# A Secure Data Hiding Scheme for Binary Images

Yu-Chee Tseng, *Member, IEEE*, Yu-Yuan Chen, and Hsiang-Kuang Pan

***Abstract*—This letter presents a novel steganography scheme capable of concealing a piece of critical information in a host message which is a binary image (e.g., a facsimile). A binary matrix and a weight matrix are used as secret keys to protect the hidden information. Given a host image of size $m \times n$, the proposed scheme can conceal as many as $\lfloor \log_2(mn+1) \rfloor$ bits of data in the image by changing, at most, two bits in the host image. This scheme can provide a higher security, embed more information, and maintain a higher quality of the host image than available schemes.**

***Index Terms*—Cryptography, data hiding, prisoners' problem, security, steganography.**

## I. Introduction

THE increasing popularity of digital media has ushered in concern over security-related issues. The *confidentiality* of a document is typically achieved by *encryption*. However, as an encrypted message normally reveals the importance of its content, the ciphertext also attracts the interest of cryptanalysts. *Steganography* differs from encryption, in that it embeds critical information in a noncritical host message (e.g., webpages and advertisements) to distract opponents' attention [8], [13]. Therefore, steganography is also known as *data/information hiding*.

The study of steganography can be traced to [10], in which the *Prisoners' Problem* was proposed. In this scenario, Alice and Bob were in jail, and attempted an escape plan. However, all their communications must go through the warden, Willie. If detecting any encrypted messages, Willie would frustrate their plan by putting them into solitary confinement. Therefore, Alice and Bob must find a way to conceal their secret in an innocuous-looking covertext. The history and bandwidth concerns of the *subliminal channel* are discussed in [11], [12].

Data hiding is typically achieved by altering some nonessential information in the host message. For example, given a color image, the least-significant bit (LSB) of each pixel can be changed to embed the hidden secret [14]. A hiding scheme based on the conventional keystream generator is proposed in [5]. Information hiding for security documents (e.g., currency) is discussed in [6]. References [1] and [2] consider how to apply public-key cryptography to steganography. Reviews of steganography are in [2], [3], and [7].

Hiding data in a binary image is a more challenging task, since changing any pixel can be easily detected. References [16] and [17] address this subject. The quality of the image, once data are concealed in it, is further considered in [15]. Watermarking on binary images is discussed in [9]. To improve the image hiding quality and hiding capacity, this letter presents a novel scheme capable of hiding a large amount of data by changing a small number of bits in the original binary image. Specifically, given an $m \times n$ image block, the proposed scheme can conceal as many as $\lfloor \log_2(mn+1) \rfloor$ bits of data in the block by changing, at most, two bits in the block. This approach is much more efficient than available schemes [15]–[17], which can hide, at most, one bit in each block by changing, at most, one bit in the block.

Three aspects of the advantages of the proposed scheme should be considered. First, let us assume that the maximum number of pixels that can be modified in the binary image is fixed. We can consider an image block of size $2mn$. The proposed scheme can hide $\lfloor \log_2(2mn+1) \rfloor$ bits by changing, at most, two bits in the image. In contrast, available schemes can partition the image into two blocks, each of size $mn$. Then, at most, two bits in the image can be modified to conceal two bits of data. Thus, the proposed scheme offers a data-hiding ratio that is $\lfloor \log_2(2mn+1) \rfloor / 2$ times that of available schemes. Second, if, on the contrary, equalizing the amount of embedded data is desired, the image quality after modification will be significantly improved, since fewer pixels are altered. Third, due to the above reasons, the proposed scheme is more secure than available ones because the existence of hidden data is less detectable.

The rest of this letter is organized as follows. Section II presents our data-hiding scheme. Section III discusses our experimental results. Finally, conclusions are drawn in Section IV.

## II. Proposed Data-Hiding Scheme for Binary Images

The proposed scheme uses a binary matrix and an integer weight matrix as secret keys. The operator XOR is adopted so that the keys can not be compromised easily. Another important function of the weight matrix is to increase the data-hiding capacity. The inputs to our scheme are as follows.

1) $F$ is a host binary image (i.e., bitmap), which is to be modified to embed data. Here, $F$ is partitioned into blocks of size $m \times n$. For simplicity, we assume that the size of $F$ is a multiple of $m \times n$.
2) $K$ is a secret key shared by the sender and the receiver. It is a randomly selected bitmap of size $m \times n$.

Paper approved by K. Rose, the Editor for Source Channel Coding of the IEEE Communications Society. Manuscript received May 9, 2000; revised May 10, 2001, November 30, 2001. The work of Y.-C. Tseng was supported by Lee and MTI Center for Networking Research at NCTU, the Ministry of Education under Contract 90-H-FA07-1-4, and the National Science Council, Taiwan, R.O.C., under Contract NSC89-2218-E-009-095. This paper was presented in part at the IEEE Symposium on Computers and Communications, France, 2000.

Y.-C. Tseng is with the Department of Computer Science and Information Engineering, National Chiao Tung University, Hsin-Chu 30050, Taiwan, R.O.C. (e-mail: yctseng@csie.nctu.edu.tw).

Y.-Y. Chen and H.-K. Pan are with the Department of Computer Science and Information Engineering, National Central University, Chung-Li 32054, Taiwan, R.O.C. (e-mail: yychen@itri.org.tw; jerry@formosoft.com).

Publisher Item Identifier 10.1109/TCOMM.2002.801488.

0090-6778/02$17.00 © 2002 IEEE

3) $W$ is a secret-weight matrix shared by the sender and the receiver. It is an integer matrix of size $m \times n$ whose content satisfies some requirements (to be stated later).
4) $r$ is the number of bits to be embedded in each $m \times n$ block of $F$. The value of $r$ satisfies $2^r - 1 \leq mn$.
5) $B$ is critical information consisting of $kr$ bits to be embedded in $F$, where $k$ is the number of $m \times n$ blocks in $F$.

### A. Weight Management

The proposed scheme uses the weight matrix $W$ to represent the embedded data. This section presents an illustrative example to demonstrate how to manage weights. Section II-B presents the complete scheme.

Assume that the size of $K$ and $W$ is $3 \times 3$. Below, we consider a $3 \times 3$ image block $F_i$, which is a part of the host image $F$. The purpose is to show how to embed $r = 2$ bits of data in $F_i$. Let us assume the following inputs:

$$F_i = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \quad K = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad W = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}.$$

First, a bitwise exclusive-OR on $F_i$ and $K$ is performed.

$$F_i \oplus K = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

Next, let $\otimes$ be the componentwise multiplication operator on two equal-size integer matrices. The following computation is conducted:

$$(F_i \oplus K) \otimes W = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{bmatrix}.$$

Summing all elements in the rightmost matrix yields $\text{SUM}[(F_i \oplus K) \otimes W] = 1 + 3 + 2 + 1 + 3 = 10$.

Next, two data bits, denoted as $b_1 b_2$, are to be embedded into $F_i$. Assume that $F_i$ is transformed into $F_i'$. Regarding $b_1 b_2$ as a binary number, the proposed scheme will ensure the validity of the following invariant:

$$\textbf{I1}.\ \text{SUM}[(F_i' \oplus K) \otimes W] \equiv b_1 b_2 \pmod 4.$$

With this invariant, the receiver can derive $b_1 b_2$ by computing $\text{SUM}[(F_i' \oplus K) \otimes W] \bmod 4$.

Next, modifying $F_i$ to ensure **I1** is demonstrated. The goal is to change as few bits in $F_i$ as possible. Since $\text{SUM}[(F_i \oplus K) \otimes W] \equiv 2$, if, fortunately, $b_1 b_2 = 2$, then $F_i$ does not need to be changed. Otherwise, some bit(s) must be modified. Observe that if we complement bit $[F_i]_{j,k}$, then $[F_i \oplus K]_{j,k}$ will be complemented. If $[F_i \oplus K]_{j,k}$ is swapped from 0 to 1, then the modular sum will be increased by $w_{j,k}$; otherwise, the sum will be decreased by $w_{j,k}$. For instance, if we swap $[F_i]_{1,1}$, the sum will be decreased by $w_{1,1} = 1$, and if we swap $[F_i]_{1,2}$, the sum will be increased by $w_{1,2} = 2$. In this example, it is not hard to verify that we only need to complement one bit in $F_i$ to increase or decrease the sum by 1, 2, or 3. How to ensure the success of the swapping process will be discussed later.

### B. Hiding Steps

*Definition 1:* An $m \times n$ matrix $W$ can serve as a weight matrix if each element of $\{1, 2, \ldots, 2^r - 1\}$ appears at least once in $W$, i.e., $\{[W]_{i,j}, i = 1 \ldots m, j = 1 \ldots n\} = \{1, 2, \ldots, 2^r - 1\}$.

The rationale behind this definition will become clear later. Note that it is trivial to find a legal $W$ because we have already imposed the condition that $2^r - 1 \leq mn$. In fact, many choices are available for choosing $W$. Specifically, we can first pick $2^r - 1$ elements in matrix $W$ and randomly assign $\{1, 2, \ldots, 2^r - 1\}$ to them. The remaining $mn - (2^r - 1)$ elements in $W$ can then be assigned with arbitrary values. Based on such an assignment, the number of choices for $W$ is

$$C_{2^r-1}^{mn} * (2^r - 1)! * (2^r - 1)^{mn - (2^r - 1)}.$$

For instance, if $m = n = 8$ and $r = 5$, there are $C_{31}^{64} * 31! * 31^{33}$ possible $W$s. This number should be sufficiently large to prevent a brute-force attack.

Let $W$ be a legal weight matrix and $F_i$ be an image block, which is a part of $F$. Below, we show how to embed $r$ bits of data, say $b_1 b_2 \ldots b_r$, into $F_i$ by changing, at most, 2 bits in $F_i$. The goal is to modify $F_i$ into $F_i'$ to ensure the following invariant:

$$\textbf{I2}: \text{SUM}[(F_i' \oplus K) \otimes W] \equiv b_1 b_2 \ldots b_r \pmod{2^r}.$$

Below, the embedding scheme is derived in four steps.

1) Compute $F_i \oplus K$.
2) Compute $\text{SUM}[(F_i \oplus K) \otimes W]$.
3) From the matrix $F_i \oplus K$, compute for each $w = 1 \ldots 2^r - 1$ the following set:

$$S_w = \{(j,k) | ([W]_{j,k} = w \wedge [F_i \oplus K]_{j,k} = 0) \vee \\ ([W]_{j,k} = 2^r - w \wedge [F_i \oplus K]_{j,k} = 1)\}.$$

Intuitively, $S_w$ represents the set containing each matrix index $(j, k)$, such that complementing $[F_i]_{j,k}$ would increase the sum in step 2 by $w$. Two possibilities to achieve this are if $[W]_{j,k} = w$ and $[F_i \oplus K]_{j,k} = 0$, then complementing $[F_i]_{j,k}$ will increase the weight by $w$; and if $[W]_{j,k} = 2^r - w$ and $[F_i \oplus K]_{j,k} = 1$, then complementing $[F_i]_{j,k}$ will decrease the weight by $2^r - w$, or, equivalently, increase the sum by $w$ (under mod $2^r$).

The following lemmas indicate some important properties of these sets. (Detailed proofs can be found in [4].)

*Lemma 1:* For each $w = 1 \ldots 2^r - 1$, such that $w \neq 2^{r-1}$, the following statement is true:

$$(S_w = \emptyset) \Longrightarrow (S_{2^r - w} \neq \emptyset).$$

*Lemma 2:* The set $S_{2^{r-1}} \neq \emptyset$.

4) Define a weight difference as

$$d \equiv (b_1 b_2 \ldots b_r) - \text{SUM}[(F_i \oplus K) \otimes W] \pmod{2^r}.$$

The sum in step 2 must be increased by $d$ to satisfy **I2**. If $d = 0, F_i$ does not need to be changed. Otherwise, the following steps are executed to transform $F_i$ into

$$F=\begin{array}{cccc|cccc}
\multicolumn{4}{c}{F_1} & \multicolumn{4}{c}{F_2}\\
\hline
0&1&0&1&0&1&1&0\\
1&0&0&0&1&1&1&1\\
1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0\\
\hline
1&1&1&0&1&0&0&0\\
0&0&1&1&1&0&1&0\\
1&1&0&1&0&1&1&1\\
1&0&1&1&0&1&1&1\\
\hline
\multicolumn{4}{c}{F_3} & \multicolumn{4}{c}{F_4}
\end{array}
\qquad
K=\begin{array}{|c|c|c|c|}
\hline
1&1&0&0\\ \hline
0&1&0&0\\ \hline
1&1&1&0\\ \hline
0&0&1&0\\ \hline
\end{array}
\qquad
W=\begin{array}{|c|c|c|c|}
\hline
1&2&3&4\\ \hline
5&6&7&1\\ \hline
2&3&4&5\\ \hline
6&7&1&2\\ \hline
\end{array}$$

Fig. 1. Example of host image $F$, secret key $K$, and weight matrix $W$.

$$\begin{array}{cccc|cccc}
\multicolumn{4}{c}{F_1\oplus K} & \multicolumn{4}{c}{F_2\oplus K}\\
\hline
1&0&0&1&1&0&1&0\\
1&1&0&0&1&0&1&1\\
0&1&1&0&1&1&1&0\\
0&0&1&0&0&0&0&0\\
\hline
0&0&1&0&0&1&0&0\\
0&1&1&1&1&1&1&0\\
0&0&1&1&1&0&0&1\\
1&0&0&1&0&1&0&1\\
\hline
\multicolumn{4}{c}{F_3\oplus K} & \multicolumn{4}{c}{F_4\oplus K}
\end{array}
\qquad
\begin{array}{cccc|cccc}
\multicolumn{4}{c}{F_1'} & \multicolumn{4}{c}{F_2'}\\
\hline
0&1&0&1&0&1&1&0\\
1&0&0&1&1&1&1&1\\
1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0\\
\hline
1&1&1&0&1&0&0&0\\
0&0&1&1&1&1&1&0\\
1&1&0&1&0&0&1&1\\
1&0&1&0&0&1&1&1\\
\hline
\multicolumn{4}{c}{F_3'} & \multicolumn{4}{c}{F_4'}
\end{array}$$

(a) (b)

Fig. 2. (a) $F \oplus K$. (b) Modified host image.

$F_i'$. For ease of presentation, let us define $S_w = S_{w'}$ for any $w \equiv w'$ (mod $2^r$).

a) Randomly select an $h \in \{0, 1, \ldots, 2^r - 1\}$, such that $S_{hd} \neq \emptyset$ and $S_{-(h-1)d} \neq \emptyset$.
b) Randomly select a $(j, k) \in S_{hd}$ and complement the bit $[F_i]_{j,k}$.
c) Randomly select a $(j, k) \in S_{-(h-1)d}$ and complement the bit $[F_i]_{j,k}$.

Intuitively, to increase the sum by $d$, two nonempty sets $S_{hd}$ and $S_{-(h-1)d}$ can be selected. This is possible since these sets indicate the locations where $F_i$ can be complemented to increase the weights by $hd$ and $-(h-1)d$, respectively. Consequently, a total increase of the weight by $d$ is obtained.

However, the above steps are logically flawed, which was not mentioned intentionally for ease of presentation. In fact, the set $S_0$ (and similarly $S_{2^r}, S_{2\cdot 2^r}, S_{3\cdot 2^r}$, etc.) is not yet defined. Similar to other $S_w$s, $S_0$ can be regarded as the set of indices such that complementing these locations in $F_i$ will result in an increase of the weight by 0. Since this can be achieved by changing *nothing* on $F_i, S_0$ can be regarded as a nonempty set. Whenever the statement "complement the bit $[F_i]_{j,k}$" is encountered, this step is simply omitted. This amendment makes step 4 logically correct.

Finally, whether step 4 is successful depends on the success of step a) to identify a qualified $h$. This is proved below.

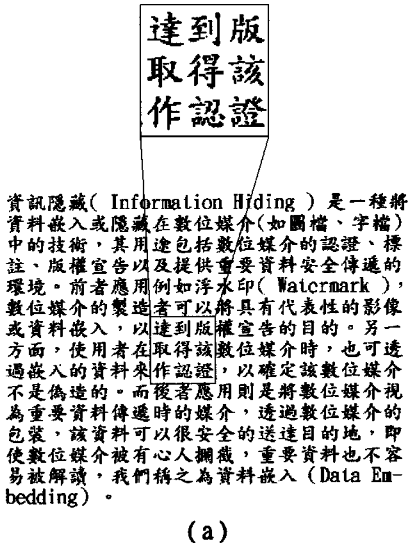
*Lemma 3:* Step 4 always succeeds, and, at most, two bits of $F_i$ are modified to embed $r$ bits of data.

The following example demonstrates how our scheme works. Let the host image be $F$, secret key be $K$, and weight matrix be $W$, as shown in Fig. 1. First, $F$ is partitioned into four $4 \times 4$ blocks $F_1 \ldots F_4$. Let $r = 3$, so we can embed 12 bits, say $B = 001\,010\,000\,001$, into $F$.

The XOR result of each $F_i, i = 1 \ldots 4$ with $K$ is in Fig. 2(a). For $F_1, \mathrm{SUM}[(F_1 \oplus K) \otimes W] \equiv 0 \pmod 8$. Since the embedded data is 001, the weight must be increased by 1. Since $[F_1 \oplus K]_{2,4} = 0$ and $[W]_{2,4} = 1$, we can complement $[F_1]_{2,4}$. For $F_2, \mathrm{SUM}[(F_2 \oplus K) \otimes W] \equiv 2$. Since the embedded data is 010, $F_2$ does not need to be modified. For $F_3, \mathrm{SUM}[(F_3 \oplus K) \otimes W] \equiv 2$. Since the embedded data is 000, the weight must be increased by 6, which can be done by complementing $[F_3]_{4,4}$. For $F_4, \mathrm{SUM}[(F_4 \oplus K) \otimes W] \equiv 4$. Since the embedded data is 001, the weight must be increased by 5. There is no single point in $F_4$ which can accomplish this task. Therefore, two bits in $F_4$ must be changed. One possibility is $S_{10} = S_2 = \{(2, 2)\}$ and $S_{-5} = S_3 = \{(1, 3), (2, 1), (3, 2), (3, 4)\}$. In this example, we choose to complement $[F_4]_{2,2}$ and $[F_4]_{3,2}$. Fig. 2(b) displays the final modified image.

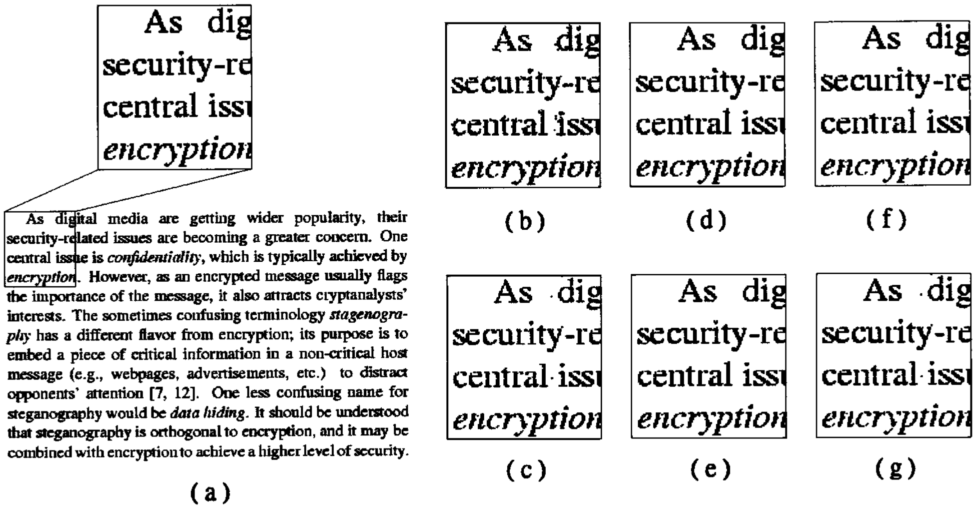
## III. Experimental Results

Herein, Wu and Lee's (WL) scheme [16] and the proposed scheme are implemented to visualize the data-hiding effect.


達到版
取得該
作認證
(a)
(b)
(c)
(d)
(e)
(f)
(g)

資訊隱藏( Information Hiding ) 是一種將資料嵌入或隱藏在數位媒介(如圖檔、字檔)中的技術，其用途包括數位媒介的認證、標註、版權宣告以及提供重要資料安全傳遞的環境。前者應用例如浮水印( Watcrmark )，數位媒介的製造者可以將具有代表性的影像或資料嵌入，以達到版權宣告的目的。另一方面，使用者在取得該數位媒介時，也可透過嵌入的資料來作認證，以確定該數位媒介不是偽造的。而後者應用則是將數位媒介視為重要資料傳遞時的媒介，透過數位媒介的包裝，該資料可以很安全的送達目的地，即使數位媒介被有心人攔截，重要資料也不容易被解讀，我們稱之為資料嵌入（Data Embedding）。

Fig. 3. Embedding effect on Chinese characters. (a) Original host image. (b) After embedding 1686 bytes by the proposed scheme with block size 8 × 8. (c) After embedding 357 bytes by WL scheme with block size 8 × 8. (d) After embedding 297 bytes by the proposed scheme with block size 32 × 32. (e) After embedding 29 bytes by WL scheme with block size 16 × 16. (f) After embedding 357 bytes by the proposed scheme with block size 28 × 28. (g) After embedding 357 bytes by WL scheme with block size 8 × 8.


As dig
security-re
central issu
encryption
(a)
(b)
(c)
(d)
(e)
(f)
(g)

As digital media are getting wider popularity, their security-related issues are becoming a greater concern. One central issue is *confidentiality*, which is typically achieved by *encryption*. However, as an encrypted message usually flags the importance of the message, it also attracts cryptanalysts' interests. The sometimes confusing terminology *stagenography* has a different flavor from encryption; its purpose is to embed a piece of critical information in a non-critical host message (e.g., webpages, advertisements, etc.) to distract opponents' attention [7, 12]. One less confusing name for steganography would be *data hiding*. It should be understood that steganography is orthogonal to encryption, and it may be combined with encryption to achieve a higher level of security.

Fig. 4. Embedding effect on English characters. (a) Original host image. (b) After embedding 1650 bytes by the proposed scheme with block size 8 × 8. (c) After embedding 348 bytes by WL scheme with block size 8 × 8. (d) After embedding 340 bytes by the proposed scheme with block size 32 × 32. (e) After embedding 122 bytes by WL scheme with block size 16 × 16. (f) After embedding 344 bytes by the proposed scheme with block size 32 × 32. (g) After embedding 344 bytes by WL scheme with block size 8 × 8.

Two host images were tested, as shown in Figs. 3(a) and 4(a). Also, the image quality after data embedding is taken into account by making two slight enhancements. First, pixels around black-and-white margins are altered with a higher priority. Second, if a block $F_i$ is completely black or white, no data will be concealed in it because changing any bit in $F_i$ is easily visible. To avoid confusion resulting from this enhancement, a block $F_i$ which is not completely black or white, but which will become completely black or white when being hidden with data, is not used for concealing data. However, this block is still converted into a completely black or white block to be transmitted (based on our scheme, 2 bits, at most, of $F_i$ will be modified). Consequently, when the receiver receives a completely black or white block, this block is regarded as containing no hidden data. Our simulation experience indicates that the data-hiding ratio is only slightly affected by these enhancements, because many choices are typically available to modify a block.

We conclude our comparisons and observations in the following.

1) *Equal Block Size:* We use the same block size and compare images' quality after data hiding. The results are in parts (b) and (c) of Figs. 3 and 4, where the block size is 8 × 8. Our results are noisier, since as many as 2 bits in each block are modified, compared to 1 bit of the WL's. In this case, image quality is traded for a higher data-hiding ratio. In general, our scheme can conceal about four-to-ten times more data than that of WL's.

2) *Equal Image Quality:* This experiment attempts to equalize the image quality by adjusting the block size. The WL scheme will modify, on average, 0.5 bit in each block hidden with data. The same image quality can be maintained by using a block size that is four times larger than that used in the WL scheme. Thus, in the worst case, 2 bits are modified in each of our blocks, or equivalently $2/4 = 0.5$ bit in each of the WL blocks. Based on this assumption, the experimental results are summarized in parts (d) and (e) of Figs. 3 and 4, where the block size is $16 \times 16$ for WL's scheme and $32 \times 32$ for our scheme. In this case, the WL scheme can embed, at most, 1 bit in each $16 \times 16$ block, and ours $\lfloor \log(32^2 + 1) \rfloor = 10$ bits in each $32 \times 32$ block. Our data-hiding ratio is at least 2.5 higher than that of WL.

3) *Equal Amount of Embedded Data:* Here, the amount of embedded data is further equalized by adjusting the block sizes to compare the image quality after data hiding in the WL scheme and the proposed scheme. These results are summarized in parts (f) and (g) of Figs. 3 and 4. Notably, since the hiding ratio of the WL scheme depends on the nature of the host image, we have to adjust the block sizes in order to embed approximately the same amount of hidden data for a fair comparison. Specifically, the block sizes used in Figs. 3(f), 3(g), 4(f), and 4(g) are $28 \times 28$, $8 \times 8$, $32 \times 32$, and $8 \times 8$, respectively. In this case, our scheme delivers a better image quality than the WL scheme.

## IV. Conclusion

This letter has presented a novel steganography scheme capable of concealing a large amount of data in a binary image. The proposed scheme has the following features: it uses a secret key and a weight matrix to protect the hidden data, it uses a weight matrix to increase the data-hiding ratio, and it uses an XOR operator to increase the security. One future research direction is to account for human visual effects during the data embedding process.

## References

[1] R. J. Anderson, “Stretching the limits of steganography,” in *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, 1996, pp. 39–48.

[2] R. J. Anderson and F. A. P. Petitcolas, “On the limits of steganography,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 474–481, May 1998.

[3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” *IBM Syst. J.*, vol. 35, no. 3–4, Feb. 1996.

[4] Y.-Y. Chen, H.-K. Pan, and Y.-C. Tseng. (2000) A secure data hiding scheme for binary images. CSIE Dept., Nat. Chiao-Tung Univ. [Online]. Available: http://www.csie.nctu.edu.tw/~yctseng

[5] E. Franz *et al.*, “Computer-based steganography,” in *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, 1996, pp. 7–21.

[6] D. Gruhl and W. Bender, “Information hiding to foil the casual counterfeiter,” in *Proc. Workshop Information Hiding, IH'98*, Portland, OR, Apr. 1998.

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

[8] D. Kohn, *The Codebreakers: The Story of Secret Writing*. New York: Scribner, 1996.

[9] M. Pierrot-Deseilligny and H. Le-Men, “An algorithm for digital watermarking of binary images, application to map and text,” presented at the Int. Workshop Comput. Vision, Hong Kong, China, Sept. 1998.

[10] G. J. Simmons, “The prisoners' problem and the subliminal channel,” in *Proc. CRYPTO'83*, 1983, pp. 51–67.

[11] ——, “Results concerning the bandwidth of subliminal channels,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 463–473, May 1998.

[12] ——, “The history of subliminal channels,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 452–462, May 1998.

[13] W. Stallings, *Cryptography and Network Security*. Englewood Cliffs, NJ: Prentice-Hall, 1999.

[14] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” in *Proc. IEEE Int. Conf. Image Processing*, vol. 2, 1994, pp. 86–90.

[15] M. Wu, E. Tang, and B. Liu, “Data hiding in digital binary image,” presented at the IEEE Int. Conf. Multimedia and Expo, ICME'00, New York, 2000.

[16] M. Y. Wu and J. H. Lee, “A novel data embedding method for two-color facsimile images,” in *Proc. Int. Symp. Multimedia Inform. Processing*, Chung-Li, Taiwan, R.O.C, Dec. 1998.

[17] J. Zhao and E. Koch, “Embedding robust labels into images for copyright protection,” in *Proc. Int. Conf. Intellectual Property Rights for Inform., Knowledge, New Techniques*, Munich, Germany, 1995, pp. 242–251.