each chromosome in the population a fitness function f(x) is evaluated.
- [New population] the steps are repeated until a new population is found.
- [Selection] Two guardian chromosomes are selected as per their wellness using a fitness function.

  [Crossover] To frame another posterity (children) a hybrid likelihood is traversed. Posterity is a careful duplication of the parents when no cross over is performed.

  [Mutation] At every locus (position in chromosome) there is a possibility of a new posterity with mutation.

  [Accepting] Refers to the placing of new posterity in another general population.

  - [Replace] The newly created populace is utilized in the algorithm for the next run.
  - [Text] In the event of the end condition being satisfied stop and revisit the best solution in current population.
  - Goto the Fitness step. [5]

A secure steganographic framework is proposed by Shamimunnisabi et.al.[8]. Embedding of the secret text message is done in the coefficients of the Integer Wavelet Transform. The system is said to become robust by the usage of Genetic Algorithm. The method is found be tolerant to RS analysis. The message bits are embedded in 4 LSB's of the Integer Wavelet Transform coefficients using a mapping function. The process of Optimal pixel Adjustment is based on the fitness evaluation.

A secure and novel stegano-algorithm is suggested by dinesh kumar et.al. and is found to be extremely RS resistant. The combination of Genetic Algorithm with Integer Wavelet Transformis used in the proposed method. The coefficients of the wavelet transform are the locations for embedding the secret message. The process of optimal pixel adjustment using genetic algorithm and optimal pixel adjustment is done. A mapping function for all the blocks of the image is found using Genetic algorithm [13].

D. Support Vector Machine (SVM)

Support Vector machines are based on supervised learning models. Usually associated with learning algorithms SVM's

analyses data that is mainly used for regression and classification analysis.

In the article proposed by Akram AbdelQader et.al. [15] the cover and the secret images are divided into blocks of 8 x 8. Each block is subjected to Discrete Cosine Transform. Based on the linear SVM learning process for the DCT feature is done and bits of the cover image is replaced with the bits of secret data.

SVM is mainly used for characterization / relapse issues using a regulated machine learning calculation. A procedure referred to as bit trap is used to change information. The ideal limit of these changes is calculated. SVM has the high generalization ability to separate data into two classes, thus it is naturally suitable to classify the cover-image[16].

In the method proposed by Hanizan Shaker Hussain 1 et.al. [17] the cover image features are extracted. A SVM training dataset is constructed. The best parameter, the penalty parameter and the gamma value is found using cross validation technique and is used to train and generate the SVM function f(x).

TABLE I . ANALYSIS OF DIFFERENT SOFT COMPUTING APPROACHES.

S.No	Soft Computing Paradigm used	Cover Image & Size	PSNR (dB)	MSE / SSIM	Hiding Capacity / Speed/ payload ratio
1.	Genetic Algorithm [8]	Lena 512x512	46.83 (K=3)*	NA	1048576 (bits)
2.	Genetic Algorithm [13]	Lena 512x512	39.94	NA	50%
3.	Hybrid Fuzzy Neural Network [9]	Lena	39.47	0.8 (SSIM)	1.43 sec
4.	Fuzzy Logic [10]	Lena 512x 512	52.03	NA	0.5 bpp
5.	Genetic Algorithm [14]	Lena 512x 512	34.68	22.11	1048576 (bits) 50%
6.	Support Vector Machine [15]	Elephant 256 x 256	44.305	NA	64 x 64 image
7.	Support Vector Machine [17]	Lena NA	49.86	NA	NA

*K represents the no of LSB's used.

ACKNOWLEDGMENT

My heartfelt thanks to Dr.C.P.Sumathi who gave expert guidance and support in completing this article.

REFERENCES

[1] https://image.slidesharecdn.com/manika-150520175836-lva1-app6892/95/steganography-13-638.jpg?cb=1432144833

[2] Ratnakirti Roy, Anirban Sarkar, Suramoy Changder, " Chaos Based Edge Adaptive Image Steganography", International Conference on Computational Intelligence Modelling Techniques & Applications (CIMTA)2013, Proceedia Technology(2013), 138-146. (www.Sciencedirect.com)

[3] Taozhang, Shuai Ren, " Application of CL multi-wavelet transform and DCT in Information Hiding Algorithm", International Journal of Computer Networks and Information Security, 2011, 1, 11-17.

[4] Zadeh, L.A(2005), "The Concept of a Generalized Constraint – A Bridge from Natural Languages to Mathematics NAFIPS 2005 – Annual Meeting of the North American Fuzzy Information Processing Society.

[5] Usha.B.A, et.al " High Capacity Data Embedding Method in Image Steganography using Genetic Algorithm", International Journal of Computer Applications(0975 – 8887), Volume 121-No.14, July 2015, 30-33.

[6] Anamika sharma, Ajay Kushwaha, " Image Steganography Scheme Using Neural Network in Wavelet Transform Domain", International Journal of Scinetific Engineering and Research , ISSN (online) 2347-3878, Volume 3 Issue 10, October 2015, 153-158.

[7] Kensuke Naoe, Yoshiyasu Takefuji, "Damageless Information Hiding using Neural Network on YCbCr Domain", International Journal of Computer Science and Network Security, Vo8, No.9, September 2008.

[8] Shamimunnisabi, Cauvery N.K, "Empirical Computation of RS-Analysis for Building Robust Steganography Using Integer Wavelet Transform and Genetic Algorithm", International Journal of Engineering Trends and Technology, Volume 3 Issue 3 , 2012, ISSN:2231-5381, 448-456.

[9] Saleema.A, Dr.T.Amarunnishad, " A New Steganograhy Algorithm Using Hybrid Fuzzy Neural Network", International Conference on Emerging Trends in Engineering, Science and Technology- 2015, 2212-0173, Procedia Technology 24(2016), 1566 -1574.

[10] Sara Sajasi, Amir Masoud Eftekhari Moghadam, " A high Quality Image Steganography Scheme Based on Fuzzy Inference System", 13th Iranian Conference on Fuzzy Systems , 978-1-4799-1228-5/13 © 2013 IEEE.

[11] https://en.wikipedia.org/wiki/Fuzzy_logic

[12] Fatma Hassan Al-Rubbaiy, " Concealment of Information and encryption by using Fuzzy Technique", Journal of the college of Basic Education, Volume 16, Issue 69, 25-34.

[13] Dinesh Kumar, Narendra Yadav, "High Embedding Capacity and Secured Steganographic Model by Using RS based Genetic Algorithm and IWT", Research & Reviews : Journal of Engineering and Technology ISSN :2319-9873.

[14] Medisetty Nagendra Kumar, S.Srividya, "Genetic Algorithm Based Color Image Steganography using Integer Wavelet Transform and Optimal Pixel Adjustment Process", International Journal of Innovative Technology Exploring Engineering (IJITEE) ISSN :2278-3075, Volume 3, Issue 5, October 2013, 60-65.

[15] Akram AbdelQader, Fadel AlTamimi, " A Novel Image Steganography Approach Using Multi Layers DCT features based on Support Vector Machine Classifier", The International Journal of Multimedia & its Applications (IJMA) Vol.9, No.1, February 2017, 1-10.

[16] Rohit Tanwar, Sona Malhotra, "Scope of Support Vector Machine in Steganography", IOP Conf.Series: Materials and Engineering 225 (2017) 012077 doi:10.1088/1757-899X/225/1/012077.

[17] Hanizan Shaker Hussain, Roshidi Din, Aida Musthapa, Fawwaz Zamir Mansor, " LSB Algorithm Based on Support Vector Machine in Digital Image Steganography", Journal of Telecommunication, Electronic and Computer Engineering, E-ISSN :2289-8131 Vol 9, N0.2-12, 13-18.

[18] Witold Petrycz, Andrezej skowron, Vladik Kreinovich, "Handbook of Granular Computing", page 112.