Generalization and Analysis of the Paper Folding Method for Steganography

Weiming Zhang, Jiufen Liu, Xin Wang, and Nenghai Yu

***Abstract*—Wet paper codes (WPCs) are designed for steganography, in which the sender and recipient do not need to share the changeable positions. In this paper, we propose the N-page construction for wet paper coding, which can generate a family of WPCs following the upper bound on embedding efficiency from one single WPC. The Paper Folding method, one of our previous methods, is a special case of the N-page construction with $N = 2^k$. We deduce recursions for calculating embedding efficiency of N-page construction, and obtain explicit expression on embedding efficiency of 2^k-page construction. Furthermore, we derive the limit of distance between the embedding efficiency of 2^k-page construction and the upper bound of embedding efficiency as k tends to infinity. Based on the limit, we analyze how the embedding efficiency is influenced by the proportion of wet pixels (wet ratio) in the cover, showing that embedding efficiency only drops about 0.32 as the wet ratio increases to 0.9999.**

***Index Terms*—Embedding efficiency, Paper Folding method, relative payload, steganography, wet paper codes (WPCs), ZZW construction.**

I. Introduction

STEGANOGRAPHY is used to communicate messages under the cover of innocence signals such as digital images. For the security of steganography, messages are embedded into the cover by altering the least significant components of the cover. Therefore, the sender needs to select a channel that includes only insignificant parts of the cover before embedding messages. However, if the rules for determining the selection channel are public, the attacker can use this information to detect the existence of the covert communication. To solve this problem, Fridrich *et al.* [1]–[3] proposed wet paper codes (WPCs), which enable the sender to determine the selection channel freely, and the recipient to extract the embedded messages without any knowledge about the selection channel. WPCs have been used in various branches of information hiding [3]–[5]. For the security in steganographic applications, an important problem about WPC is how to restrain the modification of the cover, or in other words, how to improve the embedding efficiency, which is defined as the average number of bits embedded per unit modification.

In fact, WPC is a model of embedding messages into a cover with defective cells. Taking the image as an example, we denote changeable pixels by dry positions and defective pixels by wet positions. The wet paper model is a generalization of the dry paper model that is for embedding messages into covers without defective pixels. For the dry paper model, many coding methods have been designed to improve the embedding efficiency, such as codes in [6]–[14]. Recent advance shows that any code can generate a family of codes by the ZZW embedding construction [15], which is proved to follow the theoretic upper bound on embedding efficiency [16], [17]. The authors also generalized the ZZW construction to the wet paper model, which was called the Paper Folding method [18]. A similar generalization was developed independently by Filler *et al.* [19], called Wet ZZW construction, which can yield a larger code family than the Paper Folding method. In [19], WPCs with small overhead are designed, which are important for the ZZW construction.

In terms of embedding efficiency, methods described in [18] and [19] outperform previous WPCs [9], [20], [21]. However, no explicit formula is deduced to calculate the embedding efficiency for methods in [18] and [19]. For the Paper Folding method, embedding efficiency is expressed by recursions [18], and for Wet ZZW construction, embedding efficiency is estimated by combining analytic and experimental results [19]. Therefore, it is still hard to analyze the properties of ZZW construction for the wet paper model as for the dry paper model in [16] and [17]. For instance, the experimental results in [18] and [19] show that the embedding efficiency will decrease when the proportion of wet pixels (wet ratio γ) increases. But we cannot answer how the wet ratio γ will influence the embedding efficiency as $\gamma \to 1$.

To analyze the ZZW construction for the wet paper model, in this paper, we propose the N-page construction, which yields the same code family as the Wet ZZW construction [19] and becomes the Paper Folding method [18] when $N = 2^k$. By using the new construction, we pay our attention to analyzing the embedding efficiency. In fact, the N-page construction helps us deduce recursions for calculating the embedding efficiency and an explicit expression for the embedding efficiency of 2^k-page construction. Based on this expression, we derive the limit of distance between the embedding efficiency of 2^k-page construction and the upper bound on embedding efficiency as $k \to \infty$, which extends the limit theorem [16] on ZZW construction from the dry paper model to the wet paper model. By this limit result,

Manuscript received January 27, 2010; revised July 08, 2010; accepted August 01, 2010. Date of publication August 12, 2010; date of current version November 17, 2010. This work was supported by the Natural Science Foundation of China (60803155). The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Fernando Perez-Gonzalez.

W. Zhang and N. Yu are with the School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China (e-mail: zwmshu@gmail.com; ynh@ustc.edu.cn).

J. Liu and X. Wang are with the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, China (e-mail: jiufenliu@163.com; wangxinwsj@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2010.2065804

we analyze how the embedding efficiency drops when wet ratio $\gamma \to 1$.

The rest of this paper is organized as follows. Section II introduces the model of WPCs. The N-page construction is described in Section III, and the formula for calculating the embedding efficiency of N-page construction is deduced in Section IV. The asymptotic behavior of 2^k-construction is analyzed in Section V, and the paper is concluded in Section VI.

II. Model of WPCs

We denote matrices and vectors by boldface font, and consider only binary WPCs, which means the cover is a binary sequence, e.g., the least significant bits (LSBs) of a gray-scale image. Assume that a block of cover consists of n bits such as $\mathbf{x} = (x_1, \ldots, x_n)$. First the sender determines a selection channel with l changeable bits x_j, $j \in J \subset \{1, 2, \ldots, n\}$, $|J| = l$. The selection channel J is not known to the recipient. The sender will embed a secret message $\mathbf{m} = (m_1, \ldots, m_m)$ into $\mathbf{x}$ by only modifying some bits in the selection channel. Because the message is usually encrypted before being embedded, we assume that the message is a binary pseudorandom sequence.

In the terms of WPCs, we claim that the bits in the selection channel are dry and the other bits are wet; define the wet ratio as $\gamma = (n - l)/n$, and dry ratio as $1 - \gamma$. If a WPC can embed m bits of messages into an n-length cover with wet ratio γ by R_a changes to the cover on average, we say the code has relative payload $\alpha = m/l = m/(1 - \gamma)n$, change rate $c = R_a/l = R_a/(1 - \gamma)n$, and the code is denoted by WPC(α, c). Define embedding efficiency as $e = m/R_a = \alpha/c$. It has been proved [20] that the embedding efficiency is bounded from above by

$$e(c) \le \frac{H_2(c)}{c} \tag{1}$$

where $H_2(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$ is the binary entropy function.

WPCs can be constructed from random linear codes [1], [2], in which, to embed $\mathbf{m}$ into $\mathbf{x}$, the sender changes some bits in the selection channel, i.e., some x_j, $j \in J$, to get the stego-object $\mathbf{y} = (y_1, \ldots, y_n)$, satisfying

$$\mathbf{D}\mathbf{y}^T = \mathbf{m}^T \tag{2}$$

where $\mathbf{D}$ is an $m \times n$ binary pseudorandom matrix. $\mathbf{D}$ is usually generated from the stego key shared with the recipient. Therefore, if the recipient knows the message length m, he/she can generate the same matrix $\mathbf{D}$ by using the shared key and extract the message $\mathbf{m}$ by calculating $\mathbf{D}\mathbf{y}^T$ without any knowledge about the selection channel J.

To solve (2), the sender can first delete the variables y_j for $j \notin J$ and these corresponding columns in $\mathbf{D}$ to get a new system of m equations and l variables with a $m \times l$ coefficients matrix $\mathbf{H}$. If $\mathbf{H}$ has full rank, the sender can find $\mathbf{y}$ by Gaussian elimination with cubic complexity. To assure that $\mathbf{H}$ is of full rank with high probability, the sender should let $m < l$, which means an overhead of $l - m$ bits.

In the ZZW construction [15], the WPC approaching maximum relative payload 1 is needed, which requires a very small overhead. The WPCs based on Gaussian elimination [1] have small overhead. However, because of the high complexity of Gaussian elimination, the sender has to divide the cover and the message into small segments and communicate the length of the message for every block, which will also cause capacity loss and make the implementation complex. The alternative method of WPCs for large relative payload is based on the LT process [2], which imposes the column weights of $\mathbf{D}$ to follow the distribution as in LT codes and thus achieves the log-linear complexity. WPCs implemented via the LT process can embed long messages at once, which need a negligible overhead as long as the cover is long enough. In practice, the overhead of LT codes converges to 0 as $l = 10^6$, but a larger overhead is needed for medium range codes. For example, the overhead is about 6% for $l = 10^4$. By incorporating Gaussian elimination and the LT process, a method with a small overhead for medium length of covers was proposed by Filler *et al.* [19], who used a matrix with the following form:

$$\mathbf{D} = \begin{pmatrix} \mathbf{W}_1 \\ \mathbf{W}_2 \\ \mathbf{W}_3 \end{pmatrix} \tag{3}$$

where $\mathbf{W}_2 \in \{0, 1\}^{m_1 \times n}$ is a random sparse LT matrix, and $\mathbf{W}_1 \in \{0, 1\}^{h \times n}$, $\mathbf{W}_3 \in \{0, 1\}^{m_2 \times n}$ are random binary matrices. Herein, h is a shared parameter. By $\mathbf{W}_1\mathbf{y}^T$, h bits can be embedded to communicate the coded m_1 and m_2, which will be used to form $\mathbf{W}_2$ and $\mathbf{W}_3$ by the recipient. The main payload is embedded with $\mathbf{W}_2\mathbf{y}^T$ by the LT process. The random rows of $\mathbf{W}_3$ are added "on the fly" while implementing Gaussian elimination on $\mathbf{D}$, which are used to reduce the overhead from the LT code. This method has a $\mathcal{O}(m_2^2 l)$ complexity and an overhead less than 2 bits on average. Because h bits are used for communicating the length of the message, the total overhead is $h + 2$ bits.

The methods in [2] and [19] can approach maximum relative payload 1 with change rate 0.5, i.e., yield the WPC(1, 0.5) with an embedding efficiency of 2. Note that, at the relative payload 1, the upper bound on embedding efficiency is just 2. However, for the security of steganography, we usually need WPCs with smaller relative payloads and higher embedding efficiency. Next, we will propose a method that can achieve high embedding efficiency for various relative payloads.

III. N-Page Construction

A. Two-Page Construction

We first introduce the basic method, two-page construction (TPC), which divides the original cover into two disjoint blocks. Without loss of generality, assume the original cover consists of $2n$ bits, and is divided into $\mathbf{x}_1^2 = (x_{1,1}^2, x_{1,2}^2, \cdots, x_{1,n}^2)$ and $\mathbf{x}_2^2 = (x_{2,1}^2, x_{2,2}^2, \cdots, x_{2,n}^2)$. The embedding process includes two steps, and the superscript "2" in the original cover indicates that these blocks will be used in the second step. The first step is the outer coding by a WPC(α, c) and the second step is the inner coding by a WPC(1, 0.5).

The Outer Coding: First, as shown in Fig. 1, fold $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ to get a new "wet paper" $\mathbf{x}_1^1$ with exclusive-or operation, such that $\mathbf{x}_1^1 = (x_{1,1}^1, x_{1,2}^1, \cdots, x_{1,n}^1)$ and $x_{1,i}^1 = x_{1,i}^2 \oplus x_{2,i}^2$, $1 \le i \le n$. Obviously, as long as there is one bit in $(x_{1,i}^2, x_{2,i}^2)$ changeable, the $x_{1,i}^1$ can be changed, i.e., $x_{1,i}^1$ is dry. Therefore, we define

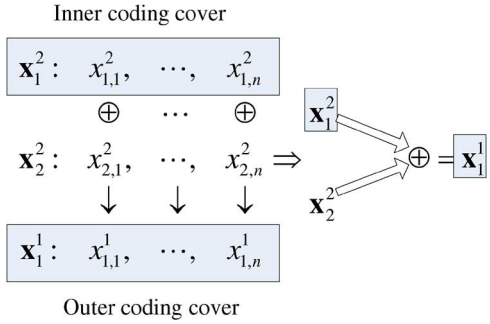

Fig. 1. Illustration of the TPC. The coding channels are labeled by shadows.

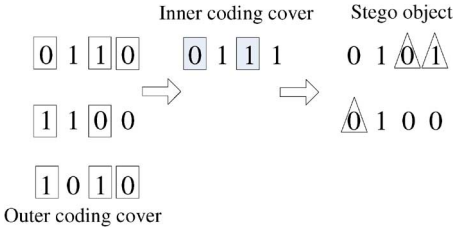

Fig. 2. Example of the TPC. The dry elements in the original cover and the outer coding cover are labeled by squares and the dry elements in the inner coding cover are labeled by shadows. Note that the inner coding cover will be changed to (0,1,1,1) after the outer coding. The modified bits are labeled by triangles in the stego object.

that $x^1_{1,i}$ is wet if and only if both $x^2_{1,i}$ and $x^2_{2,i}$ are wet. Thus we get the outer coding cover $\mathbf{x}^1_1$, into which we embed the first message $\mathbf{m}_1$ by a WPC(α, c).

The Inner Coding: After the outer coding, we use $\mathbf{x}^2_1$ to construct an inner coding cover by redefining dry/wet elements as follows: $x^2_{1,i}$ is defined as a dry bit if and only if both $x^2_{1,i}$ and $x^2_{2,i}$ are dry in the original cover and $x^1_{1,i}$ needs to be changed in the outer coding. In fact, if $x^1_{1,i}$ needs to be changed in the outer coding, there are two cases. Case I is that there is only one bit in $(x^2_{1,i}, x^2_{2,i})$ dry, and we have to flip this dry bit to modify $x^1_{1,i}$. Case II is that both $x^2_{1,i}$ and $x^2_{2,i}$ are dry. In Case II, we label the "i" as a dry position for the inner coding cover and which bit in $(x^2_{1,i}, x^2_{2,i})$ should be modified will be determined by the inner coding. After defining the inner coding cover, we embed the second message $\mathbf{m}_2$ into it by using a WPC with the maximum relative payload, i.e., WPC(1, 0.5). For any dry position "i" in the inner coding cover, if $x^2_{1,i}$ does not equal the needed value, we flip $x^2_{1,i}$; otherwise, we flip $x^2_{2,i}$, which will simultaneously finish the change needed by the outer coding. After the inner coding, we get the stego object and send it to the recipient.

To extract the messages, the recipient first divides the stego object into two blocks of length n, and folds them to obtain the outer coding channel. By applying WPC(α, c) and WPC(1, 0.5) to the outer coding channel and the inner coding channel, the recipient can extract the message $\mathbf{m}_1$ and $\mathbf{m}_2$, respectively.

Example: An example of the TPC is shown in Fig. 2, in which the block length $n = 4$ and the original cover $\mathbf{x}^2_1 = (0, 1, 1, 0)$, $\mathbf{x}^2_2 = (1, 1, 0, 0)$. By folding the two blocks, we get the outer coding cover $\mathbf{x}^1_1 = (1, 0, 1, 0)$. The dry elements in the original cover and the outer coding cover are labeled by squares in Fig. 2. Assume the message to be embedded into the outer coding cover is $\mathbf{m}_1 = (0, 1, 1)$, and the coefficient matrix generated from the shared key for the WPC in this step[1] is

$$\mathbf{D}_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \tag{4}$$

To make $\mathbf{D}_1 \mathbf{x}^{1T}_1 = \mathbf{m}^T_1$, the outer coding cover should be changed to (0, 0, 0, 1) that means all the three dry bits in the outer coding cover need to be modified. Note that in the fourth pair $(x^2_{1,4}, x^2_{2,4})$, only $x^2_{1,4}$ is dry, and thus we must flip $x^2_{1,4}$ to modify the fourth bit in the outer coding cover, while the other two modifications in positions "1" and "3" will be done in the inner coding because both bits in the corresponding pairs are dry. Therefore, we obtain the inner coding cover (0, 1, 1, 1) with two dry elements in positions "1" and "3", which is still denoted by $\mathbf{x}^2_1$ for simplicity. Assume the message to be embedded into the inner coding cover is $\mathbf{m}_2 = (0, 0)$, and the random matrix generated for the WPC in this step is

$$\mathbf{D}_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}. \tag{5}$$

To make $\mathbf{D}_2 \mathbf{x}^{2T}_1 = \mathbf{m}^T_2$, $x^2_{1,3}$ should be modified, and thus we flip $x^2_{1,3}$. For the other dry position "1", $x^2_{1,1}$ does not need to be changed, and thus we should flip $x^2_{2,1}$ to finish the modification in the outer coding. In Fig. 2, the modified bits are labeled by triangles in the stego object.

After receiving the stego object, the recipient divides it into two blocks, and folds them to get the outer coding channel (0, 0, 0, 1). The inner coding channel is just the first block (0, 1, 0, 1). Generating the random matrices $\mathbf{D}_1$ and $\mathbf{D}_2$ from the shared key and multiplying by the two coding channels, respectively, the recipient can extract the messages $\mathbf{m}_1$ and $\mathbf{m}_2$.

In this example, we embed 5 bits of messages with three changes. Note that the number of changes is determined by the outer coding. The inner coding of TPC does not increase the number of changes, in which we embed the extra message $\mathbf{m}_2$ with some changes introduced by the outer coding.

B. N-Page Construction

By iteratively using TPC, we propose the following N-page construction, which can be implemented by k steps, where $k = \lceil \log_2 N \rceil + 1$. Without loss of generality, assume that the binary wet paper cover $\mathbf{x}$ can be divided into N disjoint blocks of length n, such that $\mathbf{x}^k_j = (x^k_{j,1}, x^k_{j,2}, \ldots, x^k_{j,n})$, $1 \le j \le N$. Herein, the superscript "k" in $\mathbf{x}^k_j$ indicates that these blocks will be used in the kth step.

The following N-page construction consists of one outer coding by a WPC(α, c) and $k-1$ steps of inner coding by $k-1$ WPCs with maximum relative payload. We take five-page construction as example to describe the embedding and extraction procedures. Because the embedding procedure of five-page construction includes four steps, we denote the original cover

[1]Note that the cover in the example is very short, on which it is hard to do wet paper coding. Herein, two artificial WPCs without overhead are used to show the embedding process of TPC.

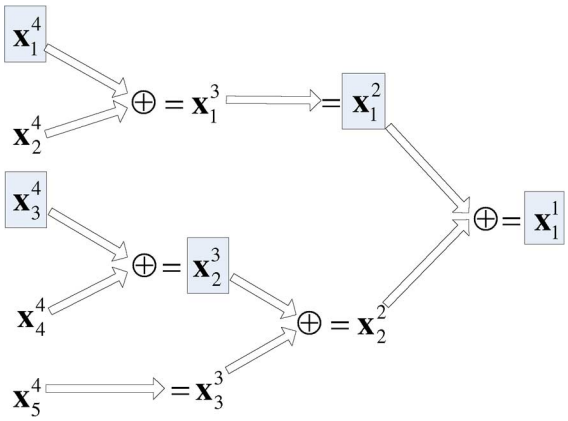

Fig. 3. Illustration of the five-page construction.

blocks by $\mathbf{x}_1^4$, $\mathbf{x}_2^4$, $\mathbf{x}_3^4$, $\mathbf{x}_4^4$, and $\mathbf{x}_5^4$, which are first folded by exclusive-or operation, as shown in Fig. 3.

First, do outer coding in $\mathbf{x}_1^1$, which will determine the change positions in $\mathbf{x}_1^1$, and the inner coding cover on $\mathbf{x}_1^2$. Second, embed messages into $\mathbf{x}_1^2$ with inner coding, which will determine the change positions in $\mathbf{x}_1^2$ ($\mathbf{x}_1^3$) and $\mathbf{x}_2^2$. By the change positions in $\mathbf{x}_2^2$, we define the inner coding cover on $\mathbf{x}_2^3$. Third, embed messages into $\mathbf{x}_2^3$, which will determine the change positions in $\mathbf{x}_2^3$ and $\mathbf{x}_3^3$ ($\mathbf{x}_5^4$). Because the change positions in both $\mathbf{x}_1^3$ and $\mathbf{x}_2^3$ have been fixed, we can define inner coding covers on $\mathbf{x}_1^4$ and $\mathbf{x}_3^4$. Fourth, we embed messages into $\mathbf{x}_1^4$ and $\mathbf{x}_3^4$ by inner coding, which will fix on the change positions in $\mathbf{x}_1^4$, $\mathbf{x}_2^4$, $\mathbf{x}_3^4$, and $\mathbf{x}_4^4$. In fact, we can cascade $\mathbf{x}_1^4$ and $\mathbf{x}_3^4$ to embed messages in this step. After the fourth step, we obtain the change positions in $\mathbf{x}_j^4$, $1 \le j \le 5$, and actual changes are made on them, which simultaneously completes the changes needed in all steps and yields the stego object.

Denote the WPCs used in the above four steps by WPC_1, WPC_2, WPC_3, and WPC_4, which are constructed from a shared key. After receiving the stego object, the recipient folds the stego object as the same form as shown in Fig. 3 and then generates the four WPCs from the shared key to extract messages in the four coding channels as labeled by shadows in Fig. 3. The extraction process on the four coding channels can be executed in parallel.

Generally, for the N-page construction, the inner coding in the jth step ($j = 2, \ldots, k+1$) only embeds extra messages with some modifications introduced by the $(j-1)$th step. By inheriting the merit of TPC, the inner coding of the N-page construction does not increase the number of changes. Therefore, to sufficiently utilize the dry bits in the inner coding cover, we should apply the WPC with the maximum relative payload, i.e., WPC(1, 0.5), to the inner coding. For the outer coding, we can use a WPC(α, c) for $\alpha \le 1$, which determines the number of changes. The analysis in Section IV will show that the embedding efficiency of WPC(α, c) will essentially influence the embedding efficiency of the N-page construction, and with a given relative payload α, we hope that the embedding efficiency of WPC(α, c) is as high as possible. In other words, with a given α, the change rate of the WPC used in the outer coding is desired to be as small as possible.

IV. Performance Analysis of N-Page Construction

A. Two-Page Construction

To analyze the N-page construction, we first consider the TPC. In TPC, the original cover consists of two disjoint blocks of length n, such that $\mathbf{x}_1^2 = (x_{1,1}^2, x_{1,2}^2, \cdots, x_{1,n}^2)$ and $\mathbf{x}_2^2 = (x_{2,1}^2, x_{2,2}^2, \cdots, x_{2,n}^2)$. Assume the wet ratios of the two blocks are γ_1 and γ_2, respectively, and the first block is independent of the second one. We embed messages in the outer coding by a WPC(α, c) and in the inner coding by a WPC(1, 0.5).

As described in Section III-A, in the outer coding cover $\mathbf{x}_1^1$, an element $x_{1,i}^1$ $(1 \le i \le n)$ is defined to be wet if and only if both $x_{1,i}^2$ and $x_{2,i}^2$ are wet. Therefore, the wet ratio of the outer coding cover is $\gamma_1\gamma_2$ and the dry ratio is $1 - \gamma_1\gamma_2$. Applying the WPC(α, c) to the outer coding cover, we can embed $n(1 - \gamma_1\gamma_2)\alpha$ bits of messages with on average $n(1-\gamma_1\gamma_2)c$ changes.

In the inner coding cover, $x_{1,i}^2$ $(1 \le i \le n)$ is defined as a dry element if and only if both $x_{1,i}^2$ and $x_{2,i}^2$ are dry in the original cover and $x_{1,i}^1$ needs to be changed in the outer coding. The probability is $(1-\gamma_1)(1-\gamma_2)$ for both $x_{1,i}^2$ and $x_{2,i}^2$ being dry, and the corresponding $x_{1,i}^1$ needs to be changed by WPC(α, c) with the probability c, so the dry ratio of the inner coding cover is $(1-\gamma_1)(1-\gamma_2)c$. Thus, we can embed on average $n(1 - \gamma_1)(1 - \gamma_2)c$ bits of messages into the inner coding cover by using WPC(1, 0.5).

Consequently, the length of messages embedded by the outer coding is

$$n(1 - \gamma_1\gamma_2)\alpha. \tag{6}$$

The inner coding embeds $n(1-\gamma_1)(1-\gamma_2)c$ bits. Define

$$E(\gamma_1, \gamma_2, c) = (1-\gamma_1)(1-\gamma_2)c \tag{7}$$

and then the length of the message embedded in the inner coding cover is

$$nE(\gamma_1, \gamma_2, c) = n(1-\gamma_1)(1-\gamma_2)c. \tag{8}$$

Because the total number of dry bits in the original cover is $n(1-\gamma_1) + n(1-\gamma_2)$, the relative payload of TPC is

$$\frac{n(1-\gamma_1\gamma_2)\alpha + nE(\gamma_1, \gamma_2, c)}{n(1-\gamma_1)+n(1-\gamma_2)} = \frac{(1-\gamma_1\gamma_2)\alpha + E(\gamma_1, \gamma_2, c)}{(1-\gamma_1)+(1-\gamma_2)}. \tag{9}$$

On the other hand, the average number of changes in TPC is

$$n(1 - \gamma_1\gamma_2)c \tag{10}$$

which is determined by the outer coding. Therefore, the change rate for this construction is

$$\frac{n(1-\gamma_1\gamma_2)c}{n(1-\gamma_1)+n(1-\gamma_2)} = \frac{(1-\gamma_1\gamma_2)c}{(1-\gamma_1)+(1-\gamma_2)}. \tag{11}$$

To analyze the "N-page construction," we also need to calculate the change rate in the two blocks, $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$, respectively. As mentioned in Section III-A, when $x_{1,i}^1$ needs to be changed in the outer coding, there are two cases. Case I is that only one bit in $(x_{1,i}^2, x_{2,i}^2)$ is dry, and we just flip this dry bit. Case II is that both $x_{1,i}^2$ and $x_{2,i}^2$ are dry. In Case II, $x_{1,i}^2$ and $x_{2,i}^2$ will be

changed with the equal probability 1/2 in the inner coding because the embedded message is a pseudorandom sequence and is independent of the cover. Note that the wet ratio of the first original cover block $\mathbf{x}_1^2$ is γ_1; thus, the change rate of it can be calculated by

$$\begin{aligned}&\frac{nc\left[P\left\{\text{Only } x_{1,i}^2 \text{ is dry}\right\}+\frac{1}{2}P\left\{\text{Both } x_{1,i}^2 \text{ and } x_{2,i}^2 \text{ are dry}\right\}\right]}{n(1-\gamma_1)}\\&=\frac{nc\left[(1-\gamma_1)\gamma_2+\frac{1}{2}(1-\gamma_1)(1-\gamma_2)\right]}{n(1-\gamma_1)}\\&=\frac{c(1+\gamma_2)}{2}\triangleq C(\gamma_2,c).\end{aligned}\tag{12}$$

Symmetrically, the change rate of $\mathbf{x}_2^2$ is equal to $C(\gamma_1,c)=c(1+\gamma_1)/2$.

B. Balanced Two-Page Construction

The following balanced two-page construction (BTPC) is a special case of the TPC for the wet ratio $\gamma_1=\gamma_2=\gamma$, which is the scenario in practice. Assume that the sender has a cover $\mathbf{x}$ with the wet ratio γ. To do TPC, he/she first randomly permutes the elements in $\mathbf{x}$ based on the shared key, and then divides it into two disjoint blocks of length n, such that $\mathbf{x}_1^2=(x_{1,1}^2,x_{1,2}^2,\cdots,x_{1,n}^2)$ and $\mathbf{x}_2^2=(x_{2,1}^2,x_{2,2}^2,\cdots,x_{2,n}^2)$. Thus, we can assume that each block keeps the same wet ratio γ because of the random permutation.

In this case, by (6) and (8), the outer coding embeds $n(1-\gamma^2)\alpha$ bits of messages, and the inner coding embeds $nE(\gamma,\gamma,c)$ bits of messages. For simplicity, we denote $E(\gamma,\gamma,c)$ by $E_2(\gamma,c)$ such that

$$E_2(\gamma,c)=E(\gamma,\gamma,c)=c(1-\gamma)^2.\tag{13}$$

Therefore, the length of messages embedded by BTPC is $n(1-\gamma^2)\alpha+nE_2(\gamma,c)$. With (10), the average number of changes is $n(1-\gamma^2)c$.

C. Three-Page Construction

In the three-page construction, we assume the cover consists of three disjoint blocks, $\mathbf{x}_1^3$, $\mathbf{x}_2^3$, and $\mathbf{x}_3^3$, with the same wet ratio γ, where

$$\mathbf{x}_j^3=\left(x_{j,1}^3,x_{j,2}^3,\cdots,x_{j,n}^3\right),\quad j=1,2,3.\tag{14}$$

The folding procedure is shown in Fig. 4. Because the wet ratio of $\mathbf{x}_j^3$ is γ, $1\le j\le 3$, the wet ratio of $\mathbf{x}_2^2$ is γ^2 and the wet ratio of $\mathbf{x}_1^1$ is γ^3.

First, by WPC(α,c), the outer coding embeds $n(1-\gamma^3)\alpha$ bits of messages into $\mathbf{x}_1^1$ with on average $n(1-\gamma^3)c$ changes. Second, by (8), the inner coding can embed $nE(\gamma,\gamma^2,c)=n(1-\gamma)(1-\gamma^2)c$ bits of messages into $\mathbf{x}_1^2$. Given (12), the change rate of $\mathbf{x}_2^2$ is $C(\gamma,c)$. Third, applying the inner coding of BTPC to $\mathbf{x}_2^3$, we can embed $nE_2(\gamma,C(\gamma,c))$ bits of messages by (13), because the change rate of $\mathbf{x}_2^2$ is $C(\gamma,c)$.

Consequently, the outer coding embeds $n(1-\gamma^3)\alpha$ bits of messages. The inner coding embeds in total $nE(\gamma,\gamma^2,c)+nE_2(\gamma,C(\gamma,c))$ bits of messages. Define

$$E_3(\gamma,c)=E(\gamma,\gamma^2,c)+E_2\left(\gamma,C(\gamma,c)\right).\tag{15}$$

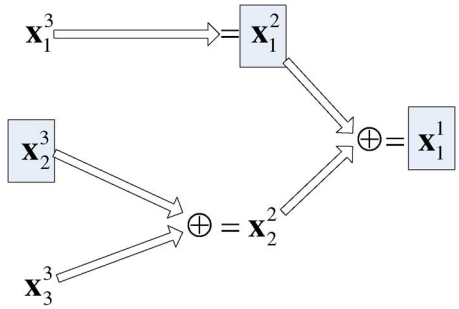

Fig. 4. Illustration of the three-page construction.

Thus, the three-page construction can on average embed $n(1-\gamma^3)\alpha+nE_3(\gamma,c)$ bits of messages with $n(1-\gamma^3)c$ changes.

D. N-Page Construction

Iteratively, we can get the performance of N-page construction for $N\ge 4$. Let $k=\lceil\log_2 N\rceil+1$. Assume that the original cover $\mathbf{x}$ has a wet ratio γ. After random permutation, $\mathbf{x}$ is divided into N disjoint blocks $\mathbf{x}_j^k$, $1\le j\le N$, such that

$$\mathbf{x}_j^k=\left(x_{j,1}^k,x_{j,2}^k,\cdots,x_{j,n}^k\right),\quad 1\le j\le N.\tag{16}$$

The random permutation makes every block keep the same wet ratio γ. Let $N_1=\lfloor N/2\rfloor$ and $N_2=\lfloor(N+1)/2\rfloor$, and thus $N=N_1+N_2$. We split the N blocks into two groups such that the first group consists of the first N_1 blocks $(\mathbf{x}_1^k,\mathbf{x}_2^k,\cdots,\mathbf{x}_{N_1}^k)$ and the second group consists of the last N_2 blocks $(\mathbf{x}_{N_1+1}^k,\mathbf{x}_{N_1+2}^k,\cdots,\mathbf{x}_{N_1+N_2}^k)$. Compress the two groups with exclusive-or operation such that

$$\mathbf{y}_1=\bigoplus_{j=1}^{N_1}\mathbf{x}_j^k,\quad \mathbf{y}_2=\bigoplus_{j=1}^{N_2}\mathbf{x}_{N_1+j}^k.\tag{17}$$

Therefore, $\mathbf{y}_\mu$ has wet ratio γ^{N_μ}, $\mu=1,2$. Compress $\mathbf{y}_1$ and $\mathbf{y}_2$ such that

$$\mathbf{z}=\mathbf{y}_1\oplus\mathbf{y}_2.\tag{18}$$

The wet ratio of $\mathbf{z}$ is $\gamma^{N_1+N_2}=\gamma^N$.

First, employ TPC to $\mathbf{y}_1$ and $\mathbf{y}_2$. The outer coding can embed $n(1-\gamma^N)\alpha$ bits of messages with on average $n(1-\gamma^N)c$ changes by a WPC(α,c). By (8), the inner coding can embed $nE(\gamma^{N_1},\gamma^{N_2},c)$ bits of messages into $\mathbf{y}_1$. By (12), the change rate of $\mathbf{y}_1$ is equal to $C(\gamma^{N_2},c)$ and the change rate of $\mathbf{y}_2$ is equal to $C(\gamma^{N_1},c)$.

Second, apply the inner coding of N_μ-page construction to the μth group, $\mu=1,2$. For the first group, because the change rate of $\mathbf{y}_1$ is $C(\gamma^{N_2},c)$, the length of embedded messages is $nE_{N_1}(\gamma,C(\gamma^{N_2},c))$. For the second group, because the change rate of $\mathbf{y}_2$ is $C(\gamma^{N_1},c)$, the length of embedded messages is $nE_{N_2}(\gamma,C(\gamma^{N_1},c))$.

The function $E_N(\gamma,c)$ is defined recursively as follows:

$$C(\gamma,c)=\frac{c(1+\gamma)}{2}\tag{19}$$

$$E(\gamma_1,\gamma_2,c)=(1-\gamma_1)(1-\gamma_2)c\tag{20}$$

$$E_2(\gamma,c)=E(\gamma,\gamma,c)=(1-\gamma)^2c\tag{21}$$

$$E_3(\gamma,c)=E(\gamma,\gamma^2,c)+E_2\left(\gamma,C(\gamma,c)\right).\tag{22}$$

For $N \geq 4$, let $N = N_1 + N_2$, where $N_1 = \lfloor N/2 \rfloor$ and $N_2 = \lfloor (N+1)/2 \rfloor$. Define

$$E_N(\gamma, c) = E(\gamma^{N_1}, \gamma^{N_2}, c) + E_{N_1}\left(\gamma, C(\gamma^{N_2}, c)\right) + E_{N_2}\left(\gamma, C(\gamma^{N_1}, c)\right). \quad (23)$$

Therefore, for the N-page construction, the inner coding can embed $nE_N(\gamma, c)$ bits of messages, which does not increase the number of changes. The outer coding embeds $n(1-\gamma^N)\alpha$ bits of messages and induces on average $n(1-\gamma^N)c$ changes. Thus, the length of messages embedded by the N-page construction is

$$n(1-\gamma^N)\alpha + nE_N(\gamma, c). \quad (24)$$

The average number of changes is

$$n(1-\gamma^N)c. \quad (25)$$

Because the number of dry bits in the original cover $\mathbf{x} = (\mathbf{x}_1^k, \mathbf{x}_2^k, \cdots, \mathbf{x}_N^k)$ is $Nn(1-\gamma)$, the relative payload α_N, change rate c_N, and embedding efficiency e_N can be calculated by

$$\alpha_N = \frac{(1-\gamma^N)\alpha + E_N(\gamma, c)}{N(1-\gamma)} \quad (26)$$

$$c_N = \frac{(1-\gamma^N)c}{N(1-\gamma)} \quad (27)$$

$$e_N = \frac{\alpha_N}{c_N} = \frac{\alpha}{c} + \frac{E_N(\gamma, c)}{(1-\gamma^N)c}. \quad (28)$$

In fact, by N-page construction, we generate a family of WPCs, WPC(α_N, c_N), $N \geq 1$, from one code WPC(α, c), with decreasing the relative payload α_N and increasing the embedding efficiency e_N. When $N = 1$, we just get the original code WPC(α, c), and therefore, the maximum relative payload reached by the code family is α. We point out that, when taking $N = 2^k$, $k \geq 0$, the N-page construction is just the Paper Folding method proposed by the authors in [18].

The N-page construction is compared with the Meet-in-the-Middle method [20] and the method based on syndrome trellis codes (STC) [22]. For N-page construction, we generate the code family from WPC(1, 0.5), and thus the code family can reach the maximal relative payload 1. The relative payload and embedding efficiency are calculated by (26) and (28) for wet ratio $\gamma = 0.1$ and 0.9. In the Meet-in-the-Middle method, we use random codes with codimension $p = 20$, as proposed in [20]. In the STC, we take the constraint heigh $h = 11$ as used in [22]. The performances of Meet-in-the-Middle and STC are estimated by embedding messages into a cover with 2^{20} pixels. As shown in Fig. 5, the N-page code family includes the Paper Folding code family as a subset. Both N-page construction and STC outperform the Meet-in-the-Middle method. Comparing with STC, the N-page construction can achieve higher embedding efficiency for small relative payloads. However, the embedding efficiency of the N-page construction decreases as the wet ratio γ increases, while the Meet-in-the-Middle method and STC are independent of γ.

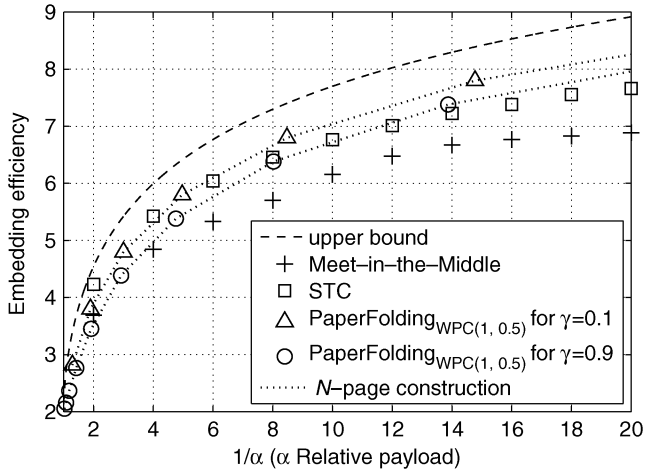

Fig. 5. Comparison between the Meet-in-the-Middle method, STC, and N-page construction for wet ratio $\gamma = 0.1$ and 0.9.

E. Capacity Loss in Practical Implementation

In the analysis above, we did not consider the capacity loss due to the overhead. In practice, the sender should first embed the page number N, which needs about 10 bits because N usually will not be larger than 1000. By bit replacement, the sender embeds the 10 bits into the first ten elements of the cover which can include wet positions. In other words, we allow to modify wet pixels for embedding these 10 bits. On average, five pixels will be modified including only $5\gamma < 5$ wet pixels, which has negligible impact on the statistical detectability.

The sender uses the rest cover to do N-page construction that consists of $k-1$ WPC(1, 0.5) for the inner coding and one WPC(α, c) for the outer coding, where $k = \lceil \log_2 N \rceil + 1$. WPC(1, 0.5) can be obtained by the methods in [2], [19] as described in Section II, which needs an overhead of 20 bits in practice. If we implement WPC in the outer coding by other methods, e.g., the STC method [22], 20 bits is also enough to communicate the length of the message. Therefore, the overhead for N-page construction is about $20k$ bits.

The practical N-page construction with the overhead is also compared with STC. Fig. 6 shows the experimental results obtained by embedding messages into covers with 2^{20} pixels. Due to the overhead, the N-page code family from WPC(1, 0.5) for $\gamma = 0.9$ drops below the STC even for the small relative payload.

We note that the embedding efficiency of STC is very close to the upper bound at the relative payload 0.5. In fact, STC has change rate $c \approx 0.12$ for $\alpha = 0.5$, i.e., yields a WPC(0.5, 0.12), which we denote by "STC0.5". When using "STC0.5" in the outer coding of the N-page construction, we can generate more efficient code families. As shown in Fig. 6, for the large wet ratio $\gamma = 0.9$, the N-page code family generated from "STC0.5" outperforms the code family generated from WPC(1, 0.5). When the wet ratio γ decreases to 0.1, the N-page code family generated from "STC0.5" is closer to the upper bound on embedding efficiency.

The N-page construction inherits the following merit of ZZW construction [15]: when the WPC(α, c) is close to the upper bound on the embedding efficiency at a relative payload α, the

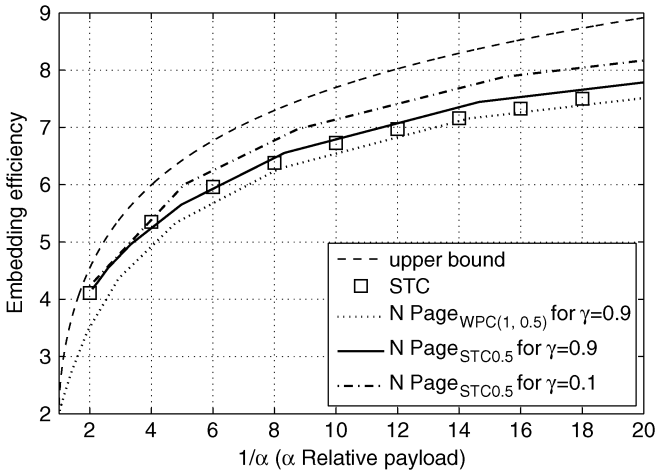

Fig. 6. Performance of N-page code families with the overhead. Code families are generated from WPC(1, 0.5) and STC0.5, respectively. STC0.5 denotes the code obtained by the STC method at relative payload 0.5, which has the change rate about 0.12.

code family generated from the WPC(α, c) will be close to the upper bound for the relative payloads smaller than α. In fact, it has been proved in [16] and [17] that the ZZW code family will follow the upper bound on the embedding efficiency as the relative payload tends to zero. However, ZZW construction is the special case of 2^k-page construction for $\gamma = 0$. For $\gamma > 0$, will the embedding efficiency of the code family still follow the upper bound? How will the embedding efficiency of the code family drop when the wet ratio γ tends to 1? How will the performance of code family in zero payload limit be influenced by the overhead? To answer these questions on asymptotic behavior, we concentrate on the 2^k-page construction.

V. Analysis of 2^k-Page Construction

A. Explicit Expression on Embedding Efficiency of 2^k-Page Construction

By the N-page construction, we can generate a family of WPCs from a WPC(α, c), and the relative payload tends to zero when $N \to \infty$. The performance of steganographic schemes in zero-payload limit is important for both embedding in a large cover and analyzing the security of batch steganography [23], [24]. However, it is still difficult to analyze the asymptotic property of N-page construction, because its embedding efficiency is expressed in a recursive form. For simplifying this problem, we analyze 2^k-page construction, that is, the Paper Folding method in [18]. Although the 2^k-page construction yields only a subset of the code family generated by the N-page construction, this subset can typically reflect the properties of the whole code family as shown in Fig. 5.

Next, explicit expressions on the performance of the 2^k-page construction will be derived, from which we deduce the limit of the distance between the embedding efficiency of 2^k-page construction and the upper bound on the embedding efficiency as a function of change rate (1). This result can approximately display the asymptotic behavior of the N-page construction.

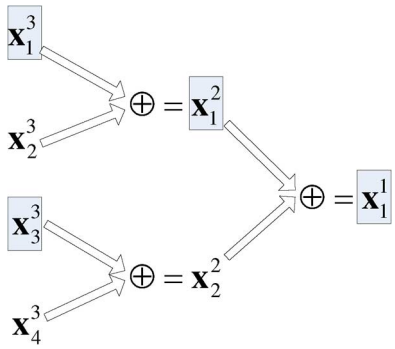

Fig. 7. Illustration of the four-page construction.

In the BTPC described in Section IV-B, because $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ have the same wet ratio γ and the change rate of $\mathbf{x}_1^1$ is c, by (12), the change rates of $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ are both equal to

$$C(\gamma, c) = \frac{c(1+\gamma)}{2}. \tag{29}$$

To deduce the embedding efficiency of the 2^k-page construction by recursively employing the BTPC, we rewrite $C(\gamma, c)$ as

$$C(\gamma, c) \triangleq C_1(\gamma, c). \tag{30}$$

For the four-page construction, assume that the cover consists of four n-length blocks, $\mathbf{x}_1^3$, $\mathbf{x}_2^3$, $\mathbf{x}_3^3$, and $\mathbf{x}_4^3$, with the same wet ratio γ. As shown in Fig. 7, the embedding procedure includes three steps. First, by the outer coding of BTPC, we embed $n(1-\gamma^4)\alpha$ bits of messages into $\mathbf{x}_1^1$ by a WPC(α, c). Second, because the wet ratios of $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ are both γ^2, by (13), we embed $nE_2(\gamma^2, c) = nc(1-\gamma^2)^2$ bits of messages into $\mathbf{x}_1^2$, and by (30) the change rates of $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ are both $C_1(\gamma^2, c)$. Therefore, (13) implies that we can embed $2nE_2(\gamma, C_1(\gamma^2, c)) = 2nC_1(\gamma^2, c)(1-\gamma)^2$ bits of messages into $\mathbf{x}_1^3$ and $\mathbf{x}_3^3$. The total number of embedded bits is

$$n(1-\gamma^4)\alpha + nc(1-\gamma^2)^2 + 2nC_1(\gamma^2, c)(1-\gamma)^2. \tag{31}$$

For the eight-page construction, we assume the cover consists of eight blocks of length n, $(\mathbf{x}_1^4, \mathbf{x}_2^4, \ldots, \mathbf{x}_8^4)$, with the same wet ratio γ. Fig. 8 shows that the embedding procedure includes four steps. First, the outer coding embeds $n(1-\gamma^8)\alpha$ bits of messages into $\mathbf{x}_1^1$ by a WPC(α, c). Second, because the wet ratios of $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ are both γ^4, by (13) we embed $nE_2(\gamma^4, c) = nc(1-\gamma^4)^2$ bits of messages into $\mathbf{x}_1^2$, and by (30) the change rates of $\mathbf{x}_1^2$ and $\mathbf{x}_2^2$ are $C_1(\gamma^4, c)$. In the third step, we cascade $\mathbf{x}_1^3$ and $\mathbf{x}_3^3$ to do inner coding of BTPC, and embed $2nE_2(\gamma^2, C_1(\gamma^4, c)) = 2nC_1(\gamma^4, c)(1-\gamma^2)^2$ bits of messages. Because the wet ratio of $\mathbf{x}_j^3$ is γ^2 for $1 \le j \le 4$, (30) implies the change rate of $\mathbf{x}_j^3$, $1 \le j \le 4$, is

$$C_1\left(\gamma^2, C_1(\gamma^4, c)\right). \tag{32}$$

Define

$$C_1\left(\gamma, C_1(\gamma^2, c)\right) \triangleq C_2(\gamma, c). \tag{33}$$

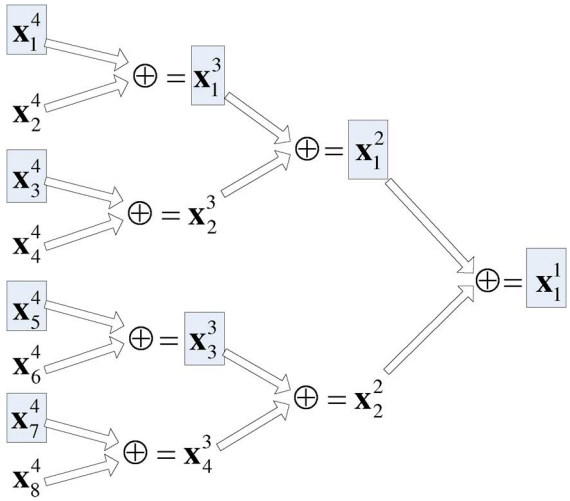

Fig. 8. Illustration of the eight-page construction.

Thus, (32) can be rewritten as

$$C_2(\gamma^2, c). \tag{34}$$

In the fourth step, cascade $\mathbf{x}_1^4$, $\mathbf{x}_3^4$, $\mathbf{x}_5^4$, and $\mathbf{x}_7^4$ to do inner coding of BTPC, the length of embedded messages is

$$4nE_2\left(\gamma, C_2(\gamma^2, c)\right) = 4nC_2(\gamma^2, c)(1-\gamma)^2. \tag{35}$$

The total number of embedded bits is

$$n(1-\gamma^8)\alpha + nc(1-\gamma^4)^2 + 2nC_1(\gamma^4, c)(1-\gamma^2)^2 + 4nC_2(\gamma^2, c)(1-\gamma)^2. \tag{36}$$

To get the general expression on the performance of the 2^k-page construction, we recursively define

$$C_n(\gamma, c) = C_1\left(\gamma, C_{n-1}(\gamma^2, c)\right), \quad n \geq 2. \tag{37}$$

For the 2^k-page construction, the embedding procedure consists of $k+1$ steps. First, the outer coding embeds $n(1-\gamma^{2^k})\alpha$ bits by a WPC(α, c). The length of the message embedded in the second step is

$$nc\left(1-\gamma^{2^{k-1}}\right)^2. \tag{38}$$

In the jth step for $3 \leq j \leq k+1$, the length of the embedded messages is

$$n2^{j-2}C_{j-2}\left(\gamma^{2^{k-(j-2)}}, c\right)\left(1-\gamma^{2^{k-1-(j-2)}}\right)^2. \tag{39}$$

Therefore, the total number of bits embedded by the 2^k-page construction is

$$L_{2^k} = n\alpha\left(1-\gamma^{2^k}\right) + nc\left(1-\gamma^{2^{k-1}}\right)^2 + n\sum_{j=1}^{k-1} 2^j C_j\left(\gamma^{2^{k-j}}, c\right)\left(1-\gamma^{2^{k-1-j}}\right)^2. \tag{40}$$

It is easy to calculate recursively that

$$C_j\left(\gamma^{2^{k-j}}, c\right) = \frac{c\prod_{i=1}^{j}\left(1+\gamma^{2^{k-i}}\right)}{2^j}, \quad 1 \leq j \leq k-1. \tag{41}$$

Thus,

$$L_{2^k} = n\alpha\left(1-\gamma^{2^k}\right) + nc\left(1-\gamma^{2^{k-1}}\right)^2 + n\sum_{j=1}^{k-1}\left(1-\gamma^{2^{k-1-j}}\right)^2 c\prod_{i=1}^{j}\left(1+\gamma^{2^{k-i}}\right). \tag{42}$$

Because the number of dry bits in the original cover is $2^k n(1-\gamma)$, the relative payload of 2^k-page construction is

$$\alpha_{2^k} = \frac{L_{2^k}}{2^k n(1-\gamma)}. \tag{43}$$

By (27), the change rate is

$$c_{2^k} = \frac{\left(1-\gamma^{2^k}\right)c}{2^k(1-\gamma)}. \tag{44}$$

By using (42), (43), and (44), we can obtain the embedding efficiency of the 2^k-page construction such that

$$e_{2^k} = \frac{\alpha_{2^k}}{c_{2^k}} = \frac{\alpha}{c} + \sum_{i=0}^{k-1}\frac{1-\gamma^{2^i}}{1+\gamma^{2^i}}. \tag{45}$$

Equation (45) shows how the embedding efficiency is influenced by the wet ratio γ. When $\gamma = 0$, the performance of the 2^k-page construction is the same as that of the ZZW construction [15]. Therefore, the 2^k-page construction can be viewed as a generalization of the ZZW construction. However, when the wet ratio $\gamma = 0$, the implementation by ZZW construction is simpler, which needs only two steps.

B. Asymptotic Property of 2^k-Page Construction

To analyze the asymptotic property of 2^k-page construction, we need the following lemma.

Lemma 1: Define

$$\sigma(\gamma) = \sum_{i=0}^{\infty}\frac{\gamma^{2^i}}{1+\gamma^{2^i}}. \tag{46}$$

The series $\sigma(\gamma)$ converges when $\gamma \in [0, 1)$. Furthermore, for any $\varepsilon > 0$, let

$$T = \left\lceil \frac{1}{\ln 2}\left(\ln\ln\left(\frac{\varepsilon}{1+\varepsilon}\right) - \ln\ln\gamma\right) - 1\right\rceil \tag{47}$$

and then $\sigma(\gamma)$ can be estimated by the sum of the first $T+1$ items such that

$$\sigma(\gamma) - \sum_{i=0}^{T}\frac{\gamma^{2^i}}{1+\gamma^{2^i}} < \varepsilon. \tag{48}$$

The following Theorem 1 gives the limit of the distance between the embedding efficiency of the 2^k-page construction and the upper bound (1) as k tends to infinity.

Theorem 1: Under the notation established in (44), (45) and Lemma 1,

$$\begin{aligned}\lim_{k\to\infty}\left[\frac{H(c_{2^k})}{c_{2^k}}-e_{2^k}\right]&=\log_2\frac{1}{c}+\frac{1}{\ln 2}-\frac{\alpha}{c}+\log_2(1-\gamma)+2\sigma(\gamma)\\&\triangleq\lambda(\alpha,c)+I(\gamma)\end{aligned}\tag{49}$$

where

$$\lambda(\alpha,c)\triangleq\log_2\frac{1}{c}+\frac{1}{\ln 2}-\frac{\alpha}{c}\tag{50}$$

$$I(\gamma)\triangleq\log_2(1-\gamma)+2\sigma(\gamma).\tag{51}$$

Proof:

$$\begin{aligned}\frac{H(c_{2^k})}{c_{2^k}}-e_{2^k}&=-\log_2(c_{2^k})-\left(\frac{1}{c_{2^k}}-1\right)\log_2(1-c_{2^k})\\&\quad-\frac{\alpha}{c}-\sum_{i=0}^{k-1}\frac{1-\gamma^{2^i}}{1+\gamma^{2^i}}\\&=k+\log_2\frac{1}{c}+\log_2\left(\frac{1-\gamma}{1-\gamma^{2^k}}\right)\\&\quad-\left(\frac{1}{c_{2^k}}-1\right)\log_2(1-c_{2^k})-\frac{\alpha}{c}\\&\quad-\sum_{i=0}^{k-1}\frac{1-\gamma^{2^i}}{1+\gamma^{2^i}}\\&=\log_2\frac{1}{c}+\log_2\left(\frac{1-\gamma}{1-\gamma^{2^k}}\right)\\&\quad-\left(\frac{1}{c_{2^k}}-1\right)\log_2(1-c_{2^k})\\&\quad-\frac{\alpha}{c}+2\sum_{i=0}^{k-1}\frac{\gamma^{2^i}}{1+\gamma^{2^i}}.\end{aligned}\tag{52}$$

Note that c_{2^k} tends to zero as $k\to\infty$, and thus by L'Hôpital's rule, we have

$$\lim_{k\to\infty}\left(\frac{1}{c_{2^k}}-1\right)\log_2(1-c_{2^k})=-\frac{1}{\ln 2}.\tag{53}$$

Because $0\le\gamma<1$,

$$\lim_{k\to\infty}\log_2\left(\frac{1-\gamma}{1-\gamma^{2^k}}\right)=\log_2(1-\gamma).\tag{54}$$

In (52), by using Lemma 1, (53) and (54), we prove the theorem. ∎

In Theorem 1, $I(\gamma)$ is the increment of distance to the upper bound caused by the wet ratio γ. When $\gamma=0$, the limit (49) becomes $\lambda(\alpha,c)$, which is equal to the limit obtained by Fridrich [16] for the ZZW construction, although the limit in [16] is derived by taking the embedding efficiency as a function of the relative payload. Fridrich [16] proposed to compare codes with $\lambda(\alpha,c)$. Likewise, we can evaluate the performance of a code WPC(α,c) at the wet ratio γ by using $\lambda(\alpha,c)+I(\gamma)$.

TABLE I
SOME TYPICAL VALUES OF $\hat{I}(\gamma)$ WITH RESPECT TO THE WET RATIO γ

γ	0.1	0.5	0.9	0.99	0.999	0.9999
$\hat{I}(\gamma)$	0.0500	0.1923	0.2963	0.3167	0.3187	0.3189

Next, we answer how the increment $I(\gamma)$ will ascend when the wet ratio γ tends to 1. Taking $\varepsilon=0.0001$ in Lemma 1, we estimate $\sigma(\lambda)$ by

$$\hat{\sigma}(\gamma)=\sum_{i=0}^{T}\frac{\gamma^{2^i}}{1+\gamma^{2^i}}+\varepsilon.\tag{55}$$

Replacing $\sigma(\gamma)$ by $\hat{\sigma}(\gamma)$ in (51), we get an estimator $\hat{I}(\gamma)$ for $I(\gamma)$ such that $\hat{I}(\gamma)-I(\gamma)<2\varepsilon=0.0002$. Some typical values of $\hat{I}(\gamma)$ are listed in Table I, which shows that $\hat{I}(\gamma)$ goes up to about 0.3 at $\gamma=0.9$ and the ascending speed of $\hat{I}(\gamma)$ is very slow for $\gamma>0.9$. When the dry ratio decreases to 1/10000 ($\gamma=0.9999$), the dropping amount of embedding efficiency due to γ is only 0.3189.

In the above analysis, we did not consider the capacity loss due to the overhead. The overhead is influenced by the block length n and the wet ratio γ and in the general case an overhead of $\log_2(n)$ bits for each WPC is needed. The 2^k-page construction consists of $k+1$ WPCs and thus the total overhead needs $(k+1)\log_2(n)$ bits. With this overhead, equation (42) for the payload should be modified as $L_{2^k}-(k+1)\log_2(n)$. Because the change rate keeps the same as expressed by (44), the loss in embedding efficiency can be calculated by

$$I_h=\frac{(k+1)\log_2(n)}{nc\left(1-\gamma^{2^k}\right)}\tag{56}$$

where c is the change rate in the outer coding. Note that I_h will tend to infinity with increasing k. Thus, due to the overhead, the distance between the embedding efficiency of 2^k-page construction and the upper bound cannot approach a finite limit. However, comparing with the decreasing speed of the relative payload, the increasing speed of I_h is very slow. For example, when taking $n=4\times10^4$, $c=0.5$, and $\gamma=0.9$, an overhead of 20 bits for each WPC is enough, and I_h climbs to only 0.05 as the relative payload α_{2^k} drops to 4.2×10^{-13}.

VI. CONCLUSION

Improving the embedding efficiency of WPCs can reduce the embedding changes, and thus make the steganography based on WPCs more secure. The Paper Folding method [18] and Wet ZZW construction [19] are extensions of ZZW construction [15] from the dry paper model to the wet paper model, and both methods provide a high embedding efficiency.

In this paper, we propose the N-page construction that is a generalization of the Paper Folding method and an equivalent version of Wet ZZW construction. The N-page construction makes it possible to deduce the formulas for calculating the embedding efficiency of methods in [18] and [19]. From these formulas, we analyze the asymptotic behavior of 2^k-construction, which is important for embedding messages into a long cover or a batch of covers [23], [24]. By the limit derived in Section V-B, we conclude that the wet ratio will not influence the embedding efficiency seriously for embedding messages into long covers.

The result in Theorem 1 can be viewed as a generalization of the limit theorem derived by Fridrich in [16], which is about ZZW construction for wet ratio $\gamma = 0$. Theorem 1 now is only about 2^k-construction. In fact, the extension of Theorem 1 for N-page construction at $\gamma = 0$ has also been obtained in [17], showing that the inferior limit is still $\lambda(\alpha, c)$, but the superior limit is about $\lambda(\alpha, c) + 0.086$. Thus, we present the following conjecture: for $\gamma > 0$, the inferior limit between the embedding efficiency of N-page construction and the upper bound on the embedding efficiency is $\lambda(\alpha, c) + I(\gamma)$, and the superior limit is about $\lambda(\alpha, c) + I(\gamma) + 0.086$.

APPENDIX

Proof of Lemma 1:

Proof: Let $\gamma \in [0, 1)$, and

$$u_i = \frac{\gamma^{2^i}}{1 + \gamma^{2^i}} \tag{57}$$

and then

$$\lim_{i \to \infty} \frac{u_{i+1}}{u_i} = \lim_{i \to \infty} \left(r^{2^i} \frac{1 + r^{2^i}}{1 + r^{2^{i+1}}} \right) = 0. \tag{58}$$

According to d'Alembert Ratio Test, $\sigma(\gamma)$ converges.

On the other hand, let T be a positive integer, and

$$\sigma(\gamma) = \sum_{i=0}^{\infty} \frac{\gamma^{2^i}}{1 + \gamma^{2^i}} = \sum_{i=0}^{T} \frac{\gamma^{2^i}}{1 + \gamma^{2^i}} + \sum_{i=T+1}^{\infty} \frac{\gamma^{2^i}}{1 + \gamma^{2^i}}. \tag{59}$$

Obviously,

$$\sum_{i=T+1}^{\infty} \frac{\gamma^{2^i}}{1 + \gamma^{2^i}} \leq \sum_{i=T+1}^{\infty} \gamma^{2^i}. \tag{60}$$

By adding items into the series in the right hand of (60), we get

$$\sum_{i=T+1}^{\infty} \gamma^{2^i} \leq \gamma^{2^{T+1}} \sum_{i=0}^{\infty} \gamma^{i 2^{T+1}} = \frac{\gamma^{2^{T+1}}}{1 - \gamma^{2^{T+1}}}. \tag{61}$$

For any $\varepsilon > 0$, let

$$\frac{\gamma^{2^{T+1}}}{1 - \gamma^{2^{T+1}}} < \varepsilon \tag{62}$$

and we get

$$T > \frac{1}{\ln 2} \left(\ln \ln \left(\frac{\varepsilon}{1 + \varepsilon} \right) - \ln \ln \gamma \right) - 1. \tag{63}$$

Thus, taking

$$T = \left\lceil \frac{1}{\ln 2} \left(\ln \ln \left(\frac{\varepsilon}{1 + \varepsilon} \right) - \ln \ln \gamma \right) - 1 \right\rceil \tag{64}$$

we have

$$\sigma(\gamma) - \sum_{i=0}^{T} \frac{\gamma^{2^i}}{1 + \gamma^{2^i}} < \varepsilon. \tag{65}$$

REFERENCES

[1] J. Fridrich, M. Goljan, P. Lisoněk, and D. Soukal, "Writing on wet paper," *Special Issue on Media Security, IEEE Trans. Signal Process.*, vol. 53, pp. 3923–3935, Oct. 2005.

[2] J. Fridrich, M. Goljan, and D. Soukal, "Efficient wet paper codes," in *Proc. 7th Int. Workshop on Information Hiding*, 2005, vol. 3727, LNCS, pp. 204–218.

[3] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography using wet paper codes," in *Proc. ACM Multimedia and Security Workshop on Multimedia and Security*, 2004, pp. 4–15.

[4] H. Gou and M. Wu, "Improving embedding payload in binary images with "super-pixels"," in *Proc. IEEE Int. Conf. Image Processing (ICIP 2007)*, 2007, pp. 277–280.

[5] J. Yu, X. Wang, J. Li, and X. Nan, "A fragile document watermarking technique based on wet paper code," in *Proc. Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2008)*, 2008, pp. 25–28.

[6] R. Crandall, Some Notes on Steganography 1998 [Online]. Available: http://os.inf.tu-dresden.de/westfeld/crandall.pdf, Posted on steganography mailing list

[7] Y. C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1227–1231, Aug. 2002.

[8] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography," *LNCS Trans. Data Hiding and Multimedia Security*, vol. 4902, pp. 1–22, 2008.

[9] D. Schönfeld and A. Winkler, "Embedding with syndrome coding based on BCH codes," in *Proc. ACM 8th Workshop on Multimedia and Security*, 2006, pp. 214–223.

[10] C. Munuera, "Steganography and error-correcting codes," *Signal Process.*, vol. 87, pp. 1528–1533, 2007.

[11] W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," *IEEE Commun. Lett.*, vol. 11, no. 8, pp. 680–682, Aug. 2007.

[12] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 390–394, Sep. 2006.

[13] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, 2007, vol. 6050, pp. 02–03.

[14] M. Khatirinejad and P. Lisoněk, "Linear codes for high payload steganography," *Discrete Appl. Math.*, vol. 157, pp. 971–981, 2009.

[15] W. Zhang, X. Zhang, and S. Wang, "Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes," in *Proc. 10th Information Hiding*, 2008, vol. 5284, LNCS, pp. 60–71, Springer-Verlag.

[16] J. Fridrich, "Asymptotic behavior of the ZZW embedding construction," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 151–154, Mar. 2009.

[17] W. Zhang and X. Wang, "Generalization of the ZZW embedding construction for steganography," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 564–569, Sep. 2009.

[18] W. Zhang and X. Zhu, "Improving the embedding efficiency of wet paper codes by paper folding," *IEEE Signal Process. Lett.*, vol. 16, no. 2, pp. 794–797, Sep. 2009.

[19] T. Filler and J. Fridrich, "WET ZZW construction for steganography," in *IEEE Workshop on Information Forensic and Security (WIFS)*, London, U.K., Dec. 7–9, 2009.

[20] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 102–110, Mar. 2006.

[21] C. Fontaine and F. Galand, "How Reed-Solomon codes can improve steganographic schemes," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/274845, Article 274845, 10 pages.

[22] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using Trellis-coded quantization," in *Proc. SPIE, Electronic Imaging, Media Forensics and Security XII*, San Jose, CA, Jan. 18–20, 2010.

[23] A. D. Ker, "A capacity result for batch steganography," *IEEE Signal Process. Lett.*, vol. 14, no. 8, pp. 525–528, Aug. 2007.

[24] T. Filler, A. D. Ker, and J. Fridrich, "The square root law of steganographic capacity for markov covers," in *Media Forensics and Security XI, Proc. SPIE 7254*, 2009, pp. 0801–0811.

Weiming Zhang received the M.S. and Ph.D. degrees from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2002 and 2005, respectively.

Currently, he is an associate professor with the School of Information Science and Technology, University of Science and Technology of China, Hefei. His research interests include information hiding and cryptography.

Jiufen Liu received the B.S. degree in mathematics from Henan University, China, in 1985, the M.E. degree in mathematics from Beijing Normal University, China, in 1990, and the Ph.D. degree in mathematics from Zhejiang University, China, in 2001.

Since 1990, she has been with the faculty of the Zhengzhou Information Science and Technology Institute, Zhengzhou, China, where she is currently an associate professor. Her research interests include information hiding and wavelets.

Xin Wang received the M.S. degree from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2002.

Currently, she is a Lecturer in the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. Her research interests include image watermarking and digital blind image forensics.

Nenghai Yu received the B.S. degree from Nanjing University of Posts and Telecommunications, in 1987, the M.E. degree from Tsinghua University, in 1992, and the Ph.D. degree from University of Science and Technology of China, in 2004

He is currently a professor with the University of Science and Technology of China, Hefei. His research interests include multimedia security, multimedia information retrieval, video processing, and information hiding.