Applied Soft Computing 30 (2015) 375–389

Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method

Sara Sajasi*, Amir-Masoud Eftekhari Moghadam

Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Iran

ARTICLE INFO

Article history:
Received 21 January 2013
Received in revised form 21 January 2015
Accepted 21 January 2015
Available online 29 January 2015

Keywords:
Image steganography
Noise Visibility Function (NVF)
Hybrid GA/PSO algorithm
Human Visual Sensitivity (HVS)
Least Significant Bit (LSB)
Cryptography

ABSTRACT

Steganography is the science of hiding secret message in an appropriate digital multimedia in such a way that the existence of the embedded message should be invisible to anyone apart from the sender or the intended recipient. This paper presents an irreversible scheme for hiding a secret image in the cover image that is able to improve both the visual quality and the security of the stego-image while still providing a large embedding capacity. This is achieved by a hybrid steganography scheme incorporates Noise Visibility Function (NVF) and an optimal chaotic based encryption scheme. In the embedding process, first to reduce the image distortion and to increase the embedding capacity, the payload of each region of the cover image is determined dynamically according to NVF. NVF analyzes the local image properties to identify the complex areas where more secret bits should be embedded. This ensures to maintain a high visual quality of the stego-image as well as a large embedding capacity. Second, the security of the secret image is brought about by an optimal chaotic based encryption scheme to transform the secret image into an encrypted image. Third, the optimal chaotic based encryption scheme is achieved by using a hybrid optimization of Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) which is allowing us to find an optimal secret key. The optimal secret key is able to encrypt the secret image so as the rate of changes after embedding process be decreased which results in increasing the quality of the stego-image. In the extracting process, the secret image can be extracted from the stego-image losslessly without referring to the original cover image. The experimental results confirm that the proposed scheme not only has the ability to achieve a good trade-off between the payload and the stego-image quality, but also can resist against the statistics and image processing attacks.

1. Introduction

With the rapid growth of network and Internet communications, information security becomes an important topic in real-time data transmission. In order to increase security, it is necessary to develop solutions protecting data, especially secret data. Information hiding has emerged as an effective scheme which makes private communication secure.

Steganography is a branch of information hiding carried out by embedding important data (e.g. text and image) in multimedia such as images, audios or videos. Since the digital images are the most widely used medium on the Internet and take advantage of human limited visual perception of colors and also provide a larger embedding capacity ratio, they are considered to be good carriers for steganography schemes. The image in which secret image will be inserted is called "*cover image*". The image that carries secret image is called "*stego-image*".

In order to enhance the security, many steganography schemes have been developed which encrypt the secret data by employing a data encryption scheme before hiding it [1–7]. Data encryption is used to protect secret data against illicit access by transforming it into an unrecognizable form using a particular cipher algorithm along with a secret key to obtain the cipher data [8]. In the decryption stage, only the user who has the key can retrieve the secret data from the cipher one. In general, the main purpose of a cryptography scheme is to make the secret data unreadable by a third party without hiding the existence of it. Steganography, in contrast, attempts to make data invisible to the unauthorized users. In this way, they are unable to notice the existence of the hidden data. Despite the differences among steganography and cryptography, combining them seems to allow a better private communication.

A steganography scheme is usually evaluated based on three parameters: *embedding capacity* (*payload*), *visual quality*, and *security*. The first parameter, payload, is determined by the amount of data concealed into a cover image. Higher payload allows inserting more data into the cover image. However, the embedding capacity can be increased insofar as the security of the secret data can still be ensured after embedding. The second parameter, visual quality, is considered to be good when the difference between the cover image and the stego-image can be perfectly imperceptible by *Human Visual Sensitivity* (*HVS*). Unfortunately, the fact is that there is an inverse relationship between the visual quality and the embedding capacity. This means that achieving just one requirement will totally sacrifice the other. The most straightforward solution to deal with this trade-off is to establish a balance between both of them. Finally, security preserves the secret data from being stolen by attackers. The major concern of this study focuses on increasing both the visual quality and the security of the stego-image while the capacity of the embedded secret image is kept at an acceptable level.

Typically, image steganography can simply be grouped into two types. The first type is an irreversible image steganography scheme which embeds the secret image

* Corresponding author. Tel.: +98 921 493 5248.
E-mail addresses: sara.sajasi@gmail.com (S. Sajasi), eftekhari@qiau.ac.ir (A.-M. Eftekhari Moghadam).

http://dx.doi.org/10.1016/j.asoc.2015.01.032
1568-4946/

into the cover image to achieve the stego-image. The advantage of an irreversible image steganography scheme is that it provides a high embedding capacity, although the stego-image cannot recover the cover image losslessly when the secret image is extracted from the stego-image. The second type is the reversible steganographic scheme which can produce a lossless recovery of the cover image from the stego-image when the secret image is extracted. It is appropriate for the applications (such as military maps, remote sensing images, medical images, etc.) where the cover image must be exactly reconstructed. However, we follow the first type schemes and propose an irreversible steganography scheme in order to achieve higher embedding capacity than the reversible schemes do.

1.1. Related work

Many steganography schemes have previously been proposed [10,11] in three domains: transform domain, spatial domain, and adaptive domain. The main focus of the first domain is on producing less distortion when embedding relatively small amount of data. To achieve this, first the cover image is transformed into a transform domain. Consequently, the secret data can be embedded into the transform coefficients. Finally, the stego-image is produced by an inverse transformation. The distinction of the transform domain schemes is due to the type of the transform function and the embedding process. To date, a great number of schemes have been developed based on the Discrete Cosine Transform (DCT) [12–17]. Most of the schemes in DCT-domain use JPEG images as a carrier. JPEG compression uses the DCT to transform the sub-image blocks into DCT coefficients. Then, the secret data can be concealed into these coefficients. Usually, steganography schemes use the low/middle frequency coefficients for embedding secret data because these coefficients are more robust during compression process than high frequency coefficients [18]. Also, a number of schemes are developed based on Discrete Wavelet Transform (DWT) [19–21]. DWT coefficients are closer to human visual system than DCT coefficients and the modification produced by noise and compression is less identifiable by human eyes. Despite the high security of the transform domain schemes, they are more sophisticated for implementation compared with the two other groups of steganography schemes.

The second group directly replaces the pixels of the cover image with the secret bits without taking the local texture into consideration. In other words, the capacity rate of each pixel in a cover image is the same and is independent of whether it is located on a smooth area or a complex area. Spatial domain schemes are more adapted with HVS and can provide more embedding capacity than transform domain schemes with an acceptable image quality. *Least Significant Bit* (*LSB*) substitution is the most commonly used scheme in spatial domain which embeds secret data by replacing K LSBs of a cover image pixels with K secret bits directly [22,23]. To date, many optimized LSB schemes have been proposed which focus on improving the stego-image quality and/or the embedding capacity [1,3,4,24–29]. An Optimal Pixel Adjustment Process (OPAP) has been proposed in [25] to improve the efficiency and the visual quality of the stego-image. GA has been employed in [4,24] to generate a substitution table in order to transform the value of the secret data to another value which is closer to the original value of the cover pixel. However, the substitution table performed well, it might not be the optimal solution. In order to obtain the optimal solution, a dynamic programming strategy has been employed in [1] to efficiently select the best from all possible substitution tables. Furthermore, a novel steganography scheme has been proposed based on LSB substitution with a key-permutation scheme where the best key has been selected using GA [3]. Moreover, PSO has been used in [27] to embed a message in an image and in [28] to hide an image within another image. Both schemes were using LSB substitution and achieved better results than the standard LSB scheme and the schemes based on GAs and dynamic programming. Although all these schemes obtained good quality stego-images, but they were not robust against image processing attacks like compression, noise, etc. [29]. This issue has been addressed in [26,29]. Distortion tolerance [26] has been proposed in spatial domain steganography to ensure that the stego-image was tolerant to image processing attacks. However, the stego-image quality was low in large payloads since the pixels used for data hiding were selected randomly. To solve this problem, PSO has been used in [29] to find the best pixel locations in an image where the secret image should be embedded. Generally, LSB substitution scheme is very simple and does not require complex computations. Also, it is able to hide a large amount of secret data. However, it has been shown in [30,31] that this scheme is not secure against statistical attacks.

Another type of embedding scheme has been proposed in [32] called Exploring Modification Direction (EMD) that employed n pixels as an embedding unit and embedded digits in $2n+1$ base. Its maximum payload was 1.161 bpp when $n=2$. Inspired by EMD, a Diamond Encoding (DE) scheme has been proposed to improve the payload of EMD [33]. In order to increase the payload, DE employed a pixel pair as an embedding unit and embedded digits in base B, where $B=2k2+2k+1$, and $k\geq 1$. A larger k indicated that a larger payload could be achieved with greater image distortion. DE was robust to LSB-based steganalysis schemes.

A main problem with the aforementioned schemes is that they concealed an equal amount of data into each pixel and cause equal degree of distortion. However, not all pixels in a cover image can tolerate an equal amount of changes without causing noticeable distortion. In other words, human vision is more sensitive to the modification of smooth areas than to the modification of complex areas. Hence, to improve the quality of the stego-image, the amount of bits are embedded in each pixel can be adaptively determined.

The third type, adaptive steganography, is a special case of the former schemes takes statistical global/local features of the image before interacting with its LSB, DCT or DWT coefficients. More recent schemes proposed to solve the above mentioned problems by exploiting the fact that more information can be conveyed in an image area with higher complexity, but conceal less on the area of lower complexity. Basically, the LSB substitution is used for embedding in this domain where the major concern is on improving the stego-image quality. The adaptive steganography schemes do not provide a great embedding capacity as well as LSB based schemes, but they are proven to be more secure with respect to attacks.

To reduce the visual artifacts in a stego-image, recently a number of studies have been developed [34–37]. In [34], eight modification directions were exploited to hide several secret bits into a cover pixel pair at a time. In [35], a steganography scheme has been proposed based on the modulus function. In [36], a secret message has been converted into a binary bit-string and embedded in the cover image according to a threshold, T, and two modulus values u and l. Finally, an adaptable process has been applied to decrease the modification of pixels values. Also, a new intelligent computing scheme based on Adaptive Neural Networks with Adaptive GA using Uniform Adaptive Relaxation (ANN AGAUAR) has been proposed in [37] to conceal a large amount of secret message into cover image efficiently and to achieve an excellent imperceptible stego-image.

Based on the sensitivity of human vision to smooth areas, a "Pixel-Value Differencing" (PVD) steganography scheme has been proposed in [38] where the size of embedding capacity can be determined according to the difference value between two consecutive pixels. The larger the difference value, the higher the embedding capacity rate. Similar to the PVD scheme, another scheme has been proposed in [39] which exploits side information and edge area of an image to embed secret data. By considering the concept of side information proposed in [40], the number of bits embedded into a pixel depended on the difference value between the pixel and its two, three, or four immediate neighboring pixels. In [31], a LSB + PVD approach has been presented which combined the PVD scheme with the LSB substitution scheme for the purpose of improving the capacity and the quality of the stego-image produced by the PVD scheme. According to their approach, smooth areas have been selected for embedding more secret data than complex areas which was in the contrary with the concept of HVS. Also, it could be detected by the steganalysis scheme proposed in [41,54]. To overcome this drawback, a novel PVD + LSB scheme has been developed in [42] to provide better PSNR values and could get rid of the detection scheme proposed in [41,54]. Furthermore, in [43] a new scheme combined PVD with the modulus function (MF-PVD) where the visual distortion degradation introduced by PVD scheme could be preserved. This was done by recording the secret data into two pixels based on computing the remainder value of them. Another scheme adopted the concept of PVD and proposed a data hiding scheme based on DE (DE-PVD) according to the local complexity of the cover image [44]. Their proposed scheme not only solved the noise problem that occurred in DE but also introduced Multiple-Base Notational System (MBNS) to embed digits in multiple bases. DE-PVD exploited PVD to estimate the base of digits to be embedded into the pixel pairs. Pixel pairs located into the complex areas were embedded with digits in larger base and the pixel pairs located into smooth areas were embedded with digits in smaller base. Moreover, two sophisticated adjustment processes were introduced for pixel pairs to maintain the division consistency and to avoid the overflow/underflow problem. DE-PVD was able to achieve better stego-image quality compared to the PVD and DE schemes. Inspired by PVD, for the purpose of increasing the embedding capacity [45], classified the embedding capacity of each pixel pair in two or three levels using the difference value of them. Then, secret bits could be hidden in each pixel pair using LSB substitution scheme. In order to provide a better stego-image quality and larger embedding capacity, a multi-pixel differencing based on modified LSB substitution scheme has been presented in [46] which considered the features of edge more efficiently than above proposed schemes. It considered a four-pixel block with three difference values to estimate how many secret bits into each block should be embedded sufficiently.

A problem arises with the aforementioned schemes is that however they make distinction between smooth areas and complex areas, but the actual edges in an image may never be taken into account. In other words, computing the difference value between two neighboring pixels may not lead to find the actual edges. To overcome this drawback, in [47], besides employing the LSB substitution scheme, the advantage of a hybrid edge detector (ED-LSB) has been considered to compute the actual edges in an image to conceal more secret bits into the edge pixels. The main limitation of this scheme was low embedding capacity. In other words, in high payloads, the visual quality of the stego-image has been decreased extremely and was completely unacceptable. To achieve larger embedding capacity [48], combined the schemes in [47] and [49]. After the hybrid edge detector applied on the cover image, the scheme in [49] has been used to compute the number of bits to be embedded for each pixel. In order to enhance the payload, the number of bits should be embedded in each edge pixel was increased by one. However, the embedding capacity was increased by this scheme, but the stego-image quality was still low.