International Journal of
Engineering in Computer Science

E-ISSN: 2663-3590
P-ISSN: 2663-3582
IJECS 2019; 1(2): 56-58
Received: 22-05-2019
Accepted: 23-06-2019

K Santha Sheela
M.E, AP, Department of CSE,
Velammal College of
Engineering and Technology
Madurai, Tamil Nadu, India.

Vennila D
Student, Department of CSE,
Velammal College of
Engineering and Technology
Madurai, Tamil Nadu, India.

CB Selva Lakshmi
AP, Department of CSE,
Velammal College of
Engineering and Technology,
Madurai, Tamil Nadu, India.

Mathi Poorani K
Student, Department of CSE,
Velammal College of
Engineering and Technology
Madurai, Tamil Nadu, India.

Correspondence
K Santha Sheela
M.E, AP, Department of CSE,
Velammal College of
Engineering and Technology
Madurai, Tamil Nadu, India.

A scrambled image hiding on image using discrete cosine transform

K Santha Sheela, Vennila D, Selva Lakshmi CB and Mathi Poorani K

DOI: https://doi.org/10.33545/26633582.2019.v1.i2a.21

Abstract
Image steganography is the study of embedding sensitive information in images without distorting their visual quality. In this paper, we have proposed an efficient image steganography algorithm to embed the secret image in the cover image. In this scheme, the secret image is encrypted by scrambling torus method and then to the transformation of the secret data with Discrete Cosine Transform (DCT) compound with secured by a secret key for torus method initialization parameters. The randomness property of the resultant image reduces the possibility of its detection by the human visual system (HVS) and Steganalysis techniques.

Keywords: Steganography, encryption, Discrete Cosine Transform (DCT)

1. Introduction

Steganography is the technique of hiding data in the digital media. In contrast to cryptography [1], it is not to prevent attackers from recovering the enciphered content, but to prevent them from thinking about the existence of the data. In this technique, privacy is satisfied by embedding the secret data in the cover image. Recently, there has been extensive research interest in image steganography [2-13]. This is due to that, it overcomes some of the inherent limitations of cryptographic methods such as huge computational complexity and the possibility of modification or decryption of the secret data by the attackers [2]. Image steganography is applicable to a large number of applications such as secure communication between two or more parties, mobile computing, online voting systems, captioning and content protection, surveillance systems, and protection of medical records [3-6].

In this paper, we have presented a new image steganography algorithm, which has used a number of techniques to hide the secret image into the cover image. The utilized methods are encryption with Discrete Cosine Transform (DCT) and data substitution by Least Significant Bit (LSB). In the context of steganography techniques, encryption refers to the transformation of the embedded data such that it looks like a random noise as described in Ref. [6, 7]. In this way, the images becomes unrecognizable for Human Visual System (HVS). There is some transform functions such as fast fourier transform (FFT), wavelet transform function and its variants like lifted wavelet transform (LWT), discrete cosine transform and etc. in comparison,

There is some transform functions such as fast fourier transform (FFT), wavelet transform function and its variants like lifted wavelet transform (LWT), discrete cosine transform and etc. in comparison, FFT creates a transformed output image based on fourier formula with no extra operation, wavelet transform functions use two parameter for vertical and horizontal correlation that can produce four type of outputs with different security for hardening the data detection. DCT is the most common algorithm utilized in image steganography as a standard for JPEG image format with image quantization and compression. It is an orthogonal transform that uses a specific basis function with features like as low bit error rate, large compression ratio, perfect synthetic effect of computational complexity and perfect data integrated capability. DCT is a useful function for non-analytical applications like image processing and signal-processing applications such as video conferencing. Other advantage of DCT is the insertion of data in unimportant bits of coefficients. While, every alteration to any coefficient will impact the whole pixels of the block. By these features for mentioned transform functions and comparing their utility, we decided to employ the DCT function to realize the final output quality in stego image in our proposed method.

The DCT transforms the secret image from the spatial domain to the frequency domain. This transformation changes the image's structure and increases the robustness of the algorithm against steganalysis attacks which can be a good topic in our future work for comparing with the recent publications in literature.

The criteria to evaluate the steganography methods is the quality of stego image. In other words, the differences of cover and stego images should be minimized so that the HVS cannot distinguish between them. Due to the great processing power of the HVS, the proposed algorithms should minimize the variations in the stego image as little as possible [8]. To quantify the quality of stego images, two criteria are considered in the literature: Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM). These measures present the differences between the pixels of stego and cover images. As it is shown in the experimental results, our algorithm improves these measures in comparison with the previous algorithms. This means that the proposed scheme enhances the visual quality of the stego images, which makes it preferable compared to the existing solutions.

The rest of this paper is organized as follows. In Section II we review the previous steganography algorithms. Section III explains the proposed algorithms in details. The effectiveness of the algorithm in investigated in Section IV.

2. Related work

The proposed image steganography schemes in the literature can be divided into the categories of spatial [9-13], and frequency domain-based approaches, and the proposed algorithms which have employed artificial intelligent techniques. The aim of these approaches is to generate stego images which don't reveal any useful information about the secret data. In the following, we briefly review the proposed algorithms in each category.

A. Spatial domain-based algorithms

Most of the spatial domain-based schemes have considered RGB color model, ranging from the simple LSB substitution method to the advanced edge and saliency-based schemes [9]. These techniques have embedded messages in the intensity of the pixels directly [10]. Ref. [11] has improved LSB by using a new Pseudo Random Number Generator (PRNG) algorithm for generating random numbers, and a secret key to protect the secret data. The embedding process starts with deriving a seed for the PRNG from the user password. Next, it generates a random walk through the cover image, which complicates the steganalysis attacks. In an attempt to improve the visual quality of the stego images, the authors in [12] have presented the LSB matching (LSBM) method, which reduces the asymmetric effects by randomly adding/subtracting one to each pixel of the input image. Sun [14] has used Huffman coding for image steganography, where the secret data is only embedded in the edge of the cover image. This is due to that, the HVS is more sensitive to slight changes in smooth areas than edge regions. Moreover, Huffman table and Huffman encoding are employed to protect secret data. In order to diminish the differences between stego and cover images, the correction techniques are employed in the proposed algorithm.

A number of the existing spatial domain-based schemes comprise two phases of shuffling and masking. In the shuffling phase, the pixel intensity values of the cover image are permuted. Next, the resultant image is masked by a pseudo-random sequence in the next phase. In some studies, the resultant image is mixed with other pixels to produce a random-like image [9]. The problem with this technique is that, if the image is compressed, the secret data may be lost. This difficulty becomes more serious if the secret data contains sensitive information.

B. Frequency domain-based approaches

In these set of algorithms, the transformed coefficients are used for data embedding, which are generated using various transformation techniques such as DCT, Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). The main idea of these approaches is to scramble the transformed coefficients firstly. The resultant coefficients are fed into the inverse of the employed transformation function, to produce a random-like cipher image.

When the frequency domain-based techniques are used for data embedding, the hidden content is spread across the entire image, which provides better resistance against statistical and image processing attacks. The shortcoming of these schemes is that, they are computationally complex, which makes them inappropriate for various real-time applications.

3. Proposed work

A. Discrete cosine transform

For each color component, the JPEG image format uses a discrete cosine transform (DCT) to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients F(u, v) of an 8 × 8 block of image pixels f(x, y) are given by

$$F(u,v)=\frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)*\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right],$$

Where C(x) = 1/sqrt(2) when x equal 0 and C(x) = 1 otherwise. Afterwards, the following operation quantizes the coefficients:

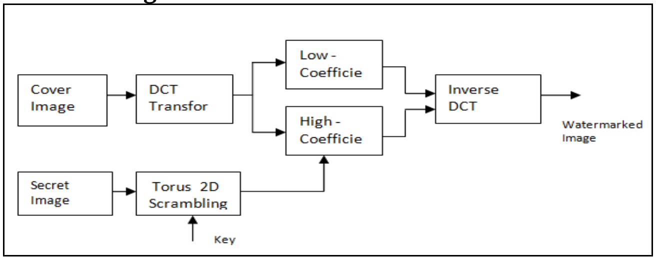
B. Torus Scrambling cosine transform

Torus auto morphism for pixel mixing a 2D torus auto morphism for the purpose of pixel mixing [13] is defined as follows:

$$\begin{pmatrix}p'\\q'\end{pmatrix}=\begin{pmatrix}1&1\\k&k+1\end{pmatrix}^{n}\begin{pmatrix}p\\q\end{pmatrix}\bmod N$$

Where (p,q) represents the original coordinate of the block of pixels, p',q' the coordinate after scatter, k is a selectable value for the transform matrix and n is the private scatter key (K,N 2 N). N is the breadth size of the image.

C. Block diagram



D. Results & Screen Shot

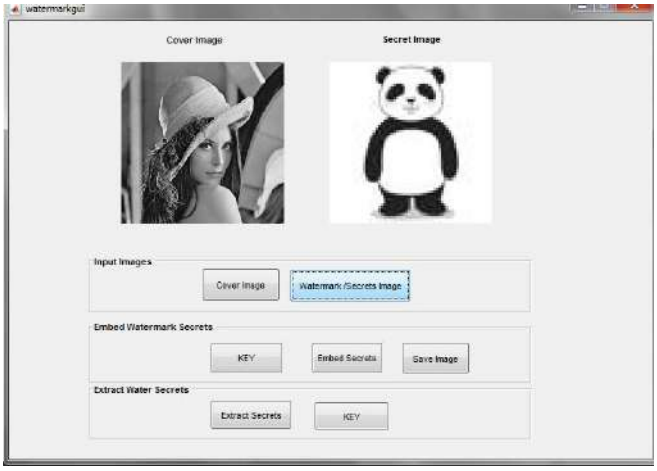


Fig 1: Cover image and secrete image

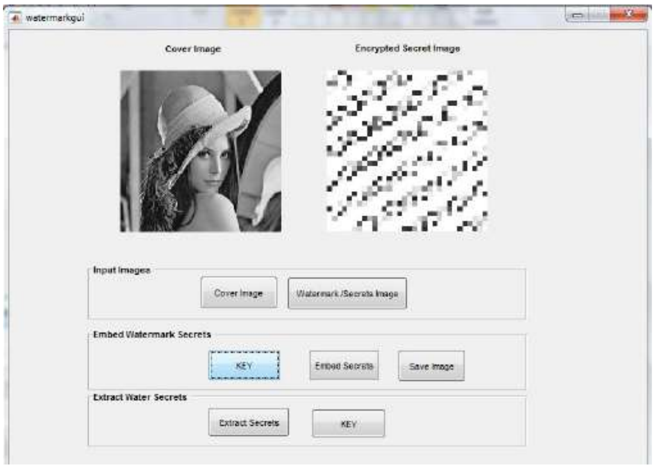


Fig 2: Cover image and scrambled secrete Image

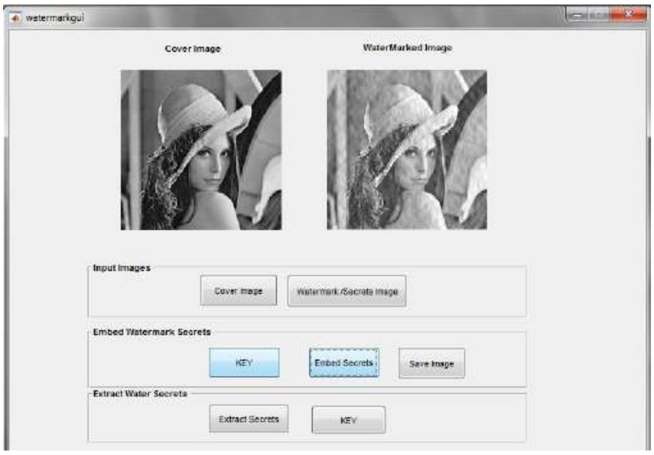


Fig 3: Scrambled secrete image embedded on cover image

4. References

1. J Daemen, V Rijmen. "The Design of Rijndael: AES-The advanced encryption standard", Springer science & business media, 2002.
2. L Bin, T Shunquan, W Ming, H Jiwu. "Investigation on cost assignment in spatial image steganography", IEEE Trans Inf. Forensics Secur. 2014; 9(8):1264-1277.
3. G Linjie, N Jiangqun, S Yun Qing. "Uniform embedding for efficient JPEG steganography", IEEE Trans Inf. Forensics Secur. 2014; 9(5):814-825.
4. W Mazurczyk, L Caviglione. "Steganography in modern smartphones and mitigation techniques", IEEE Commun Surv Tutor. 2014; 17(1):334-357.
5. J Li, X Li, B Yang, X Sun. "Segmentation-based image copy- move forgery detection scheme", IEEE Trans. Inf. Forensics Secur. 2015; 10(3):507-518.
6. A Kanso, M Ghebleh. "An algorithm for encryption of secret images into meaningful images", Optics and lasers in engineering. 2017; 90:196-208.
7. Jianhua Wu, Mengxia Zhang, Nanrun Zhou. "Image encryption scheme based on random fractional discrete cosine transform and dependent scrambling and diffusion", Journal of modern Optics, 2016.
8. S.J Thorpe. "Advances in computer graphics, Springer Science & business media", 1991, 309-341.
9. H.R Kanan, B Nazeri. "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert Syst. Appl. 2014; 41(14):6123-6130.
10. K Qazanfari, R Safabakhsh. "A new steganography method which preserves histogram: Generalization of LSB", Inform. Sci. 2014; 277:91-101.
11. W Zhang, X Zhang, S Wang. "A double layered "plus-minus one" data embedding scheme", IEEE Signal Process. Let. 2007; 14(11):848-851.
12. K Muhammad, J Ahmad, H Farman, Z Jan, M Sajjad, S.W Baik. "A secure method for color image steganography using gray-level modification and multi-level encryption", KSII Trans. Internet Inf. Syst. 2015; 9(5):1938-1962.
13. T.S Chen, J Chen, J.G Chen. A simple and efficient water marking technique based on JPEG 2000codec, in: International symposium on multimedia software engineering (ISMSE2003), IEEE, Taichung, Taiwan, 2003, 80-87.