Cover Processing-based Steganographic Model with Improved Security

Daniela Stănescu[1], Mircea Stratulat[1], Romeo Negrea[2], Ioana Ghergulescu[3]

[1]Computer Department, Politehnica University of Timisoara, 2 Vasile Parvan Boulevard, 300223 Timisoara, Romania (e-mail: daniela.stanescu@cs.upt.ro, mircea.stratulat@cs.upt.ro)

[2]Department of Mathematics, Politehnica University of Timisoara, 300006 Timisoara, Romania (e-mail: romeo.negrea@mat.upt.ro)

[3]Adaptemy, 27 Mount Street Lower, Dublin 2, Ireland (e-mail: ioana.ghergulescu@adaptemy.com)

Abstract: Steganography uses specialised techniques to conceal messages in different cover objects such as image or video so that only the sender and receiver know of the message's existence and are able to decipher it. Previous research conducted in the area has mainly focused on steganography and steganalysis techniques. This paper proposes a new model for steganography called Cover Processing-based Steganographic Model (CPSM) that processes the cover objects and transmits them in a way to improve the security of steganographic objects. A comprehensive demonstration based on information theory proves that CPSM provides improved security in terms of lower relative entropy as compared to previous models from the literature. Moreover, experimental tests show a decrease of the relative error between the cover and steganographic objects of up to 14%.

Keywords: steganographic model; cover processing; secret communication; security improvement; entropy

1 Introduction

The exchange of information plays a central role in many applications, with the Internet being the most representative example. As there is growing number of cyberattacks that affect businesses and end-users [1], the security of information storage and communication has become increasingly important. A recent study by IBM and Ponemon Institute showed that the average cost of a data breach was $3.79 million in 2015, while another study by Juniper Research forecasted that cybercrime will be a $2.1 trillion problem by 2019 [2].

In this context, there has been increased research interest on methods for securing information transmission such as steganography, watermarking and cryptography [3], [4]. While historical evidence suggests that steganography and cryptography methods have been applied since ancient times [5], their popularity and applicability were especially accelerated by the digital revolution of the past few decades [6]. Despite the fact that steganography, cryptography and watermarking are all methods for securing information, there are notable differences between them. Cryptography focuses on securing the information by making it illegible without having the proper key [7]. As opposed, steganography focuses on hiding the important information within another carrier, making it invisible to an observer. Based on the carrier type steganography can be divided into text or linguistic steganography [8], digital media steganography based on video, audio or images [9]–[11], as well as network steganography that exploits communication protocols [12]. While watermarking is also a method for embedding information, it differs from steganography in the sense that it is focused on protecting to carrier, and not the secret information [13].

Significant research effort was also dedicated to steganalysis methods[14]–[16]. Steganalysis represents the art of detecting the presence of hidden information, and depending on what the end goal is, to further determine the type of steganography, to extract the secret message or to tamper it so that the receiver can no longer extract it [14]. Therefore, steganographic systems must be both secure and robust to tampering by an active attacker or to artifacts that could result in the loss of the secret message such as network transmission errors.

Security represents the most important criteria of steganographic systems, with a system being considered secure if the existence of the message cannot be determined with higher probability than a random guessing. Existing approaches to quantify the security of steganographic systems include: information theory-based approach that considers the relative entropy or the difference between two probability distributions; ROC-based approach that considers the difference between true positive and false positive classification rates; and statistics-based approach that considers the maximum mean discrepancy to test if two samples are generated from the same distribution [14].

This paper proposes a new steganographic model called Cover Processing-based Steganographic Model (CPSM) that improves the security of steganographic objects by processing the carrier. The main advantage of the CPSM model is that the cover processing makes more difficult to detect and extract the message for an attacker. In extreme cases, it could reach a point where the detection would be too costly for an attacker. A comprehensive mathematical demonstration proves that CPSM provides improved security in terms of lower relative entropy as compared to previous models proposed in the literature. Furthermore, experimental testing shows that applying simple processing such as shifting the binary information of the cover image can lead to a decrease of the relative error between the cover and steganographic objects of up to 14%.

The rest of the paper is structured as follows. Section 2 presents related works in the area of steganography. Section 3 describes the proposed CPSM, while Section 4 presents the theoretical demonstration of the model using information theory. Section 5 presents the results of the experimental tests.

2 Related Work

Steganography has been the focus of much research interest over the past few decades, as well as increasing applicability into the real world [6]. A multitude of papers (e.g., [3], [4], [12], [14]–[22]), have reviewed the various techniques proposed in the literature for different types of steganography such as text, image, audio, video, or network steganography. Analysing those papers, one can note that past research works have mainly focused on specialised steganography and steganalysis techniques, with few generic models having been proposed.

Steganography as a method of hiding information was initially best described by Simmons in the prisoners' problem [23]. In this problem there are two prisoners that want to communicate. The only way of communication is via messages exchanged through an open channel, a warden. The warden will allow the message exchange as long as the information is open for inspection and there is no suspicion of hidden information. Furthermore, the warden will try to detect and intercept any suspicious messages. In order to communicate the prisoners will have to find a way of hiding information into innocent messages.

Zöllner et al. [24] proposed a basic embedding model that aimed to represent a steganographic system in an abstract and generic form. Figure 1 illustrates the basic embedding model for the case of image steganography. The model highlights that the sender wants to transmit a secret message m to a receiver. As the communication channel is not secure, the sender will use an innocent cover object C, in which it will hide the message using an embedding steganographic function f_E. The embedding process will result in the steganographic object S. For improved security, the system makes use of a steganographic key k that is passed as a parameter to the embedding function. The receiver will use an extraction function f_E^{-1} that will output the message m^* and the cover object C^*. If the extraction process is correct the message m^* will be the same as m. The authors also make use of information theory to model the security of a steganographic system. For a system to be considered secure, the embedding function should create a steganographic object S that has the same entropy as the cover object C (where the entropy $H(S)$ describes the uncertainty about S). However, the authors concluded that this cannot be achieved in practice assuming that the attacker can access and compare the cover and steganographic objects. Moreover, the authors concluded that only indeterministic steganography can be secure, by introducing a level of uncertainty about the cover that is higher than the entropy of the secret message.

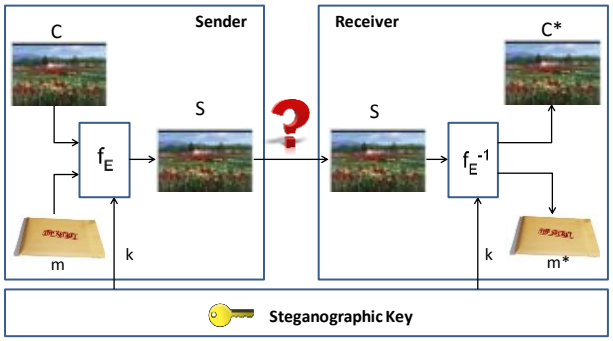

Figure 1
Basic embedding model of a steganographic system

Cachin [25] proposed an information-theoretic model for steganography that quantifies the security of the system in terms of the relative entropy between the probability distributions of the cover object C and steganographic object S. The author assumes that the sender avails of a set of innocent cover objects, in which it randomly embeds the secret message. The sender transmits steganographic objects or simply cover objects which have the purpose to confuse the attacker. The author also assumes that a passive attacker has complete access to the communication channel and has knowledge of the embedding function and of the cover object (i.e., knows the probability distribution of C). For a steganographic system to be secure the attacker should not be able to distinguish computationally between the cover and steganographic objects (i.e., the relative entropy to be ideally 0, or smaller thanεin case of anε-secure system). As the receiver would also not be able to detect the steganographic objects, the author proposes to use an oracle where the receiver has knowledge of when the sender is active. While this model presents much value from a theoretical point of view, the many assumptions limit its applicability in real-world steganographic systems.

Sallee [26] also proposed an information-theoretic model that uses statistical information of the cover object. The author also proposed a generic method to determine the maximum embedding capacity of the cover object while being resistant to first order statistical attacks, and further demonstrated the applicability of the model to JPEG images.

Raphael and Sundaram [27] have proposed a model that combines cryptography with steganography in order to increase the security of data communication. First, the secret message is encrypted using either secret or public cryptography key, and then embedded in the cover object using the steganographic key. In [28] the authors added another layer of protection to the model and proposed to transform the encrypted text into Unicode before hiding it into the cover image. However, while the authors have implemented a prototype and explained its functionality, they did not conduct a comprehensive evaluation of the proposed model.

Schöttle and Böhme [29] have proposed a universal game-theoretic framework to model adaptive embedding steganography systems which are considered to provide additional security as compared to systems based on random embedding. The model identifies the optimal adaptive embedding strategy that will maximise the security against attackers who would anticipate the adaptivity. The authors demonstrate that for real-world imperfect steganography systems the optimal embedding strategy is between naive adaptive and random uniform embedding.

Fakhredanesh et al. [30] have proposed a solution to overcome the perceptual detectability limitation of steganography systems based on cover image statistic models. By using Watson's human visual system model to compute the maximum acceptable changes in each DCT coefficients, the authors showed that steganographic objects with improved security and visually imperceptible changes can be obtained.

Song et al. [31] have proposed a digital steganography model based on additive noise and an embedding optimisation strategy aimed at providing guidance for the design of steganographic algorithms. The optimisation is done in terms of embedding modification position and direction. The authors have also validated experimentally that the proposed embedding optimisation technique can improve the security of steganographic algorithms such as LSBM and MG.

Denemark and Fridrich [32] have proposed a model-based embedding steganography method that makes use of multivariate Gaussian model to better estimate the acquisition noise, an important random aspect that makes digital images and videos suitable for steganography.

3 CPSM Overview

This section describes the proposed Cover Processing-based Steganographic Model (CPSM), that processes the cover objects and transmits them in a way to improve the security of steganographic objects from both a mathematical and practical point of view.

Figure 2 presents the functional block-level diagram of the CPSM model. The model pre-requisite is that the sender avails of a set of original cover objects C_R, which can be processed to create cover objects C that will be used in the steganographic process. The cover objects C are obtained by processing each original object C_R with the help of a processing function f_p. To confuse a possible attacker, the sender selects and incorporates the secret message only in some of the cover objects, which become steganographic objects S. However, the entire set of cover objects including those without hidden information are sent to receiver.

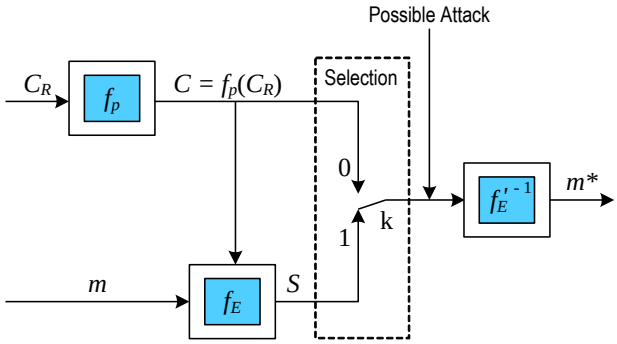

Figure 2
Functional diagram of the CPSM model

The selection of the cover objects is done with the help of a switch k. If the switch is on "0", then the cover object $C$is sent to the receiver. This does not contain any secret information but will help confuse the attacker. If the switch is on "1", then the steganographic object $S$is sent to the receiver. The operation of the switch is controlled according to a function known by both the sender and the receiver.

The processing function f_p can be based on an algorithm known by the sender, but depending on the available ways to improve the entropy of the resulting object this may not necessarily be known by the receiver. Embedding additional information into the cover object will increase its entropy, and a possible attacker could notice this increase if the cover object is not carefully selected.

Therefore, the changes made using the processing function will be done in such a way that the original cover object will not differ too much from the processed object. Transformations that could be applied through the processing function f_p include: applying noise, shifting the binary information towards higher or lower values, etc. As these transformations are applied in the same way to all of the original cover objects, the entropy increases for all objects not only for those that will be later transformed into steganographic objects. As such, it will be more difficult for a possible attacker to identify the transmitted objects containing the secret message. The critical condition is for the attacker not to have access to the original cover objects C_R.

The secret message m is embedded in some of the processed cover objects by applying the steganographic function f_E. Following this step, the complete set of objects, including steganographic objects S as well as processed cover objects $C$are sent to the receiver.

On another side, to extract the secret message the receiver will apply the inverse decoding function $f_E'^{-1}$, which consists of the inverse processing function f_p^{-1} composed with the inverse steganographic function f_E^{-1}. The composition of the two functions is done in such way that the output message m^*would be obtained

in a format as similar as possible to that of the original message m. Moreover, steganographic keys could be used to make it more difficult for an attacker to extract the secret message. However, in case of pure steganography it is not mandatory to use keys, as long as the steganographic algorithms are carefully selected [33], [34].

The next section demonstrates from a mathematical point of view how the security of steganographic systems is improved by the proposed CPSM model.

4 Theoretical Demonstration of CPSM

The aim of this section is to demonstrate that the proposed CPSM model provides an improved security as compared to the information theoretic model proposed by Cachin [25]. Cachin's approach is the most suitable for demonstrating the efficiency of steganographic systems from a probabilistic point of view. Other approaches from the literature review have only used simulations or empirical experiments to demonstrate the improved performance of their steganographic methods. According to Cachin, a steganographic object is perfectly secure if it meets the condition:

$$D(P_C \parallel P_S) = 0 \tag{1}$$

where, P_C is the probability distribution of the cover object C, while P_S is the probability distribution of the steganographic object S.

Moreover, $D(P_C \parallel P_S)$ represents the *relative entropy*, a measure of the difference between the two probability distributions P_C and P_S that characterise the steganographic process. The relative entropy is defined based on the Kullback–Leibler divergence [35]as in equation (2), where the units of entropy are bits and the log is logarithm to the base 2.

$$D(P_C \parallel P_S) = \sum_{c \in C} P_C(c) \cdot log \frac{P_C(c)}{P_S(c)} \tag{2}$$

If the condition from equation (1) is met there is no difference between the two probability distributions, and thus an attacker cannot distinguish between the cover object C and the steganographic object S. In this case, the attacker needs to analyse all the objects sent (C and S) and will not be able to extract in real time the hidden message from S using a polynomial algorithm. If there are differences between P_S and P_C, the attacker can focus only on the steganographic objects and will be able to extract the hidden message from S using a polynomial algorithm.

As perfect steganography is difficult to achieve in practice, it is desired to have a probability distribution P_S as close as possible to P_C. In this context, Cachin [25]defines a steganographic system to be ε-secure if:

$$D(P_C \parallel P_S) \leq \varepsilon \tag{3}$$

The smaller ε is, the harder will be for the attacker to distinguish between C and S, thus the harder to extract the hidden message from S.

Let k represent the switch from Figure 2 that can take two values:

$$k = \begin{cases} 0, & \text{if } c \in C_0 \\ 1, & \text{if } c \in C_1 \end{cases} \tag{4}$$

where the C alphabet is defined as:

$$C = C_0 \oplus C_1 \tag{5}$$

which means that C_0 and $C_1$are partitions of C, with C_0representing the subset when cover objects are transmitted to the receiver and C_1 representing the subset when steganographic objects are transmitted to the receiver, as such:

$$C_0 \cup C_1 = C, \text{ respectively } C_0 \cap C_1 = \emptyset \tag{6}$$

According to [25], in the above case a steganographic system is ε-secure for:

$$\varepsilon = \delta^2 / \ln 2 \tag{7}$$

where:

$$\delta = \Pr[c \in C_0] - \Pr[c \in C_1] \tag{8}$$

In equation (8), Pr denotes probability, while$\delta > 0$ because $\Pr[c \in C_0] > \Pr[c \in C_1]$, otherwise there would be big differences between P_S and P_C.

All of these are demonstrated starting from the following relationship:

$$P_S(c) = \begin{cases} \dfrac{P_C(c)}{1+\delta}, & \text{if } c \in C_0 \\ \dfrac{P_C(c)}{1-\delta}, & \text{if } c \in C_1 \end{cases} \tag{9}$$

which results by partitioning $C = C_0 \oplus C_1$ based on the total probability expressed as in equation (10), and conditional probability expressed as in equation (11) [36].

$$P(A) = \sum_{i \in I} P(A_i) \cdot P(A|A_i) \tag{10}$$

where, $i \in I$ indexes $A_i$mutually exclusive and exhaustive partitions of A.

$$P(A|B) = \frac{P(A \cap B)}{P(B)}, \text{ or } P(A \cap B) = P(A|B) \cdot P(B) \tag{11}$$

Indeed, we have:

$$\Pr[S = c] \overset{def}{=} \Pr[S = c | c \in C_0] \cdot \Pr[c \in C_0] + \Pr[S = c | c \in C_1] \cdot \Pr[c \in C_1] \tag{12}$$

However,

$$\begin{aligned}\Pr[S = c|c \in C_0] &= \Pr[C = c|c \in C_0 \text{ or } c \notin C_1] \\ &= \frac{\Pr[C = c \cap (c \in C_0 \text{ or } c \notin C_1)]}{\Pr[c \in C_0 \text{ or } c \notin C_1]} \\ &= \frac{\Pr(C = c)}{1 + \delta}\end{aligned} \tag{13}$$

if $c \in C_0$, because:

$$\begin{aligned}1 + \delta &= 1 + \Pr[c \in C_0] - \Pr[c \in C_1] \\ &= \Pr[c \in C_0] + 1 - \Pr[c \in C_1] \\ &= \Pr[c \in C_0] + \Pr[c \notin C_1] \\ &= \Pr[c \in C_0 \text{ or } c \notin C_1]\end{aligned} \tag{14}$$

Similarly:

$$\begin{aligned}\Pr[S = c|c \in C_1] &= \Pr[C = c|c \notin C_0 \text{ or } c \in C_1] \\ &= \frac{\Pr[C = c \cap (c \notin C_0 \text{ or } c \in C_1)]}{\Pr[c \notin C_0 \text{ or } c \in C_1]} \\ &= \frac{\Pr(C = c)}{1 - \delta}\end{aligned} \tag{15}$$

if $c \in C_1$, because:

$$\begin{aligned}1 - \delta &= 1 - \Pr[c \in C_0] + \Pr[c \in C_1] \\ &= \Pr[c \notin C_0] + \Pr[c \in C_1] \\ &= \Pr[c \notin C_0 \text{ or } c \in C_1]\end{aligned} \tag{16}$$

Moreover,

$$\Pr[c \in C_0] = \begin{cases} 1, & \text{if } c \in C_0 \\ 0, & \text{if } c \in C_1 \end{cases} \tag{17}$$

$$\Pr[c \in C_1] = \begin{cases} 0, & \text{if } c \in C_0 \\ 1, & \text{if } c \in C_1 \end{cases} \tag{18}$$

According to [24], steganographic systems cannot be secure if an attacker knows C and S, thus being able to compare two objects that are similar but still contain different information. To address this issue, the authors introduce a degree of uncertainty to the cover object C. This will confuse the attacker, as the comparison will be done between the steganographic object S containing hidden information, and a cover object C that the attacker does not know and only estimates how it looks like. We will investigate the behaviour of entropy, which characterises both elements considered in the comparison by the attacker, namely: information and uncertainty.

An example in this sense would be capturing a photo and using it as a medium for transmitting some secret information. The sender will choose the scene and will capture it using a photo camera. The original photo representing the cover object C is processed to incorporate the secret message becoming the steganographic

object S, which is sent over an unsecured channel. When intercepted by an attacker, this recognises the scene represented in the photo but does not have access to the original photo C, hence the uncertainty. As the original photo C is not available, the attacker cannot compare it with the intercepted steganographic object S, and will not be able to extract the secret message from S.

In order to obtain the original cover object, one approach would be for the attacker to identify the scene captured in the photo, make similar photos and compare them with S. As digital camera sensors are sensitive to factors that cannot be accurately controlled such as temperature, the attacker would notice small differences even between photos of the scene captured consecutively. Therefore, if differences are noticed due to uncontrolled factors no matter how many attempts are made to obtain the cover object C, the attacker might conclude that it is normal for the steganographic object S to also present differences. As opposed, if all captured photos are identical and only S presents differences, the attacker might think that S contains a hidden message.

As such, the steganographic model proposed by Zöllner et al. [24] involves choosing a cover object that is unknown to a possible attacker, and pre-processing it using different equipment or digital techniques before being used to create the steganographic object. However, the authors do not demonstrate that the model provides improved security. The steganographic model proposed by Cachin [25] involves choosing a set of cover objects, with only some of them being used to create the steganographic object. In case of this model, the sender transmits both the cover and the steganographic objects to the receiver.

The CPSM steganographic model proposed in this paper involves choosing a set of cover objects that are individually processed, and only some of them are used to create steganographic objects. Next, we will prove mathematically that applying a processing function on the cover objects can improve the security of steganographic systems.

As illustrated in Figure 2 the CPSM model applies a processing function f_p on each cover object. By applying this function, the relative error ε will decrease to be lower than the value obtained by Cachin.

Suppose that the chosen processing function takes the form:

$$f_p(x) = a \cdot x, \text{ where } a > 1 \tag{19}$$

Using this function, the set of cover objects C can be obtained based on the initial set C_R, as follows:

$$C = f_p(C_R) \tag{20}$$

Following the processing we will prove that:

$$\varepsilon = \frac{1}{a^2} \cdot \delta^2 / \ln 2 \tag{21}$$

thus, the ε measure obtained is lower than the one obtained by Cachin and presented in equation (7).

To prove equation (21), we start from Theorem 1 and Theorem 2 proposed in [25], according to which:

$$D(P_C \parallel P_S) \leq D(P_{C_R} \parallel P_S) \leq \delta^2 / \ln 2 \tag{22}$$

By performing a change of variable on equation (2) the relative entropy can be expressed in terms of the new variable d, as:

$$D(P_C \parallel P_S) = \sum_{d \in C} P_C(d) \cdot \log \frac{P_C(d)}{P_S(d)} \tag{23}$$

However,

$$P_S(d) = \begin{cases} \dfrac{P_C(d)}{1+\delta}, & \text{if } d \in C_0 \\ \dfrac{P_C(d)}{1-\delta}, & \text{if } d \in C_1 \end{cases} \tag{24}$$

where:

$$\delta = \Pr[d \in C_0] - \Pr[d \in C_1] \tag{25}$$

Therefore,

$$D(P_C \parallel P_S) = \sum_{d \in C_0} P_C(d) \cdot \log(1+\delta) + \sum_{d \in C_1} P_C(d) \cdot \log(1-\delta) \tag{26}$$

For $C = f_p(C_R)$ we have:

$$P_C(d) = \left| \frac{1}{f_p{}'(f_p^{-1}(d))} \right| \cdot P_{C_R}(f_p^{-1}(d)) \tag{27}$$

if:

$$f_p(x) = a \cdot x \Rightarrow \begin{cases} f_p^{-1}(x) = \dfrac{x}{a} \\ f_p{}'(x) = a \end{cases} \tag{28}$$

The following notation is adopted:

$$f_p^{-1}(d) = \frac{d}{a} = c \tag{29}$$

where $d \in C$, which implies that:

$$c \in C_a = \frac{1}{a} C \tag{30}$$

In the context of the paper, C represents the set of pixels from an image, thus C_a represents the set of pixels scaled with the a constant. Therefore, based on equations (26) and (27) results that:

$$\begin{aligned} D(P_C \parallel P_S) &= \frac{1}{a}\sum_{d\in C_0} P_{C_R}\left(\frac{d}{a}\right)\cdot\log(1+\delta) + \frac{1}{a}\sum_{d\in C_1} P_{C_R}\left(\frac{d}{a}\right)\cdot\log(1-\delta) \\ &= \frac{1}{a}\sum_{c\in C_0}\frac{1}{a}P_{C_R}(c)\cdot\log(1+\delta) + \frac{1}{a}\sum_{c\in C_1}\frac{1}{a}P_{C_R}(c)\cdot\log(1-\delta) \\ &= \frac{1}{a^2}\sum_{c\in C_0} P_{C_R}(c)\cdot\log(1+\delta) + \frac{1}{a^2}\sum_{c\in C_1} P_{C_R}(c)\cdot\log(1-\delta) \\ &= \frac{1}{a^2}\cdot\left[\frac{1+\delta}{2}\cdot\log(1+\delta) + \frac{1-\delta}{2}\cdot\log(1-\delta)\right] \end{aligned} \tag{31}$$

because,

$$\sum_{c\in C_0} P_{C_R}(c) = \frac{1+\delta}{2} \tag{32}$$

$$\sum_{c\in C_1} P_{C_R}(c) = \frac{1-\delta}{2} \tag{33}$$

Moreover, using the fact that

$$\log(1+x) \le \frac{x}{\ln 2} \tag{34}$$

results:

$$\begin{aligned} D(P_C \parallel P_S) &\le \frac{1}{a^2}\left(\frac{1+\delta}{2}\cdot\frac{\delta}{\ln 2} + \frac{1-\delta}{2}\cdot\frac{-\delta}{\ln 2}\right) \\ &\le \frac{1}{a^2}\cdot\frac{\delta^2}{\ln 2} \end{aligned} \tag{35}$$

On another side:

$$\begin{aligned} D(P_{C_R} \parallel P_S) &= \sum_{c\in C_0} P_{C_R}(c)\cdot\log(1+\delta) + \sum_{c\in C_1} P_{C_R}(c)\cdot\log(1-\delta) \\ &= \frac{1+\delta}{2}\cdot\log(1+\delta) + \frac{1-\delta}{2}\cdot\log(1-\delta) \\ &\le \frac{1+\delta}{2}\cdot\frac{\delta}{\ln 2} + \frac{1-\delta}{2}\cdot\frac{-\delta}{\ln 2} \\ &\le \frac{\delta^2}{\ln 2} \end{aligned} \tag{36}$$

where,

$$\delta = P_{C_R}[c|c \in C_0] - P_{C_R}[c|c \in C_1] \tag{37}$$

and:

$$\begin{aligned} 1 + \delta \quad &= P_{C_R}[c|c \in C_0] + 1 - P_{C_R}[c|c \in C_1] \\ &= P_{C_R}[c|c \in C_0] + P_{C_R}[c|c \notin C_1] \end{aligned} \tag{38}$$

If $|C_0| = |C_1|$, then:

$$\sum_{c \in C_0} P_{C_R}(c) = \sum_{c \in C_1} P_{C_R}(c) = \frac{1}{2} \tag{39}$$

because,

$$\sum_{c \in C} P_{C_R}(c) = 1 \tag{40}$$

Finally, based on equations (31) and (36) results that:

$$\frac{D(P_C \parallel P_S)}{D(P_{C_R} \parallel P_S)} = \frac{1}{a^2} \tag{41}$$

where $a > 1$.

The conclusion that can be drawn from the theoretical demonstration is that processing the cover object with a coefficient where $a > 1$, leads to a decrease by $1/a^2$in the relative entropy between the probability distribution of the steganographic object obtained and the probability distribution of the cover object. Therefore, the proposed CPSM model enables improved security of steganographic systems thought three different aspects: (i) the generation of a set of cover objects that are known by the sender but not necessarily known by the receiver, (ii) the individual processing of the cover objects, and (iii) the random selection of one or multiple cover objects in which to embed the secret messages.

In order to support the receivers, it is desired to inform them about the procedure used for selecting the cover objects that will be used as steganographic objects. If this information is missing, the receiver will have to apply the inverse decoding function $f_E'^{-1}$ for the full set of received objects, thus requiring a longer time to retrieve the hidden message. It is also possible that multiple messages that are retrieved to have significance, thus confusing the receiver. To avoid such situations, one solution would be to inform the receiver about the function used in order to select the cover objects used in the steganographic process.

5 Experimental Validation of CPSM

A number of experimental tests were conducted in order to validate the proposed CPSM model from an empirical perspective. The Segment Compression Steganographic Algorithm (SCSA) proposed in [37] was used for the experimental testing. SCSA is based on the Karhunen-Loève Transform (KLT) that is widely considered to achieve optimal signal processing for data representation, compression and analysis. A detailed description of the algorithm can be found in [37].

A multitude of colour images with different size and content characteristics were used as cover objects. The secret messages were also represented by colour images that were incorporated within the cover objects on the least important bits. In line with the principle of the CPSM model, the cover objects were first processed by applying a number of transformations. In particular, the binary information of each pixel was shifted with a number of steps towards black, and respectively white.

Tables 1 to 3 present the experimental results for the three scenarios considered for hiding the secret messages (i.e., on the least important 1, 2 and 4 bits of the cover objects). Columns 2 to 5 present the name and size in pixels of the cover objects and secret messages. Columns 6 to 10 present the computed relative errors between the cover objects and the steganographic objects for five different cases: the pixels binary information was shifted towards black with a value of 10 and respectively 6, the cover object was not processed, and the pixels binary information was shifted towards white with a value of 6 and 10. The last column presents the improvement (as percentage) of the relative error that was achieved through the processing of the cover object.

The results analysis shows that processing the cover objects can decrease the relative error between the cover and the steganographic objects. In particular, shifting the pixels binary information towards black leads to a decreased relative error, for all three test scenarios using the SCSA algorithm to hide the message on 1, 2 and 4 bits. The results show that the maximum improvement of the relative error was 13.68% in case of the 'sphinx' cover object and 'Hawk' secret message using SCSA on 4 bits. While for some cases the improvement of the relative error is not significant, one observation made was that in such cases the cover objects usually presented large areas with the same information (e.g., background). Therefore, one can safely conclude that such cover objects are not recommended for steganography.

Figure 3 illustrates the processing for one example considered in the experimental testing (i.e., 'Wildflowers' cover object and 'watch' secret message using SCSA on 4 bits). The images show that the difference between the cover and steganographic objects is unnoticeable, for all three scenarios: unprocessed cover object, processing towards black and towards white respectively. In terms of the

relative error between the cover and steganographic object, the improvement achieved was 2.09% (see Table 3, line 2).

The experimental results validate that the CPSM model can lead to better steganographic objects and thus improved security, as compared to not processing the cover objects.

Table 1

Cover object processing experimental results using the SCSA algorithm on 1 bit

	Cover Object		Secret Message		Cover Object Processing					
Seq.	Name	Size [px]	Name	Size [px]	ε^{-10}	ε^{-6}	ε^{0}	ε^{6}	ε^{10}	%
1	lena	256x256	firefox	128x128	0.19735	0.19744	0.19745	0.19760	0.19778	2.17
2	Aquaria	256x256	firefox	128x128	0.19558	0.19611	0.19657	0.19652	0.19664	5.42
3	dogs	640x480	wildflowers	200x135	0.19510	0.19530	0.19592	0.19595	0.19605	4.86
4	dogs	640x480	watch	200x135	0.19506	0.19545	0.19617	0.19637	0.19689	9.38
5	fruit	512x512	lena	256x256	0.19428	0.19460	0.19557	0.19635	0.19664	1.21
6	fruit	512x512	Aquaria	256x256	0.19413	0.19452	0.19554	0.19635	0.19670	1.32
7	Lena512	512x512	Aquaria	256x256	0.19630	0.19631	0.19631	0.19638	0.19646	0.08
8	Lena512	512x512	lena	256x256	0.19619	0.19620	0.19620	0.19625	0.19628	0.04
9	building	640x480	wildflowers	200x135	0.18922	0.19062	0.19504	0.19772	0.19850	4.10
10	building	640x480	watch	200x130	0.18731	0.18930	0.19586	0.20201	0.20422	9.02
11	Alicia	1024x1024	Lena512	512x512	0.19419	0.19505	0.19576	0.19576	0.19576	0.8
12	Alicia	1024x1024	fruit	512x512	0.19102	0.19402	0.19566	0.19566	0.19566	2.4
13	Alicia	1024x1024	dogs	640x480	0.19081	0.19384	0.19565	0.19565	0.19565	2.5
14	car	1024x1036	dogs	640x480	0.19457	0.19459	0.19459	0.19461	0.19461	0.02
15	car	1024x1036	fruit	512x512	0.19400	0.19402	0.19402	0.19402	0.19403	0.015
16	car	1024x1036	Leno512	512x512	0.19638	0.19639	0.19639	0.19639	0.19640	0.01
17	football	1600x1200	building	640x480	0.19305	0.19416	0.19574	0.19629	0.19641	1.74
18	football	1600x1200	hawk	800x600	0.19301	0.19426	0.19590	0.19646	0.19660	1.86
19	football	1600x1200	sphinx	800x600	0.19435	0.19493	0.19583	0.19609	0.19617	0.9
20	fish	1600x1200	building	640x480	0.19373	0.19454	0.19559	0.19575	0.19586	1.1
21	fish	1600x1200	hawk	800x600	0.19353	0.19437	0.19552	0.19568	0.19580	1.17
22	fish	1600x1200	sphinx	800x600	0.19497	0.19538	0.19585	0.19591	0.19596	0.5

Table 2

Cover object processing experimental results using the SCSA algorithm on 2 bits

	Cover Object		Secret message		Cover Object Processing					
Seq.	Name	Size [px]	Name	Size [px]	ε^{-10}	ε^{-6}	ε^{0}	ε^{6}	ε^{10}	%
1	lena	256x256	merlin	128x128	0.54283	0.54341	0.54516	0.54465	0.54605	0.59
2	Lena	256x256	firefox	128x128	0.54657	0.54734	0.54914	0.54873	0.55023	0.53
3	Aquaria	256x256	firefox	128x128	0.54226	0.54432	0.54822	0.55144	0.55219	1.83
4	Aquaria	256x256	merlin	128x128	0.53958	0.54173	0.54277	0.54904	0.54979	1.89
5	Aquaria	256x256	watch	200x135	0.51725	0.51843	0.52248	0.52335	0.52403	1.31
6	Lena	256x256	watch	200x135	0.52042	0.52071	0.52238	0.52155	0.52341	0.57
7	Lena512	512x512	Aquaria	256x256	0.55789	0.55791	0.55757	0.55833	0.55864	0.13
8	fruit	512x512	lena	256x256	0.56109	0.54215	0.54268	0.56330	0.56588	4.58
9	fruit	512x512	Aquaria	256x256	0.56718	0.54826	0.56248	0.57653	0.57993	5.77
10	sphinx	800x600	fruit	512x512	0.50414	0.50415	0.52086	0.53481	0.53739	8.57
11	hawk	800x600	fruit	512x512	0.51281	0.51281	0.51001	0.51974	0.52670	2.70
12	Alicia	1024x1024	hawk	800x600	0.51574	0.53007	0.53995	0.54134	0.54134	4.96
13	Alicia	1024x1024	sphinx	800x600	0.51144	0.52137	0.52615	0.52680	0.52680	3.00
14	car	1024x1036	hawk	800x600	0.53980	0.53995	0.53938	0.56009	0.54019	0.07
15	car	1024x1036	sphinx	800x600	0.52675	0.52677	0.52362	0.52679	0.52683	0.02
16	fish	1600x1200	Alicia	1024x1024	0.54490	0.54790	0.55266	0.55661	0.55705	2.22
17	football	1600x1200	Alicia	1024x1024	0.54110	0.54497	0.55655	0.56314	0.56442	4.30
18	football	1600x1200	car	1024x1036	0.52558	0.52844	0.53536	0.53898	0.53951	2.65

Table 3

Cover object processing experimental results using the SCSA algorithm on 4 bits

	Cover Object		Secret Message		Cover Object Processing					
Seq.	**Name**	**Size [px]**	**Name**	**Size [px]**	ε^{-10}	ε^{-6}	ε^{0}	ε^{6}	ε^{10}	**%**
1	merlin	128x128	firefox	128x128	2.20065	2.21202	2.23028	2.21129	2.21925	0.85
2	Wildflowes	200x135	watch	200x135	2.11924	2.10974	2.10306	2.09935	2.16363	2.09
3	Lena	256x256	Aquaria	256x256	2.34364	2.37548	2.43198	2.35479	2.39349	2.12
4	Aquaria	256x256	lena	256x256	2.19141	2.23095	2.23256	2.21132	2.25572	2.93
5	Lena512	512x512	Fruit	512x512	2.22543	2.26987	2.27184	2.22689	2.27292	2.13
6	building	640x480	Dogs	640x480	2.36194	2.36677	2.47886	2.55992	2.60113	10.12
7	sphinx	800x600	Hawk	800x600	2.41660	2.44265	2.65467	2.72818	2.74720	13.68
8	hawk	800x600	Sphinx	800x600	2.34786	2.32531	2.28728	2.41975	2.48425	5.80
9	Alicia	1024x1024	Car	1024x1036	2.36585	2.39247	2.41650	2.53694	2.47603	4.65
10	car	1024x1036	Alicia	1024x1024	2.64180	2.75105	2.55188	2.64529	2.75354	4.22
11	fish	1600x1200	football	1600x1200	2.32144	2.32860	2.35385	2.36267	2.36583	1.91

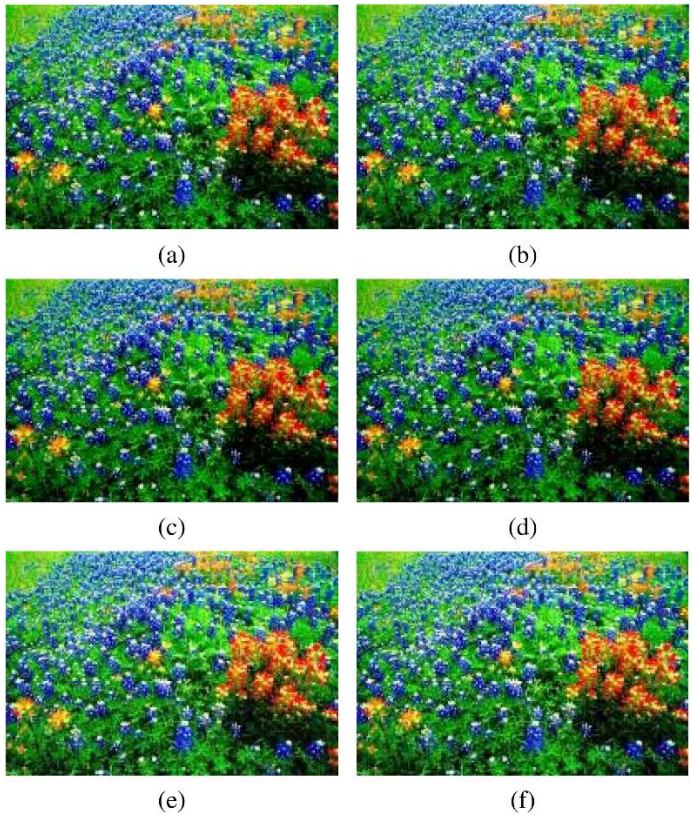

Figure 3

Exemplification of processing for ‘Wildowers’ cover object and `watch' secret message:
(a) Unprocessed cover object and (b) corresponding steganographic object; (c) Cover object with processing towards black and (d) corresponding steganographic object; (e) Cover object with processing towards white and (f) corresponding steganographic object

Conclusions

The increasing need for secure data communication methods, contributed to steganography gradually moving out of the research laboratory and into the real-world applications. To improve the security of steganographic objects, this paper has proposed the Cover Processing-based Steganographic Model (CPSM). CPSM adds a new layer of security to traditional steganographic models by processing the cover objects before embedding the messages. Moreover, to further complicate steganalysis the model makes use of random selection and embedding, where the sender transmits randomly either steganographic objects containing hidden information or processed cover objects aimed at confusing the attacker. A comprehensive demonstration based on information theory, proved that the CPSM model offers an improved security in terms of lower relative entropy as compared to the previous information-theoretic model proposed by Cachin. Experimental tests were conducted in order to further validate the benefits of the proposed model. The results showed that applying simple processing such as shifting the binary information of the cover image can lead to a decrease of the relative error between the cover and steganographic objects of up to 14%. Out future research work will aim to further improve the security of the proposed model by considering additional techniques such as processing the secret message along with the cover objects.

References

[1] Symantec, "Internet Security Threat Report 2017," Symantec Corporation, Mountain View, CA, 22, Apr. 2017 [Online] Available: https://www.symantec.com/security-center/threat-report

[2] L. Kessem, "2016 Cybercrime Reloaded: Our Predictions for the Year Ahead," Jan. 2016 [Online] Available: https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/

[3] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, Vol. 90, No. 3, pp. 727-752, Mar. 2010

[4] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, "Trends in Steganography," *Communications of the ACM*, Vol. 57, No. 3, pp. 86-95, Mar. 2014

[5] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, 2nd ed. CRC Press, 2017

[6] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevný, "Moving Steganography and Steganalysis from the Laboratory into the Real World," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security*, New York, NY, USA, 2013, pp. 45-58

[7] D. Caragata and I. Tutanescu, "On the security of a new image encryption scheme based on a chaotic function," *Signal, Image and Video Processing*, Vol. 8, No. 4, pp. 641-646, 2014

[8] A. Wilson, P. Blunsom, and A. D. Ker, "Linguistic steganography on Twitter: hierarchical language modeling with manual interaction," in *Proc. SPIE 9028, Media Watermarking, Security, and Forensics 2014*, 2014, p. 902803

[9] D. Stanescu, M. Stratulat, V. Groza, J. Ghergulescu, and D. Borca, "Steganography in YUV color space," in *2007 International Workshop on Robotic and Sensors Environments*, 2007, pp. 1-4

[10] Z. Shahid, M. Chaumont, and W. Puech, "Considering the reconstruction loop for data hiding of intra- and inter-frames of H.264/AVC," *SIViP*, Vol. 7, No. 1, pp. 75-93, 2013

[11] B. J. Mohd, S. Abed, B. Na'ami, and T. Hayajneh, "Hierarchical steganography using novel optimum quantization technique," *SIViP*, Vol. 7, No. 6, pp. 1029-1040, 2013

[12] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," *IEEE Communications Magazine*, Vol. 52, No. 5, pp. 225-229, May 2014

[13] D. Stanescu, V. Groza, M. Stratulat, D. Borca, and I. Ghergulescu, "Robust Watermarking with High Bit Rate," in *Third International Conference on Internet and Web Applications and Services, 2008. ICIW '08*, 2008, pp. 257-260

[14] B. Li, J. He, J. Huang, and Y. Q. Shi, "A Survey on Image Steganography and Steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 2, No. 2, pp. 142-172, 2011

[15] C. Paulin, S. A. Selouani, and É. Hervet, "A comparative study of audio/speech steganalysis techniques," in *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)* 2017, pp. 1-4

[16] J. Babu, S. Rangu, and P. Manogna, "A Survey on Different Feature Extraction and Classification Techniques Used in Image Steganalysis," *Journal of Information Security*, Vol. 08, No. 03, pp. 186-202, Jul. 2017

[17] R. Amirtharaj, J. Qin, and J. B. Balaguru R, "Random Image Steganography and Steganalysis: Present Status and Future Directions," *Information Technology Journal*, Vol. 11, No. 5, pp. 566-576, May 2012

[18] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *International Journal of Computer Science and Security (IJCSS)*, Vol. 6, No. 3, pp. 168-187, 2012

[19] R. J. Mstafa and K. M. Elleithy, "Compressed and raw video steganography techniques: a comprehensive survey and analysis," *Multimedia Tools and Applications*, Vol. 76, No. 20, pp. 21749-21786, Oct. 2017

[20] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools and Applications*, Vol. 77, No. 13, pp. 17333-17373, Jul. 2018

[21] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, Vol. 65, pp. 46-66, Jul. 2018

[22] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, Nov. 2018

[23] G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," in *Advances in Cryptology*, D. Chaum, Ed. Springer US, 1984, pp. 51-67

[24] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the Security of Steganographic Systems," in *Information Hiding*, Springer Berlin Heidelberg, 1998, pp. 344-354

[25] C. Cachin, "An information-theoretic model for steganography," *Information and Computation*, Vol. 192, No. 1, pp. 41-56, Jul. 2004

[26] P. Sallee, "Model-Based Steganography," in *Digital Watermarking*, T. Kalker, I. Cox, and Y. M. Ro, Eds. Springer Berlin Heidelberg, 2003, pp. 154-167

[27] A. J. Raphael and V. Sundaram, "Cryptography and Steganography-A Survey," *International Journal of Computer Technology and Applications*, Vol. 02, No. 03, pp. 626-630, May 2011

[28] A. J. Raphael and V. Sundaram, "Secured Crypto-Stegano Communication through Unicode," *World of Computer Science and Information Technology Journal*, Vol. 1, No. 4, pp. 138-143, 2011

[29] P. Schöttle and R. Böhme, "Game Theory and Adaptive Steganography," *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 4, pp. 760-773, Apr. 2016

[30] M. Fakhredanesh, R. Safabakhsh, and M. Rahmati, "A Model-Based Image Steganography Method Using Watson's Visual Model," *ETRI Journal*, Vol. 36, No. 3, pp. 479-489, Jun. 2014

[31] H.-T. Song, G.-M. Tang, G. Kou, Y.-F. Sun, and M.-M. Jiang, "Digital steganography model and embedding optimization strategy," *Multimed Tools Appl*, Nov. 2018

[32] T. Denemark and J. Fridrich, "Model based steganography with precover," in *IS&T International Symposium on Electronic Imaging 2017, Media Watermarking, Security, and Forensics 2017*, 2017, pp. 56-66

[33] Z. K. AL-Ani, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Overview: Main Fundamentals for Steganography," *Journal of Computing*, Vol. 2, No. 3, 2010

[34] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000

[35] D. Dumitrescu, I.-M. Stan, and E. Simion, "Steganography techniques," 341, 2017 [Online] Available: https://eprint.iacr.org/2017/341

[36] J. Devore, *Probability and Statistics for Engineering and the Sciences*, 8th ed. Cengage Learning, 2012

[37] D. Stanescu, I.-G. Bucur, and M. Stratulat, "Segment Compression Steganographic Algorithm," in *2010 International Joint Conference on Computational Cybernetics and Technical Informatics (ICCC-CONTI)* 2010, pp. 349-354