Security Assessment for Student's Registration Card by using Genetic Algorithm

Ei Ei Phyu, Khin Myat Myat Moe
Computer University, Magway
eieiphyu2008@gmail.com

Abstract

The demand of security is getting higher in these days due to easy reproduction of digitally created data. Digitally hide the secret information in some media content like digitized identification card, student's registration card, e-passport, etc is the emerging technique for security protection of these media. Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Military communications systems make increasing use of trace security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever trace security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use. In this system, a GA (Genetic Algorithm) based secret information hiding technique is presented for checking the security of student's registration cards. This can check that the card is real or not for security assessment of examination. The secret code like (001, 002,) or secret image is hide into the contents (images' pixels) of digitized student's registration card and we employed GA to choose the best positions for hiding process.

1. Introduction

Recent internet development technology has shown an increase in the security of media contents and a large drop in the usage of unauthorized person for these contents. For the digital media protection from unauthorized usages and copyright protection of original usages, the information hiding techniques such as watermarking, and cryptography have been developed. The purpose of information hiding is to protect the security of identification cards and other security purposes. This paper brings secret information hiding process for getting the optimal/nearly optimal embedding position of information technique and for protecting the digital media contents security.

The security assessment of digital contents such as video, audio, images and other documents, secure information hiding techniques have been adopted. There are two ways of performing information hiding method, one in spatial domain that can simply insert some character into a host digital media by changing the gray level of some pixels in the host identification card that change to digitized image, but the inserted information may be easily detected using computer analysis. In the frequency domain, we can insert some character into coefficients of a transform domain and that is difficult to detect. In this paper , information hiding process for security assessment of student identification cards is presented that optimize the fidelity performance of protected cards and easily extract the embedded character from protected cards.

- Secret information hiding technique is applied for security assessment of digital media such as video, audio, images and other documents.
- Hiding the secret information in digitized ID card or registration card could increase the confidentiality of information as well as the security that would prevent unauthorized person to detect it.

In this paper, a GA-based secret information hiding process is presented. This method optimizes the visual performance of protected student's registration cards for security assessments. The background theories of the system are presented at Section2. This paper presents an overview of the system in section3. In Section 4, some test identification is presented. At last, the conclusion is presented in section 5.

2. Background theories of the System

Multimedia contents such as pictures, video files and audio files are prone to being accidentally or maliciously modified, altered or destroyed. To deal with the issue of data integrity, authentication techniques are required to verify accuracy, correctness and validity of digital content. Digital Right Management (DRM) is an approach that

addresses the issue of piracy and ensures that the digital media is distributed to authorized parties only. The traditional forms of protecting information are steganography and cryptography, which are both used in the implementations of DRM. Steganography is a relatively insecure way of hiding information, but it is the precursor to a more robust method called watermarking, in which the message is hidden so that the source can be tracked or verified. Cryptography is commonly used for authenticating the integrity of digital data and it is achieved using digital signatures [5]. The digital information hiding technique is currently most practice and can be used to improve the secure quality of unauthorized assessments, the control quality of copyright protection as well as providing the secure transmission of media contents over internet with efficient delivery.

2.1 Information Hiding Scheme Domains

In the spatial domain techniques, they manipulate digitized contents such as pixels especially on least significant bits that have less perceptual effect on the digitized contents. This is simple and easy to implement but it is weak for various attacks and noise.

In the frequency domain techniques, information embedding is made on the frequency coefficients of images like Discrete Fourier transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).In frequency domain based information hiding schemes, various attacks and noise can be robust.

2.2 Genetic Algorithm

Algorithms (GAs) [6] are adaptive heuristic search algorithm premised on the evolutionary ideas of natural selection and genetic. The basic concept of GAs is designed to simulate processes in natural system necessary for evolution, specifically those that follow the principles first laid down by Charles Darwin of survival of the fittest. As such they represent an intelligent exploitation of a random search within a defined search space to solve a problem.

First pioneered by John Holland in the 60s, Genetic Algorithms has been widely studied, experimented and applied in many fields in engineering worlds. Not only does GAs provide alternative methods to solving problem, it consistently outperforms other traditional methods in most of the problems link. Many of the real world problems involved finding optimal parameters, which might prove difficult for traditional methods but ideal for GAs. However, because of its outstanding performance in optimization, GAs has been wrongly regarded as function optimizers. In fact, there are many ways to view genetic algorithms. Perhaps most users come to GAs looking for a problem solver. GAs as a number of different things as follows:

- GAs as problem solvers
- GAs as challenging technical puzzle
- GAs as basis for competent machine learning
- GAs as computational model of innovation and creativity
- GAs as computational model of other innovating systems
- GAs as guiding philosophy

2.3 GAs and Information Hiding Process

Genetic algorithms are important optimization techniques in evolutionary computation. The author and colleague have introduced the idea of GA-based information hiding process enhancement by searching best embedding positions in [1, 2]. These are the essential publications that connect GA optimization together with information hiding technique like digital watermarking. Furthermore, a lightweight-searching algorithm for small-range problem, which meets the inherent problem formulation of this algorithm, is proposed in [3] to alleviate the long computation time. Another GA-based information hiding algorithm was also proposed in [4].

2.4 GA based Secret Code Hiding Algorithm

Input: - Let I be the original digitized registration card

- S $\in$ {0, 1} be the digital secret code of length (N)

Processing

1. Divide the I into N x N blocks
2. Generate two uncorrelated random sequences that has the number of elements equal to the number of elements in each block, one sequence is used to embed the Secret code's bit 0(sq1) and the other sequence is use to embed the secret code's bit 1(sq2)

3. Randomly choose the embeddable positions by genetic algorithm Embed binary sequences of secret code (1, 0...) into the blocks of original digitized registration card as follows:

If (secret code's bit = = 1)

I′ (p).block = I (p).block + sq1

If (secret code's bit = = 0)

I ′(p).block = I (p).block + sq2

where p = the optimal positions chosen by GA

I′ = secured registration card

Output: Secured Registration card

2.5 Secret Code Extraction Algorithm

Input: Let I′ be the Secured Registration Card

Processing:

1. Divide I′ into N x N blocks
2. Take the mean value of each block of I and I′ for extracting secret code
3. Compute the mean differences between mean I and mean I′
4. Make secret code extraction
5. After extracting the binary sequences of secret code, convert them into the original secret information as result

Output: Original secret information

3. Overview of GA Based Information Hiding Approach

In this section, GA-based information hiding system is presented to enhance the fidelity performance of original images. By using GA to find nearly optimal positions in each block of original registration cards. To enhance the hiding performance with GA-based optimization procedures, the objective function that guides the optimization process shall be decided first. Since the visualization quality can be easily measured by some statistic indexes representing the difference between original blocks and embedded blocks, such as Mean Square Errors (MSE), and Peak Signal to Noise Ratio (PSNR), and the imperceptibility are chosen as the objective functions. Chromosomes with higher objective values have higher probability to contribute more offspring in the next generation. The objective function decides the probability of chromosomes' survival or removal during the competition.

In our system, information embedding positions within each identification card's coefficient block are chosen as the parameter space to be optimized, and consequently the GA operators will be applied in order to find out the best combination of embedding positions. By repeatedly applying the GA operators to every original identification card, the near-optimum embedding position for the original is got.

3.1 Problem Modeling

By applying the GA to the information hiding scheme, the secure card quality is improved. The embedding position of the signal within the identification card is simulated as chromosomes. Then several genetic-algorithmic operations are applied to optimize the image quality after embedding. In experiments, Peak Signal to Noise Ration with Mean Square (MSE) used to measure the objective function values during optimization.

In this paper, choose the information embedding positions within an original identification card as our search space. Then apply the genetic algorithmic operators to find the best embedding position. By repeatedly applying the GA operations, we can get near-optimal embedding positions for the original identification card and the signal. In the proposed scheme, the input identification card is transformed into frequency domain and the approximation coefficients of the input identification card are modified according to the signal.

3.2 Chromosome encoding

Chromosomes are encoded using the real data coding scheme and each chromosome represents the block positions where secret code to be embedded. Here, the length of chromosome is equal to the length of secret code.

3.3 Genetic Operator

Fitness Function: The fitness function of proposed GA-based information hiding scheme is a measure of profit that determines the quality of protected identification card. Usually, the fitness function measures how good a set of embedding positions is. This function also aims to improve the fidelity, i.e. the visible quality, of the identification card after embedding process. In this system, choose the PSNR with MSE as a fitness function as in Equation 3.1 and Equation 3.2.

$$MSE = \frac{1}{MN}\sum_{x,y}(I_{x,y} - \tilde{I}_{x,y})^2 \qquad (3.1)$$

where $\tilde{I}$ is the protected image, I is the original image, and x, y are the positions of images and MxN are resolution of image.

$$PSNR = 20\log_{10}\left(\frac{1}{MSE}\right) \quad (3.2)$$

The basic idea is that the higher a parent chromosome's fitness function value is the higher probability it has to contribute one or more offspring in the next generation.

Crossover: In this system use single point crossover method that performs the crossover between pairs of individuals. After *N* legal parent chromosomes and *M* children chromosomes are generated, crossover operator is applied to on these children chromosomes. The chromosomes are randomly mated in a pair. In the presented method, the crossover rate 0.5 is defined.

Mutation: Mutation is the random change of bit values with small probability within a chromosome. Mutation introduces some randomness into the optimization, thus, new embedding positions of blocks are generated. In our experiment, use 0.05 as the mutation rate, i.e. a bit may change (take complement) at a probability of 0.05.

Reproduction: Reproduction is a process that the children chromosomes are generated according to the fitness function values of their parents. After performing the mutation process, we use the Stochastic universal sampling (SUS) that is a single-phase sampling algorithm with minimum spread and zero bias method, to select the individuals for breeding.

Stopping Criteria: The maximum number of generations that can give the best PSNR value as stopping criteria. Repeat all the operations mentioned above until the number of generations specified has been done, and choose the best chromosome.

3.4 GA Based Secret Code Hiding Algorithm

In this section, GA based secret code hiding algorithm is presented .The original digitized student's registration card (host card) is a gray scale card. The binary sequence of information/character as secret codes is used for embedding process in digitized student's registration card. The main embedding technique is presented in the Figure 3.1.

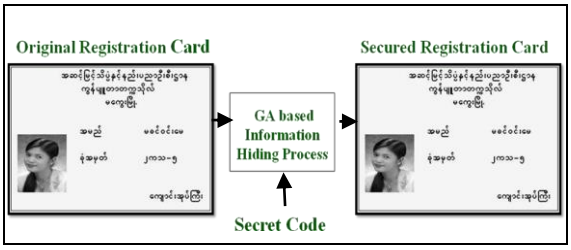

Figure 3.1 GA-based information hiding approach

3.5 Secret Code Extraction Algorithm

For extraction phase, the block positions should be passed to the detector. The secured registration card is passed into the detection system. In this GA based method, secret code extraction algorithm is performed without using the original source. Instead, the mean value of each blocks of secured registration card is used. Our extraction algorithm can be seen in Figure 3.2.

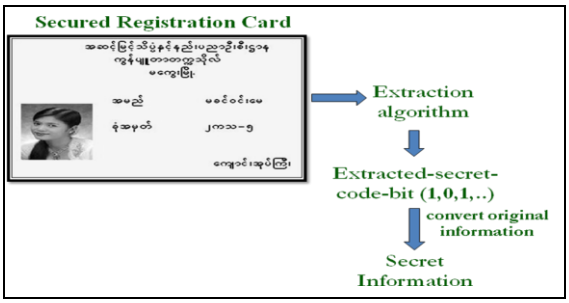

Figure 3.2 GA-based secret code Extraction approach

4. Experimental Analysis

In this portion, discuss about the two performance measures for proposed system as follows:

Imperceptibility: The perceived quality of the host image should not be distorted by the present of secret code and that measures can evaluate the imperceptibility of our proposed method by measuring the PSNR on the secured student registration cards.

Similarity: Calculate the correlation between the extracted secret code and original secret code according to the similarly equations as shown in equation 4.1

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N} w_i \times \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^{\,2}}\sqrt{\sum_{i=1}^{N} \hat{w}_i^{\,2}}} \quad (4.1)$$

where w_i is original secret code and $\hat{w}$ is extracted secret code. According to the results, the system can get good imperceptibility of the secured registration card after embedding process. So the similarity value of the secret code after extraction process is almost the same. Table 4.1 shows the test registration card with related PSNR value and similarity results.

Table (4.1) Analysis results on test registration card

Secured Id cards	Secret Code	PSNR value(dB)	Similarity Value
	A001	108.601	1
	B001	103.095	1
	aaaa	108.058	1

A001, B001 and aaaa are input secret code for embedding at original student's registration card.

4.1 Overview of Propose System

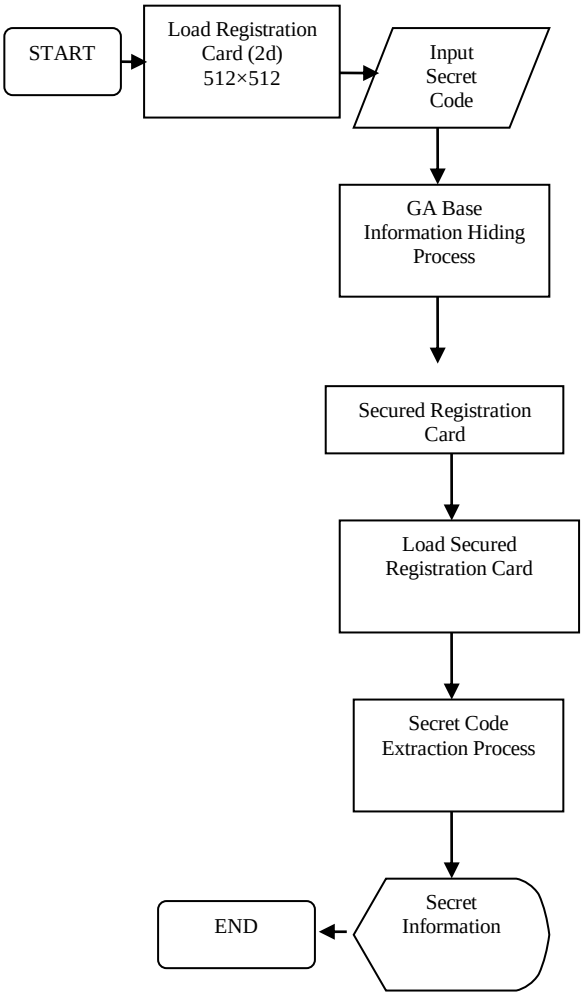

Figure 4.1 System flow diagram of the system

5. Conclusion

In this paper, the knowledge of information hiding scheme for secure student identification cards checking system is investigated. The process of secret code hiding approach, including preprocessing for input secret code, student identification cards' preprocessing, secret code embedding, and secret code extraction, is described in detail. In order to get the good positions for secret code embedding process, we apply the operators of GA until reaching the stopping criteria. To insert the secret code into the host cards, the proposed algorithm transformed the original card into gray image and secret code is inserted by GA. By using GA, the proposed method can obtain the good visualization quality of protected identification cards and we also get the nearly the same similarity value between original secret code and extracted secret code. Our approach adopts an idea in employing the GA algorithm to enhance the imperceptibility of student registration cards.

6. References

[1] Genetic Algorithm Simulation of the SHOP Scheduling Problem, by Jonathan M.Goldstein, published by An ICMS/Shell Oil Business Consultancy, September 1991.

[2] Determining Economic Equilibria using Genetic Algorithms, by Meliha Chughtai, published by Imperial College, September 1995.

[3] Evolutionary Divide and Conquer: a novel genetic approach to the TSP, by Christine L.Valenzuela, published by Imperial College, in 28 June 1995.

[4] C. H. Haung, Implementation and Improvement of Some Digital Watermarking Algorithms, MS Thesis, Dept. of CSIE, National Taiwan University, 1999.

[5] F.A.P. Petitcolas, R. Anderson, and M.G.Kuhn." Information Hiding: a survey,"*Proceeding of the IEEE,* 87(7): 1062-1077, 1999

[6] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, Addison Wesley Publishing Company, January 1989