ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Steganography on Multimedia Products by ACO

Khossro Fardad, Mosayeb Nouri, Mehdi Medadian
Department of Computer, Behbahan Branch, Islamic Azad University, Behbahan, Iran
Department of Electronic, Behbahan Branch, Islamic Azad University, Behbahan, Iran
Department of Computer, Behbahan Branch, Islamic Azad University, Behbahan, Iran

Abstract*— In this paper, we present an approach to resolve problems of steganography by ACO. By proposed approach, message bits are embedded into multiple, vague and higher LSB layers. At proposed method, Robustness of steganography would be increased against those intentional attacks which try to discover the hidden message and also some unintentional attacks like noise addition as well. The hidden message embeds in more vague areas, spreads across the entire multimedia product and provides better resistance against attacker's processes.

***Index Terms*—Steganography Approach, Capacity of Hiding, ACO**

I. INTRODUCTION

Information is becoming widely available via Internet. The advent of multimedia is allowing different applications to mix sound, images, and video and to interact with large amounts of information. The amount of information and data that investigating and analyzing in sciences have incremented. Therefore, with the greater demand in digital signal transmission and the big losses from illegal data access, data security has become a critical and imperative issue in Multimedia data transmission application. In order to protect valuable data from undesirable readers or against illegal reproduction and modifications, there have been various data encryption methods and the watermark embedding schemes on images is proposed in the literature. The data encryption approaches make the images invisible to undesirable readers, while the watermark embedded scheme hide watermarks on to the image to declare their ownership but the image is still visible.

We can classify existing data encryption techniques into three major types: position permutation, value transformation, and the combination form. The position permutation algorithms scramble the original data according to some predefined schemes. It is simple but usually has low data security. The value transformation algorithms transform the data value of the original signal with some kind of transformation. It has the potential of low computational complexity. Finally, the combination form performs both position permutation and value transformation. It has the potential of high data security.

In this paper, we focus on hiding data in complex images as they can offer high payload because of their sizes and they are ubiquitous on Internet. Image steganography schemes are divided into two groups: Spatial/image Domain and Frequency/Transform Domain. Spatial domain techniques embed messages in the intensity of the pixels directly, while in transform domain, images are first transformed and then the message is embedded in the image. The proposed approach combines both spatial domain and transform domain. The cover image uses Ant Colony Optimization algorithm and data is embedded in transform domain using discrete cosine transform (DCT) . The remainder of this paper is organized as follows: Section II describes problems of substitution technique of steganography; Section III introduces the proposed steganography approach. The obtained experimental results and comparison of the proposed method with existing DCT based steganography methods are discussed in section IV and conclusion is given in section V.

II. PROBLEMS OF SUBSTITUTION TECHNIQUE OF STEGANOGRAPHY

Each steganography approach has to satisfy three basic requirements: transparency, capacity of hidden data and robustness. Noticeably, the main problem of substitution steganography algorithm is considerably low robustness. There are two types of attacks to steganography and therefore there are two type of robustness [9]. One type of attacks tries to reveal the hidden message and another type tries to destroy the hidden message. Substitution techniques are vulnerable against both types of attacks. The adversary who tries to reveal the hidden message must understand which bits are modified. Since substitution techniques usually modify the bits of lower layers in the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

samples, it is easy to reveal the hidden message if the low transparency causes suspicious. At this research, we describe and propose solution for resolving the following problems of substitution techniques of steganography:

- Low robustness against data discovery
- Low robustness against distortions

A. First Problem (Low robustness against data discovery)

One type of robustness that is very critical for security is withstanding against the attacks which try to reveal or extract the hidden message. With proposed approach we reach a more robust substitution method that extracting the embedded message become inaccessible to adversary. Certain way to withstand against these attacks is making more difficult discovering which bits are modified. Thus, the algorithm may not change some sample due to their situations. This selecting will improve the security of the method and robustness of the technique, because if somebody tries to discover the embedded message, he has to apply a specific algorithm to read some bits of samples. But if modified samples are secret, nobody can discover the message. As we know in samples LSBs are more suspicious, thus embedding in the bits other than LSBs could be helpful to increase the robustness. Furthermore, discovering which samples are modified should be uncharted. To reach to the level of ambiguity, the algorithm will not use a predefined procedure to modify the samples but will decide, according to the environment, in this case the host file; as such it will modify indistinct samples of audio files, depending on their values and bits status. Thus, some of the samples which algorithm determines they are suitable for modifying will modify and other samples may not change. This ambiguity in selecting samples will thus increase security and robustness of the proposed algorithm [9].

B. Second Problem (Low robustness against distortions)

A significant improvement in robustness against unintentional attacks(such as signal processing manipulation) will be obtained if an embedded message is able to resist distortions with high average power. To achieve this robustness the message could embed in deeper layers. But, selecting the layer and bits for hosting is critical because the random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN). It is well known from psychoacoustics literature [5] that the human auditory system (HAS) is highly sensitive to the AWGN. This fact limits the number of bits that can be imperceptibly modified during message embedding [4]. Embedding the message bits in deeper layers absolutely causes bigger error and it will decrease the quality of transparency. Thus, the algorithm which embeds the message bits in deeper layers should modify other bits intelligently to decrease the amount of this error and reserve the transparency. Predictably, substitution techniques try to modify the bits of samples in accordance with a directive that is defined in algorithm. The target bits are definite, and the amount of resultant noise is not controlled. Of course, there are some better techniques that try to adjust the amount of resultant noise in substitution techniques. These improved algorithms alter other bits else than target bit in sample to decrease the amount of resultant noise. A key idea of the improved algorithm is message bit embedding that causes minimal embedding distortion of the host audio. It is clear that, if only one of 16 bits in a sample is fixed and equal to the message bit, the other bits can be flipped in order to minimize the embedding error. The extraction algorithm remains the same; it simply retrieves the message bit by reading the bit value from the predefined layer in the stego-file sample. In the areas where the original and message bit do not match, the standard coding method produces a constant error with 8-Quantization Steps (QS) amplitude [6]. The improved method introduces a smaller error during message embedding. If the 4th LSB layer is used, the absolute error value ranges from 1 to 4 QS, while the standard method in the same conditions causes a fixed absolute error of 8 QS. What would be improved is a level of intelligence in those substitution algorithms which try to adjust the sample bits after modifying the target bits. The basic idea of the proposed algorithm is embedding that cause minimal embedding distortion of the host audio. What is clear as much as intelligence the alteration algorithms have, the amount of resultant noise could be improved. Because the total noise will be less, when we are able to alter and adjust more samples. With doing this project successfully, we can achieve more transparency and robustness [9].

C. solutions for problems

The solution for first problem: Making more difficult discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples.

The solution for second problem: Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

To combine these two solutions, we try to satisfy “other bits alteration to decrease the amount of the error” of second solution, if we ignore the samples which are not adjustable, also “selecting not all samples” of first solution will be satisfied. Thus, evolutionary optimization algorithms will try to embed the message bits in the deeper layers

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Bit alteration it should be done by evolutionary optimization algorithms such as ACO.

III. PROPOSED APPROACH

The proposing approach embeds a secret message in a large multimedia file without degrading the quality and provides better resistance against steganalysis process. Regions of interest for embedding information are found using Ant Colony Optimization algorithm based on geographical features and DCT coefficients of these patches are utilized for hiding message. The proposed algorithm proves to be better than the DCT based LSB insertion method in [7] that message is embedded in whole image thus degrading the transitions between different geographical features hence failure to subjective test and the proposed algorithm also provides better capacity as compared to one bit per block DCT method given in [8]. This approach uses a sequential covering algorithm to discover a list of classification rules covering all or most of the pixels in the training set by adding terms to the rule list. These classification rules are applied to the image and patching is done considering the connectivity of the pixels. After this step pixel chunks are extracted and their position is stored in a *seed* which is encrypted and embedded in the header of the image. Application of ACO to the image before embedding data in DCT mid frequency coefficients reduces the blocking artifacts of DCT based steganography between adjacent blocks. Pixels belonging to different classes are highly decorrelated and the frequency characteristics in two adjacent blocks are different. Embedding data in patches formed by ACO avoids the transitions between classes which are prone to degradation due to hiding of data. In this step, message bits are embedded one by one in the successive non zero DCT coefficients of the mid frequency region of selected region. This step produces an intermediate Stego-image that conceals the message bits. It should be noted that middle frequency region of the DCT coefficients is used to conceal message bits to limit the degrading of the visual quality of the produced Stego-image after applying the next step. The quality of Stego-images is judged on the basis of subjective analysis and Peak-Signal-to-Noise-Ratio (PSNR) in decibels (dB).The subjective tests are carried out by looking at the original image and Stego-image for visual differences between the images. PSNR can be calculated using the following formula:

$$PSNR = 10\log_{10}\left(\frac{MAX_t^2}{MSE}\right)$$

MSE is calculated using the following equation:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j) - K(i,j)\|^2$$

Where is the Mean Squared Error of images and , where one of the images is considered a noisy approximation of the other. In other words , where is the bit depth of the original image . Typical values for the in image and video compression are between 30 and 50 dB. The following pseudo code shows the ACO using at proposed algorithm (figure 1).

```
Discovery List;                          {at the first step list is empty}
While (train_set>max_uncover_samples)
        t:= 1;                           {ant  indicator}
        j:=1;                            {convergence test  indicator}
         Initialize Pheromone;
   While ((t < ants) and (j < 20))
          For(i=1 to # of attributes)
          get Rule;
          End_for
    If (rule (i)==rule(i-1))             {convergence test section}
       j = j + 1;
    else
       j = 1;
    end if
      Pheromone Update;
        t=t+1;
   end loop
  select best rule and  add rule to list
```

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Train_Set = Train_Set - {set of training samples covered by rbest};
end loop

Apply Rules on the Image;

IV. RESULTS AND ANALYSIS

In this section we present the simulation results for the proposed methods. Ant Colony Optimization is applied on the image to extract the region of interest for embedding message. The performance of the proposed method is compared with approach presented at [7] and one bit per DCT block presented at [8]. The implementation of the above mentioned techniques and the PSNR tests were carried out using MATLAB 2008.

Table 1: Results for various approach

	PSNR(dB)	Capacity(bits)
Approach at [7]	32.06	254,678
Approach at [8]	56.96	36,864
Proposed approach	41.3	224,153

The stego-image generated after applying the approach proposed in this paper is subjectively better than the result of method proposed in literature [7].

V. CONCLUSION

A new approach is proposed to resolve two problems of substitution technique of audio steganography. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness. ACO is applied to the image before embedding data in DCT mid frequency coefficients so as to remove the blocking artifacts of DCT based steganography. The performance of this system has been illustrated by embedding text message within image to produce Stego-image. When the Stego-image is decoded, the text message is completely recoverable. In addition, the system's ability to cope with noise and compression of the Stego-image has been exhibited.

ACKNOWLEDGEMENT

This paper is part of a project supported by research vice president of Islamic Azad University, Behbahan Branch , Behbahan , Iran.

REFERENCES

[1] Martin Alvaro, Sapiro Guillermo and Seroussi Gadiel, "Is Image Steganography Natural?" IEEE Transactions On Image Processing, Vol.14, No. 12, December, 2005.

[2] Cvejic N. and Seppנnen T. "Increasing the capacity of LSB based audio steganography", Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338.

[3] Lee, Y. K. and Chen L. H. "High Capacity Image Steganographic Model". IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.

[4] Pal S.K., Saxena P. K. and Mutto S.K. "The Future of Audio Steganography". Pacific Rim Workshop on Digital Steganography, Japan, 2002.

[5] Westfeld A. and Pitzmann A. "Attacks on Steganographic Systems".Lecture Notes in Computer Science, vol. 1768, Springer-Verlag, Berlin,pp. 61-75, 2000.

[6] Fridrich, Jessica and others. "Steganalysis of LSB Encoding in Color Images." Proceedings of the IEEE International Conference on Multimedia. 1279–1282. New York: IEEE Press, 2000.

World Academy of Science, Engineering and Technology 54 2009.

[7] Rufeng Chu, Xinggang You, Xiangwei Kong, Xiaohui Ba, "A DCT-based Image Steganographic Method Resisting Statistical Attacks", Department of Electronic Engineering, Dalian University of Technology, Dalian, China.

[8] Atalla I. Hashad and Abd El Moneim A. Wahdan, "A robust steganography technique using discrete cosine transform Insertion", IEEE proceedings 2005.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

[9] M.Zamani, A.A.Manaf, R.B. Ahmad, A.M.Zeki and S. Abdullah, "A Genetic-Algorithm-Based Approach for Audio Steganography ", World Academy of Science, Engineering and Technology, 2009.

AUTHOR BIOGRAPHY

Khossro Fardad member of department Of Computer, Behbahan Branch, Islamic Azad University, Behbahan, Iran. His major is network and information security. Interested in the area of research in watermark and steganography using artificial intelligence.

Mosayeb Nouri member of department Of Electronic, Behbahan Branch, Islamic Azad University, Behbahan, Iran. His major is image processing and multimedia over computer network.

Mehdi Medadian member of department Of Computer, Behbahan Branch, Islamic Azad University, Behbahan, Iran. His major is Ad hoc routing and security.