A Generalized Multi-layer Information Hiding Scheme Using Wet Paper Coding

Amir Bidokhti
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
bidokhti@ee.sharif.edu

Shahrokh Ghaemmaghami
Electronics Research Institute and
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
ghaemmag@sharif.ir

Abstract—Multi-layer schemes have been proposed for steganography. Also some authors have combined these methods with the idea of wet paper codes, which are embedding codes that use side information only available to the sender, and gained higher embedding efficiency. This paper proposes a generalized multi-layer method for wet paper embedding. First, the cover bits are divided into blocks and, by combining these bits in groups of 3, a pyramid is formed. Next, the secret message is embedded through a layer-by-layer procedure. The proposed method has higher embedding efficiency in some cases and provides more flexibility for choosing the embedding payload, especially in lower payload conditions.

Keywords—Steganography; Wet Paper Codes; Embedding efficiency; Embedding payload

I. INTRODUCTION

Steganography is the technique of concealing information within seemingly innocuous carriers. It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. To this goal, the sender chooses proper parts of the cover to embed the message. This parts are called embedding channel. The choice of embedding channel in steganography is an important issue which dramatically affects steganographic security. In most traditional steganography methods, it is necessary for the communicating parties to agree on this channel or the rule to choose this channel based on both the cover and the stego signals. This issue is a potential weakness for traditional methods because the attacker also has access to the stego-signal and may be able to find the embedding channel.

To overcome the potential access of attacker to the embedding channel, Fridrich et al. [1] proposed the idea of wet paper codes. By using these codes, the receiver does not need to realize embedding channel (called dry area in wet paper context). As a result, there would be no need for an agreement on the embedding channel between the two parties. It has been shown in [1] that a message with average size equal to the size of dry area can be embedded in the cover signal with efficiency of 2 (one change per each pair of embedded bits). While wet paper steganography enables the transmitter to select the embedding channel on a pseudorandom basis or completely random, this selection is commonly based on some information which is available only to the sender.

Another goal in steganography is to embed a particular message by making minimal change to the cover signal. This is because any change to the cover signal may make it more unnatural and consequently more vulnerable to steganalysis. Authors in [2] proposed some efficient code families to be used in wet paper coding. Zhang et al. proposed [3] a two layer scheme, called paper folding, which combines pairs of bits and forms a second layer; then tried to embed message in these two layers. Filler proposed a similar scheme in [4] by combining ZZW idea [7] and wet paper. Zhang et al. [5] generalized paper folding to an N-page construction and reached an equivalent scheme. Authors in [6] extended previous methods and proposed a multi-layer construction which embeds message in a layer by layer manner using the wet paper codes. This method reaches higher embedding efficiency and brings more flexibility for choosing the embedding payload. They showed that wet ZZW and paper folding are special cases of this multi-layer construction. In this paper we generalize previous ideas and propose a multi-layer scheme which has superior efficiency in some cases and even more flexibility in embedding payload, especially in higher payload conditions.

The remaining of this paper is organized as follows: the proposed method is described in section II. In section III the performance of this scheme is investigated. The paper comes to an end with a conclusion in section IV.

II. THE PROPOSED METHOD

A. Definitions

Suppose that we have a cover signal with a wet rate equal to \( r \). The cover is divided into \( N \) blocks of length \( 3^L \): \( x_d(1), ..., x_d(3^L) \). These bits form the 0-layer. Using some equations we form upper layers (\( y_d(m,k) \) is node number \( k \) in \( m \)-th layer of block \( n \)):

\[
\begin{align*}
y_d(1,k) &= x_d(3k-2) \oplus x_d(3k-1) \oplus x_d(3k) \quad k = 1, 2, ..., 2^{L-1} \\
y_d(m,k) &= y_d(m-1,3k-2) \oplus y_d(m-1,3k-1) \oplus y_d(m-1,3k) \\
m &= 2, 3, ..., L; \quad k = 1, 2, ..., 2^{L-m}
\end{align*}
\] (1) (2)

As in [6], we call the node in the left of these equations (the node in upper layer), father and the nodes in the right (the nodes in the lower layer) brothers. We call these brothers a family. Nodes in the 0-layer are called leaf nodes. Degree of a
father is defined as sum of its children’s degrees. Dry leaf nodes have degree 1 and wet leaf nodes have degree 0.

To make the proposed construction more clear, a simple illustration is presented in Fig.1. It shows the construction for parameters: \( L=2 \) and \( N=1 \). Dark nodes are wet. Note that \( y_1(1) \) is wet because all its child nodes in the lower layer are wet and not allowed to change.

![Figure 1: A simple illustration of suggested multi-layer construction. Three bits are combined using eXclusive-OR to form a bit in upper layer.](image)

Using binomial distribution, the probability of a node in \( m \)th-layer having degree \( n \) is:

\[
P(m,u)=\binom{3^m}{u} (1-x)^{3^m-u} \quad m=0,\ldots,L; \quad u=0,\ldots,3^m \quad (3)
\]

**B. Embedding Scheme**

In the proposed method we perform embedding in a layer-by-layer manner. First we form a vector of size \( N \), composed of top nodes (\( L \)th-layer) in each block. If one of these nodes has a degree of 0 then it is considered wet; otherwise it will be a dry bit because we can change it by flipping one of dry leaf nodes in that block. Message bits are embedded in these bits using wet paper method in [1]. Using the notation in [6], probability of a node in the \( L \)th-layer with degree \( u \) to be flipped is denoted by \( P(L,u) \) and probability of such a node to be kept is denoted by \( P^c(L,u) \). We have:

\[
P^c(L,u=0)=0 \quad (4)
\]

\[
P^c(L,u>0)=\frac{P(L,u)}{2} \quad (5)
\]

\[
B_L=N\lfloor 1-P(L,0) \rfloor - N\lfloor (1-x^m) \rfloor \quad (7)
\]

Now, we suppose that embedding in the upper layer is done and explain how embedding is performed in the middle layers. For these layers we form a vector composed of first and second brothers from left in each family and perform wet paper embedding; then it is necessary to determine which of these bits are wet and which ones are dry. Four cases arise:

**Case 1:** Father node is wet. In this case brothers are wet and as a consequence they are not changeable.

**Case 2:** Father node is dry and has a degree more than \( T_2 \) and \( T_1 \) (\( T_2<T_1 \)). Here we have some subcases which are shown in Table 1. Note that in subcases 6 and 7 before embedding, we might need to flip first and second brothers from left respectively. In subcase 1, we flip one of dry brothers at random. This is to get compatible with father node.

![Table 1: Subcases of case 2](image)

**Case 3:** Father node is dry and has a degree less than \( T_1 \). Here we do the same as in case 2, except in subcases 2 and 3, that if father node is kept we consider both left brothers wet and we will not be able to embed bits in them.

**Case 4:** Father node is dry and has a degree less than \( T_2 \). Here we do the same as in case 2, except in subcase 4, that if father is kept we consider both left brothers wet and we will not be able to embed bits in them.

It is to be noted that cases 3 and 4 may occur simultaneously. After determining wet and dry nodes, we perform embedding using the method introduced in [1]. In this method, a payload equal to the number of dry bits is embedded and on average a half of these dry bits is flipped. Then we might need to flip the right brother to match with the father node. This node is not used during embedding and changing its value does not disturb the embedding process. Besides, parameters \( T_1 \) and \( T_2 \) enable us to choose the relative payload to be more flexible.

**C. Extracting data**

The extraction procedure is straightforward. Receiver first establishes the pyramid and then collects top node bits in each block to form a vector. Then, using WPC decoder proposed in [2], extracts data. Next, for lower layer, nodes with indexes not dividable by 3 are collected and data are extracted using the WPC decoder. Then, extracted data from (\( L+1 \) layers) are concatenated.

**III. PERFORMANCE ANALYSIS**

**A. Formulas for \( e \) and \( \alpha \)**

Information hiding schemes are evaluated based on their embedding efficiency (\( e \)), the average change in cover signals per each bit of the message embedded, and their relative payload (\( \alpha \)) which is the ratio of the embedded message size to
the size of the dry areas in the cover signal. An upper bound for the embedding efficiency could be shown as [2]:

\[ e \leq \frac{\alpha}{H^{-1}(\alpha)} \]  

(8)

This formula introduces an upper bound for the embedding efficiency versus the relative payload. In (8), \( \alpha \) is the relative payload and \( H^{-1} \) is the inverse of binary entropy function for \( p < \frac{1}{2} \).

Here, we calculate these two important indexes (\( e \) and \( \alpha \)) for the proposed scheme. The embedded payload in \( m \)-th-layer \((m < L)\) is found using:

\[ B_m = \sum_{k_1=1}^{2^m} \sum_{k_2=1}^{2^m} \sum_{k_3=1}^{2^m} P(m, k_1)P(m, k_2)P(m, k_3) \ast \pi_p(k_1, k_2, k_3) \]  

(9)

The function \( \pi \) is 0 for case 1 and subcases 1, 5, 6 and 7 of case 2. For the remaining subcases it is defined in Table II.

**TABLE II - DEFINITION OF FUNCTION \( \pi_p \) IN SUBCASES 2, 3 AND 4**

<table>
<thead>
<tr>
<th>Sub-case</th>
<th>Condition</th>
<th>( \pi(k_1, k_2, k_3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 and 3</td>
<td>( k_1 + k_2 + k_3 &gt; T_1 )</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>( k_1 + k_2 + k_3 \leq T_1 )</td>
<td>( \frac{P_p(m + 1, k_1 + k_2 + k_3)}{P(m + 1, k_1 + k_2 + k_3)} )</td>
</tr>
<tr>
<td>4</td>
<td>( k_1 + k_2 + k_3 &gt; T_2 )</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>( k_1 + k_2 + k_3 \leq T_2 )</td>
<td>( \frac{P_p(m + 1, k_1 + k_2 + k_3)}{P(m + 1, k_1 + k_2 + k_3)} )</td>
</tr>
</tbody>
</table>

Now we try to define function \( P_p(m, k) \). Clearly a node with degree 0 (a wet node) will never change so we have \( P_p(m, 0) = 0 \). Also, this function is defined in (5) for \( L \)-th-layer. For other layer it is easily shown that:

\[ P_p(m, k) = P(m, k) \sum_{k_1=0}^{2^m} \sum_{k_3=0}^{2^m} P(m, k_1)P(m, k_2)P(m, k_3) \pi_p(k_1, k_2, k_3) \]  

(10)

The function \( \pi_p \) is defined as in Table III. We investigate the state of two brothers of the node: When none of brothers are dry, the node will change if its father has changed. In case that both brothers are dry and father is rich (has a degree more than \( T_2 \)) the node changes in a half of times. And if its father is poor, it will change a half of times only if its father has changed. If one of brothers is dry and one is wet, we have to average the flip probability for different positions of the node in the block: right, middle or left. This is done and the result is shown in Table 2.

After all, \( \alpha \) and \( e \) are calculated as follows:

\[ \alpha = \frac{\sum_{m=0}^{2^m} B_m}{[N.3^k.(1-t)]} \]  

(11)

\[ e = \frac{\sum_{m=0}^{2^m} B_m}{[N.3^k.P_f(0,3)]} \]  

(12)

The denominator of (11) is the number of dry bits in the cover and the denominator of (12) is the average wet leaf nodes flipped during embedding.

**TABLE III - DEFINITION OF FUNCTION \( \pi_p \) FOR POSITIVE K**

<table>
<thead>
<tr>
<th>Condition</th>
<th>( \pi_p(k_1, k_2, k_3) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k_2 = k_3 = 0 )</td>
<td>( \frac{P_p(m + 1, k)}{P(m + 1, k)} )</td>
</tr>
<tr>
<td>( k_2, k_3 \neq 0 )</td>
<td>( \frac{1}{2} )</td>
</tr>
<tr>
<td>( k_2 &gt; 0 )</td>
<td>1. ( k_2 &gt; 0 ) ( k_2 &gt; T_1 )</td>
</tr>
<tr>
<td></td>
<td>1 ( P_p(m + 1, k + k_2) )</td>
</tr>
<tr>
<td></td>
<td>( \frac{1}{6} ) ( P_p(m + 1, k + k_2) )</td>
</tr>
<tr>
<td></td>
<td>( \frac{1}{6} ) ( P_p(m + 1, k + k_2) )</td>
</tr>
<tr>
<td>( k_3 = 0 )</td>
<td>( \frac{1}{2} )</td>
</tr>
<tr>
<td>( k_2 = 0 )</td>
<td>2. ( k_2 = 0 ) ( k + k_2 \leq T_2 )</td>
</tr>
<tr>
<td></td>
<td>( \frac{1}{2} ) ( P_p(m + 1, k + k_2) )</td>
</tr>
<tr>
<td></td>
<td>( \frac{1}{2} ) ( P_p(m + 1, k + k_2) )</td>
</tr>
<tr>
<td>( k_3 &gt; 0 )</td>
<td>( \frac{1}{2} )</td>
</tr>
<tr>
<td></td>
<td>( \frac{1}{2} ) ( P_p(m + 1, k + k_3) )</td>
</tr>
<tr>
<td></td>
<td>( \frac{1}{2} ) ( P_p(m + 1, k + k_3) )</td>
</tr>
</tbody>
</table>

1, 2: For these conditions we first obtain flip probability for each of 3 brothers and then average them.

**B. Results**

Now we compare performance of the proposed scheme with the performance of the method given in [6] (this method was shown to be superior to other methods such as wet ZZW [4] and paper folding [5]) Fig. 2 shows results for three different wet rates. It is clearly observed that, the proposed method is more flexible for choosing relative payload and in some cases it has a slightly improved performance, as compared to the method in [6]. Red crosses are much denser that black dots. This is mainly because in the proposed scheme one can control two parameters, \( T_1 \) and \( T_2 \), rather than just one parameter in [6]. Moreover, the embedding complexity is similar to the scheme in [6].

**IV. CONCLUSION**

In this paper a new embedding scheme has been proposed which generalizes the previous methods. First a pyramid of bits is established which a node is a combination of 3 bits in lower layer manner using wet paper codes in each layer. Two parameters, \( T_1 \) and \( T_2 \), have been introduced which make the selection of (\( e, \alpha \)) pair much more flexible. Moreover, it has been shown that the proposed method is a bit more efficient especially in lower payloads. This generalization could be extended to groups of 4, 5 and more bits, bringing more flexibility and also a tiny improvement to the embedding efficiency. Future approaches include using these multi-layer constructions in ternary bases (instead of bits) and also using heuristic combination of bits to form layers. The state-of-the-
art results for the embedding efficiency for payloads less than 1 are far from theoretical bound yet.

Figure 2: Performance of the proposed scheme and scheme in [6] for covers with different wet rates: (a) \( r=0.2 \), (b) \( r=0.5 \), (c) \( r=0.8 \)

REFERENCES