International Journal of Computational Intelligence Systems, Vol. 6, No. 4 (July, 2013), 639-647

Cryptographic Secrecy Analysis of Matrix Embedding

Jiayong Chen [a,b*] **Jiufen Liu** [a] **Weiming Zhang** [a,c] **Huisheng Liu** [a] **Xianfeng Zhao**[d]

[a] *Department of Information Research, Zhengzhou Information Science and Technology Institute, 7 Jianxue Road Zhengzhou, 450002, China*
[b] *School of Information Science and Technology, Xiamen University, 422 Simingnan Road Xiamen, 361005, China*
[c] *School of Information Science and Technology, University of Science and Technology of China, 96 Jinzhai Road Hefei, 230026, China*
[d] *Institue of Information Engineering, Chinese Academy of Sciences, 89 Minzhuang Road Beijing 100093, China*
E-mail: cjy1003@sina.com, jiufen_liu@163.com, weimingzhang@shu.edu.cn, huisheng_liu@163.com, xianfengzhao@163.com

Received 10 December 2011; accepted 15 February 2013

Abstract

For good security and large payload in information hiding, matrix embedding is a popular method for increasing the embedding efficiency. This paper analyzes the security of matrix embedding against cryptanalytic attacks. The secrecy security of matrix embedding using information theory under the conditions of known-cover attack and chosen-stego attack is studied. After that, the unicity distance of the key, message equivocation and the relationship among wet ratio, embedding rate and key equivocation for the wet paper channel are given through analyzing the key model under the known-cover attack condition. Furthermore, an effective differential attack to matrix embedding under chosen-stego attack condition is proposed. The results of analysis show that the matrix embedding is not secure enough with respect to cryptographic secrecy against the stronger adversaries.

Keywords: matrix embedding; known-cover attack; chosen-stego attack; stego-only attack; message equivocation; key equivocation

1. Introduction

The Internet of things (Iot) is a large network which integrates the current devices including Radio Frequency Identification (RFID) devices, sensors and other equipments and services etc. The Iot has an effect on the security and privacy of the involved stakeholders. In [1] and [2], the current technological and their effect on the security, privacy, and governance of Iot are discussed. With the extensive application of RFID technology, particularly people pay more and more attention to its security and privacy issues. Currently, security issues have become major factors which impede the large-scale applications of RFID technology. Security and privacy in RFID systems have been defined as [3].

Information hiding is one of the hot spots in the domain of information security, of which steganography and watermarking are the main branches. In recent years, information hiding techniques have been introduced to enhance the security of RFID systems. In [4], ID Modulation is used to embed a bit stream representing sensor information in a standards-compliant RFID channel, which is backward compatibility with pre-existing standards and hardware. In [5], a novel watermarking based on tamper detection solution for low cost RFID passive tags which use the 32 bit kill password as the cover medium is proposed. Most previous applications of information hiding (eg. matrix embedding) have emphasized either concealment security (as in steganography) or robustness to removal (as in watermarking). For good security and large

payload in steganography, it is desired to embed as many messages as possible per change of the cover-object, i.e., to have high embedding efficiency.

Matrix embedding is the most popular method for increasing the embedding efficiency. Matrix embedding was firstly proposed by Crandall in [6], applied in F5 algorithm [7] and systematically investigated in [8,9]. In recent years, many matrix embedding methods based on structured covering codes [10,11] or random linear codes [12,13] have been reported to increase the embedding efficiency and enhance the concealment security of steganography.

Traditionally, steganography only consider the concealment security of matrix embedding, i.e., how to resist the detection from the attacker in [14]. However, after determining the stego image, the attacker will further try to recover the stego key and extract the hidden messages, which will produce enough evidence in support of the existence of steganography. We call the ability of steganography to protect the stego key and message content as secret security.

Phillip firstly studied the secrecy security of matrix embedding under the condition of stego-only attack in [15]. Based on message equivocation and key equivocation, he studied the secrecy security of matrix embedding under various key models. So far, recent work in matrix embedding mainly focused on the security under the condition of stego-only attack.

Note that recovering the stego key or extracting the hidden messages is a very difficult problem, which is impossible unless the attacker get enough conditions, such as all details of the steganographic algorithm, many stego images generated from one common cover or the cover itself. In fact, the secret security of steganography is similar to the security of cryptography. According to the Kerckhoffs' principle，if the attacker can get some information base on any other assumption except knowing the key, such security is not reliable.

Therefore, it is necessary to consider the secrecy security of steganography under strong attack conditions, such as the known-cover attack, because we cannot build secret security by supposing that the attack cannot get the cover. In practice, the condition of known-cover is possible. For instance, if the attacker obtains the computer of the steganographers, e.g., the case of Russian spies in [16, 17], he may get the stego systems, the cover images and the stego images. After obtaining the cover, it is easy for the attacker to detect the existence of the steganography, but it is still hard to recover the stego key and extract the hidden message. Therefore, the secrecy security of matrix embedding under the stronger attack condition, such as known-cover should be considered by both steganographers and attackers.

In this paper, we discuss the secrecy security of matrix embedding against cryptanalytic attacks. Based on the results in [15], we further study the secrecy security of matrix embedding using information theory under the condition of known-cover attack and chosen-stego attack.

The contributions of this paper lie in the following three aspects:

(i) To the best of our known, this paper firstly studies the secrecy security of matrix embedding under the condition of known-cover attack which has become a real-world steganalysis under some special attacking conditions.

(ii) For wet paper channel, this paper shows the relationship among wet ratio, embedding rate, and key equivocation for the wet paper channel under the known-cover attack condition.

(iii) This paper presents an effective differential attack to matrix embedding under chosen-stego attack, which can recover the key by using some groups of differential equations.

The rest of this paper is organized as follows. Section 2 introduces the concepts of matrix embedding and wet paper codes, as well as some notations used in this paper. All

main results are in Section 3. Section 4 summarizes this paper briefly.

2. The Presentation of Problem

2.1. Symbols

Throughout the text, italic capital letters denote random variables, and boldface small letters denote the instances of random variables. Let Σ be the finite set of letters, Σ^n be a sequence of Σ, the length of which is n. Note that S is the cover sequence, C is the stego sequence, K is the shared key between the sender and recipient, M is the secret message, T is the way used to choose the embedding positions. Security referred behind represents the secrecy security.

Considering that both communication sides use matrix embedding to transfer secret message such as digital images, audios, and videos on the multimedia channel. Figure 1 demonstrates the flow chart of communication.

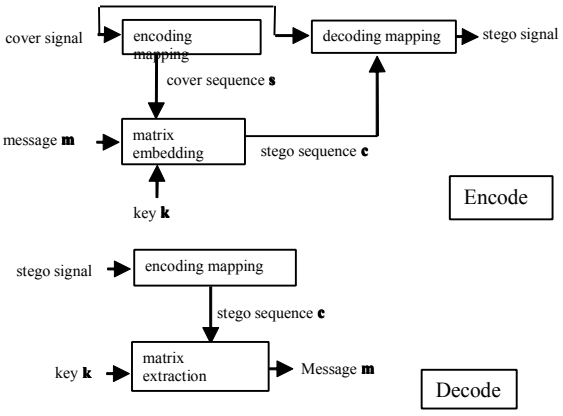

Figure. 1 information hiding system using matrix embedding

Assume that the sender wants to transfer binary message sequence $\mathbf{m}(\mathbf{m} \in F_2^q)$ with q bits. The sender first maps the cover signals to a binary cover sequence $\mathbf{s}(\mathbf{s} \in F_2^n)$ with length n such that $0<q\leq n$ by using the encoding mapping. Thus, with a binary random matrix $\mathbf{k}$ as the stego key, the sender embeds the message $\mathbf{m}$ into $\mathbf{s}$ and gets the stego sequence $\mathbf{c}(\mathbf{c} \in F_2^n)$, satisfy $\mathbf{m}=\mathbf{kc}$. The stego sequence $\mathbf{c}$ is then used to generate the stego signals. After receiving the stego signals, the recipient obtains the stego sequence $\mathbf{c}$ by using the decoding mapping, and extracts the secret message $\mathbf{m}$ by multiplying $\mathbf{c}$ by the stego key $\mathbf{k}$, such that $\mathbf{m}=\mathbf{kc}$. For example, it is the common form of encoding mapping getting the Least Significant Bits (LSB) sequence of the cover signal, and using the stego sequence to take the place of the LSB sequence of the cover signal is the common form of the corresponding decoding mapping.

As for a good encoding mapping function, the 2^n instances of the cover$\mathbf{s}$ are equiprobable. Assume that the message has been compressed, and then the 2^q instances of the message are equiprobable. The key $\mathbf{k}$ is a random matrix on $F_2^{q\times n}$.

The entropy function is denoted by $H(\cdot)$ as follows

$$H(S) = \sum_{\mathbf{s}\in F_2^n} \Pr(\mathbf{s}) \log_2 \Pr(\mathbf{s}).$$

The mutual information is defined as $I(\cdot)$, where

$$I(M,C) = \sum_{\mathbf{m}\in F_2^n} \sum_{\mathbf{c}\in F_2^n} \Pr(\mathbf{m},\mathbf{c}) \log_2 \frac{\Pr(\mathbf{m},\mathbf{c})}{\Pr(\mathbf{m})\Pr(\mathbf{c})}.$$

As for the zero-distortion channel, the channel capacity is defined as $C=H(C|S)$, and the information transfer rate is defined as $R_m=H(M)/n$. Define $H(C|S)$-$H(M)$ as **embedding redundancy**. The **unicity distance** to a stegosystem is the number of signals needed by the attacker to make the expectation of the number of pseudo-keys equal to zero. The attacker maybe use only cipher texts or both cipher texts and plaintexts for different attacking conditions.

A binary $[n,k]$ matrix embedding C is a linear subspace of F_2^n. Given the key $\mathbf{k}$, define the rank of $\mathbf{k}$ as q, and $\mathbf{k}$ is full-rank. Then for any $\mathbf{b} \in F_2^n$, the vector $\mathbf{g}=\mathbf{kb} \in F_2^n$ is called the syndrome of $\mathbf{b}$. The set $C(\mathbf{m}) = \{\mathbf{b} \in F_2^n \mid \mathbf{m} \equiv \mathbf{kb} (\mathrm{mod}\, 2)\}$ is called a coset. The cosets associated with different syndromes are disjoint. Therefore, there are 2^{n-k} disjoint cosets, with each consisting of 2^k vectors. Let $w(\mathbf{s})$ be the Hamming weight of the vector $\mathbf{s}$, and $d(\mathbf{s},\mathbf{c})$ be the Hamming distance between vectors $\mathbf{s}$ and $\mathbf{c}$. Let $e(\mathbf{m})$ be a coset leader, if $e(\mathbf{m})$ satisfy

$$w(e(\mathbf{m})) = \min\{w(\mathbf{b}) \mid \mathbf{b} \in C(\mathbf{m})\}.$$

2.2. Matrix embedding

Matrix embedding is a typical application of linear covering codes, which is proposed to improve the embedding efficiency of information hiding. Using matrix embedding, we can embed message $\mathbf{m}$ with q

bits into a binary cover sequence **s**. The embedding algorithm *Emb*() is such that

$$Emb(\mathbf{s},\mathbf{m},\mathbf{k}) = \mathbf{s} + e(\mathbf{m}-\mathbf{ks}) = \mathbf{c}.$$

The corresponding extracting algorithm *Ext*() is as follows

$$Ext(\mathbf{c},\mathbf{k}) = \mathbf{kc},$$

where

$$\mathbf{kc} = \mathbf{ks} + \mathbf{k}e(\mathbf{m}-\mathbf{ks}) = \mathbf{ks} + \mathbf{m} - \mathbf{ks} = \mathbf{m}.$$

Because **m** follows the uniform distribution, the average change number needed for the embedding process is equal to the average Hamming weight of all the coset leaders of a code *C*. The average change number is equal to the average distance to code. The distance of two arbitrary code words of the same coset to the code is equivalent, both equal to the Hamming weight of any coset leader of the coset, i.e. $d(\mathbf{s},C) = d(\mathbf{c},C) = w(e)$. Consequently, the average distance R_s of all the code words is equal to the average number of embedding changes, i.e.

$$R_s = \frac{1}{2^n}\sum_{\mathbf{s}\in F_2^n} d(\mathbf{s},C) = \frac{1}{2^{n-k}}\sum_{i=1}^{2^{n-k}} w(e(\mathbf{s})).$$

2.3. Wet paper codes

Wet paper codes were previously proposed as a tool for the construction of steganographic schemes with arbitrary (non-shared) selection channels.

Using wet paper codes, the sender can embed message into a cover when the position of the cover is restricted to be not changed, while the receiver can extract message without the information of the restricted positions.

Assume that the sender chooses *l* changeable bits s_j, $j \in L \subset \{1,2,\cdots n\}$, $|L| = l$, from a binary cover **s**= (s_1,..., s_n), while the remaining *n*-*l* bits cannot be changed. The changeable position is called dry position and the unchangeable position is called wet positions. The sender embeds the message into **s** by changing some $s_j, j \in L \subset \{1,2,\cdots n\}$ and gets **c**, which satisfy

$$\mathbf{kc}=\mathbf{m}. \quad (1)$$

Let **v**=**c**-**s**, then

$$\mathbf{kv}= \mathbf{m}-\mathbf{ks}. \quad (2)$$

Since *n*-*l* position of **s** is not allowed to change, there are *l* unknown v_j, $j \in L \subset \{1,2,\cdots n\}$, while the remaining *n*-*l* values v_i, $i \notin L$, are zeros. Thus, we can remove *n*-*l* unused columns from **k**, and denote the obtained matrix as **h**. We also remove *n*-*l* unused elements from **v**, and denote the obtained vector as **u**. We get the following equation from (2)

$$\mathbf{hu}= \mathbf{m}-\mathbf{ks}, \quad (3)$$

where **h** is a binary $q\times l$ matrix and **u** is an unknown $l\times 1$ binary vector. The encoding of wet paper codes is completed by solving (3). The wet rate of the cover is denoted as $\alpha_{wet} = (n-l)/n$, where $0 \le \alpha_{wet} < 1$. The embedding rate of wet paper codes is denoted as $r_{wet} = q/l$. In fact, the random matrix embedding can be viewed as one of the special wet paper codes, of which the wet rate is 0.

3. Secrecy security analysis

The secrecy security of matrix embedding under the conditions of stego-only attack has been studied in [15]. This paper focuses mainly on the security under the conditions of known-cover attack and chosen-stego attack separately.

3.1. Key equivocation

Theorem 1.([15]) *Under the condition of stego-only attack, the key equivocation function of matrix embedding is bounded as*

$$I(K;C) \le [q - H(M)] + [H(C) - H(S)].$$

Theorem 1 indicates that, under the condition of stego-only attack, if the embedded message has been compressed, i.e. $H(M) = q$, and the cover sequence obtained by the encoding mapping is random, i.e. $H(S) = n$, then $H(C) = n = H(S)$ and $I(K;C) = 0$. Here matrix embedding can achieve the perfect secrecy.

Now we extend Philip's theorem to known-cover attack.

Lemma 1. *Under the condition of known-cover attack, we have*

$$I(T;K,C,S,M) \ge \phi(n,q) \ge 0,$$

where $\phi(n,q) = q + \log C_n^q - \log \sum_{i=0}^{q} C_q^i C_{n-i}^{q-i}$.

Proof. Considering $I(T;K,C,S,M)$, both the way of choosing embedding position T and the embedded message M are independent of the key K, so the receiver can extract M using stego object S without T. Thus, for any given S, we have

$$\begin{aligned} I(T;K,C,S,M) &= I(T;C,S) \\ &= H(T) - H(T \mid C,S), \end{aligned}$$

where

$$H(T) = \sum_{t \in T} \Pr(\mathbf{t}) \log \frac{1}{\Pr(\mathbf{t})} = \log C_n^q .$$

The information about the way of choosing embedding positions T can only be obtained by comparing the difference between the cover object C and stego object S, consequently

$$\begin{aligned} H(T \mid C,S) &= \sum_{c,s} \Pr(\mathbf{c} \oplus \mathbf{s}) H(T \mid \mathbf{c} \oplus \mathbf{s}) \\ &= \sum_{i=0}^{q} \Pr(w(\mathbf{c} \oplus \mathbf{s}) = i) H(T \mid w(\mathbf{c} \oplus \mathbf{s}) = i). \end{aligned}$$

Because $\mathbf{c}$ is random on F_2^n , and the Hamming weight of $\mathbf{c} \oplus \mathbf{s}$ is $w(\mathbf{c} \oplus \mathbf{s})$. Then

$$\Pr(w(\mathbf{c} \oplus \mathbf{s}) = i) = \frac{C_n^i C_{n-i}^{q-i}}{\sum_{j=0}^{q} C_n^j C_{n-j}^{q-j}} = \frac{C_n^i C_{n-i}^{q-i}}{C_n^q \sum_{j=0}^{q} C_q^j} = \frac{C_n^i C_{n-i}^{q-i}}{C_n^q 2^q},$$

$$H(T \mid w(\mathbf{c} \oplus \mathbf{s}) = i) = \log C_{n-i}^{q-i} .$$

As $\sum_{i=0}^{q} \frac{C_n^i C_{n-i}^{q-i}}{C_n^q 2^q} = 1$, according to **Jensen Inequation** in [18], we have

$$\begin{aligned} H(T \mid \mathbf{c} \oplus \mathbf{s}) &= \sum_{i=0}^{q} \frac{C_n^i C_{n-i}^{q-i}}{C_n^q 2^q} \cdot \log C_{n-i}^{q-i} \\ &\le \log \left(\frac{\sum_{i=0}^{q} C_n^i C_{n-i}^{q-i} C_{n-i}^{q-i}}{C_n^q 2^q} \right) = \log \left(\frac{C_n^q \sum_{i=0}^{q} C_q^i C_{n-i}^{q-i}}{C_n^q 2^q} \right) \\ &= \log \sum_{i=0}^{q} C_q^i C_{n-i}^{q-i} - q. \end{aligned}$$

Then

$$\begin{aligned} I(T;K,C,S,M) &= H(T) - H(T \mid \mathbf{c} \oplus \mathbf{s}) \\ &\ge q + \log C_n^q - \log \sum_{i=0}^{q} C_q^i C_{n-i}^{q-i} \triangleq \phi(n,q). \end{aligned}$$

According to **Vandermonde Identical Equation** in [18], $\sum_{i=0}^{n} C_n^i \cdot C_m^{k-i} = C_{n+m}^k$, for $0 \le i \le q$, we have

$$0 = q + \log C_n^q - \log \sum_{i=0}^{q} C_q^i C_{n-q}^{q-i} < \phi(n,q),$$

$$\phi(n,q) < q + \log C_n^q - \log \sum_{i=0}^{q} C_q^i C_n^{q-i} = q.$$

As a result, $0 \le \phi(n,q) \le I(T;K,C,S,M)$.

Theorem 2. *Under the condition of known-cover attack, the key equivocation function of matrix embedding is bounded as*

$$I(K;S,C) \le [H(C \mid S) - H(M)] - \phi(n,q) .$$

Specially, I(K;S,C) achieves the maximum value when $q = n/2$.

Proof. For the proof, firstly we have

$$\begin{aligned} & H(C,K,M,T,S) \\ &= H(K,M,T,S) + \underbrace{H(C \mid K,M,T,S)}_{=0} \\ &= H(K) + H(M) + H(S) + H(T). \end{aligned} \tag{4}$$

At the same time,

$$\begin{aligned} & H(C,K,M,T,S) \\ &= H(C) + H(S \mid C) + H(K \mid C,S) + \underbrace{H(M \mid K,C,S)}_{=0} \\ &\quad + H(T \mid K,C,S,M) \\ &= H(C) + H(S \mid C) + H(K \mid C,S) + H(T \mid K,C,S,M). \end{aligned} \tag{5}$$

As a result,

$$\begin{aligned} & H(K) + H(M) + H(S) + H(T) \\ &= H(C) + H(S \mid C) + H(K \mid C,S) + H(T \mid K,C,S,M), \end{aligned}$$

and

$$\begin{aligned} & [H(S) - H(S \mid C)] + [H(K) - H(K \mid C,S)] \\ &\quad + [H(T) - H(T \mid K,C,S,M)] \\ &= H(C) - H(M). \end{aligned}$$

As

$$\begin{cases} I(C;S) = H(S) - H(S \mid C) \\ I(K;C,S) = H(K) - H(K \mid C,S) \\ I(T;K,C,S,M) = H(T) - H(T \mid K,C,S,M), \end{cases}$$

we have

$$I(C;S) + I(K;C,S) + I(T;K,C,S,M) = H(C) - H(M).$$

Then, according to Lemma 1,

$$\begin{aligned} I(K;C,S) &= H(C) - H(M) - I(C;S) - I(T;K,C,S,M) \\ &= H(C \mid S) - H(M) - I(T;K,C,S,M) \\ &\le [H(C \mid S) - H(M)] - \phi(n,q). \end{aligned} \quad (6)$$

For fixed n, we obtain following conclusions.

(iv) When $r \to 0$ or $r \to 1$, the key equivocation achieves the maximal upper bound, which is close to the hidden capacity;

(v) When $r \to 0.5$, the key equivocation achieves the minimal upper bound.

We make a theoretical analysis of the relation between the embedding rate r_{wet} of wet paper codes and the key equivocation $I(K;C,S)$ for different wet rate α_{wet}. Generally speaking, we have

(vi) When $0.5 \le \alpha_{wet} < 1$, if $r_{wet} = 1$, the key equivocation achieves the minimum value; if $r_{wet} \to 0$, the key equivocation achieves the maximum value and is close to the embedding redundancy.

(vii) When $0 \le \alpha_{wet} < 0.5$, if $r_{wet} = 0.5(1 - \alpha_{wet})$, the key equivocation achieves the minimum value; if $r_{wet} \to 0$, the key equivocation achieves the maximum value and is close to the embedding redundancy.

(viii) When $\alpha_{wet} = 0$, if $r_{wet} = 0.5$, the key equivocation achieves the minimum value; if $r_{wet} \to 0$, the key equivocation achieves the maximum value and is close to the embedding redundancy.

Theorem 2 indicates that the channel redundancy should be increased as much as possible to improve the secrecy of matrix embedding. In order to decrease the key equivocation, the sender should choose a suitable embedding rate according to the wet rate.

3.2. Unicity distance

Theorem 3. *Under the condition of stego-only attack, unicity distance of the key* $\mathbf{k}$*, i.e., the expected number of stego signals* N *for determining the key, has the following lower bound*

$$N \ge \frac{H(K) - q}{H(C) - [H(M) + H(S)]}.$$

Proof. According to Theorem 1,

$$\begin{aligned} &H(S \mid K,C,T) \\ &= H(K) - H(K \mid C) + I(T;K,C) + H(M) + H(S) - H(C), \end{aligned}$$

where $H(S \mid T,K,C) \le q$ and $I(T;K,C) = 0$.

Thus we have

$$\begin{aligned} H(K \mid C) &= H(K) + H(M) + H(S) - H(C) - H(S \mid T,K,C) \\ &\ge H(K) + H(M) + H(S) - H(C) - q. \end{aligned}$$

Denote N groups of stego objects as $\mathbf{c}^N = \{\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_N\}$, and then

$$H(\mathbf{k} \mid \mathbf{c}^N) \ge H(K) + N[H(M) + H(S) - H(C)] - q.$$

So we have

$$\log(\overline{K_p} + 1) \ge H(K) + N[H(M) + H(S) - H(C)] - q.$$

At the same time,

$$\overline{K_p} \ge 2^{H(K) - q + N[H(M) + H(S) - H(C)]} - 1.$$

So unicity distance is

$$N \ge \frac{H(K) - q}{H(C) - [H(M) + H(S)]}.$$

Theorem 4. *Under the condition of known-cover attack, unicity distance of the key* $\mathbf{k}$ *is upper bounded as*

$$N \ge \frac{H(K)}{H(C \mid S) - [H(M) + I(T;M,C,S,K)]}.$$

Proof. Denote N groups of covers and stego objects as $\mathbf{s}^N = \{\mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_N\}$ and $\mathbf{c}^N = \{\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_N\}$ respectively. Given N pairs of covers and stego objects, the set of all the possible stego keys is

$K(\mathbf{c}^N, \mathbf{s}^N) = \{\mathbf{k} \in K \mid \exists \mathbf{m}_i \in M, \mathbf{t}_i \in T, \Pr(\mathbf{m}_i) > 0 \text{ and } \mathbf{kc}_i = \mathbf{m}_i\}$.

And the expectation of the number of pseudo-keys is

$$\begin{aligned} \overline{K_p} &= \sum_{(\mathbf{c}^N, \mathbf{s}^N) \in (C^N, S^N)} \Pr(\mathbf{c}^N, \mathbf{s}^N)[K(\mathbf{c}^N, \mathbf{s}^N) - 1] \\ &= \sum_{(\mathbf{c}^N, \mathbf{s}^N) \in (C^N, S^N)} \Pr(\mathbf{c}^N, \mathbf{s}^N) K(\mathbf{c}^N, \mathbf{s}^N) - 1. \end{aligned}$$

We have

$$\begin{aligned} & H(K \mid \mathbf{c}^N, \mathbf{s}^N) \\ &= \sum_{(\mathbf{c}^N, \mathbf{s}^N) \in (C^N, S^N)} \Pr(\mathbf{c}^N, \mathbf{s}^N) H(K \mid \mathbf{c}^N, \mathbf{s}^N) \\ &\le \log \sum_{(\mathbf{c}^N, \mathbf{s}^N) \in (C^N, S^N)} \Pr(\mathbf{c}^N, \mathbf{s}^N) \mid K(\mathbf{c}^N, \mathbf{s}^N) \mid \\ &= \log(\overline{K_p} + 1), \end{aligned}$$

and $H(C \mid K, M, T, S) = 0$.

On the other hand,

$$\begin{aligned} & H(\mathbf{c}^N, \mathbf{s}^N, \mathbf{m}^N, \mathbf{t}^N, \mathbf{k}) \\ &= H(\mathbf{s}^N, \mathbf{m}^N, \mathbf{t}^N, \mathbf{k}) + \underbrace{H(\mathbf{c}^N \mid \mathbf{s}^N, \mathbf{m}^N, \mathbf{t}^N, \mathbf{k})}_{=0} \qquad (7) \\ &= N[H(S) + H(M) + H(T)] + H(K). \end{aligned}$$

Thus,

$$\begin{aligned} & H(\mathbf{c}^N, \mathbf{s}^N, \mathbf{m}^N, \mathbf{t}^N, \mathbf{k}) \\ &= H(\mathbf{s}^N) + H(\mathbf{c}^N \mid \mathbf{s}^N) + H(\mathbf{k} \mid \mathbf{c}^N, \mathbf{s}^N) + H(\mathbf{m}^N \mid \mathbf{c}^N, \mathbf{s}^N, \mathbf{k}) \\ &\quad + H(\mathbf{t}^N \mid \mathbf{m}^N, \mathbf{c}^N, \mathbf{s}^N, \mathbf{k}) \qquad (8) \\ &\le NH(S) + NH(C \mid S) + H(\mathbf{k} \mid \mathbf{c}^N, \mathbf{s}^N) + H(\mathbf{t}^N \mid \mathbf{m}^N, \mathbf{c}^N, \mathbf{s}^N, \mathbf{k}) \\ &\le N[H(S) + H(C \mid S) + H(T) - I(T; M, C, S, K)] + H(\mathbf{k} \mid \mathbf{c}^N, \mathbf{s}^N). \end{aligned}$$

From equation (7) and equation (8),

$$H(\mathbf{k} \mid \mathbf{c}^N, \mathbf{s}^N) \ge H(K) - N[H(C \mid S) - H(M) - I(T; M, C, S, K)].$$

Then

$$\log(\overline{K_p} + 1) \ge H(K) - N[H(C \mid S) - H(M) - I(T; M, C, S, K)].$$

Consequently, the expected number of pseudo-keys is

$$\overline{K_p} \ge H(\mathbf{k} \mid \mathbf{c}^N, \mathbf{s}^N) \ge 2^{H(K) - N[H(C \mid S) - H(M) - I(T; M, C, S, K)]} - 1.$$

So unicity distance has following upper bound

$$N \ge \frac{H(K)}{H(C \mid S) - [H(M) + I(T; M, C, S, K)]}.$$

3.3. Message equivocation

Theorem 5.([15]) *Under the condition of stego-only attack*, (1) *The message equivocation of the uniform permutation model is* $I(M; C) = 2^{-n} q$. (2) *The message equivocation of the Bernoulli key model with sufficiently large* nq is $I(M; C) = 2^{-n} nqH_2(p)$, *where* $H_2(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ *is the binary entropy function.*

Now we extend Theorem 5 to known-cover attack model as follows.

Theorem 6. *Under the condition of known-cover attack, the message equivocation function is bounded as*

$$I(M; S, C) \le H(C \mid S) - [I(K; M, C) + \phi(n, q)],$$

where $\phi(n, q) = q + \log C_n^q - \log \sum_{i=0}^{q} C_q^i C_{n-i}^{q-i}$, *and* (1) *For the uniform permutation model*,

$$I(K; M, C) = q - 2^{-n} q.$$

(2) *For the Bernoulli key model*,

$$I(K; M, C) \approx -2^{-n} nqH_2(p).$$

Proof. We have

$$I(M; S, C) = H(M) - H(M \mid S, C)$$

And

$$\begin{aligned} & H(C, K, M, T, S) \\ &= H(S) + H(C \mid S) + H(M \mid C, S) \qquad (9) \\ &\quad + H(K \mid M, C, S) + H(T \mid M, C, S, K), \end{aligned}$$

$$H(C, K, M, T, S) = H(S) + H(K) + H(M) + H(T). \qquad (10)$$

From Equation (9) and Equation (10),

$$\begin{aligned} & H(M) - H(M \mid S, C) \\ &= H(C \mid S) + H(K \mid M, S, C) + H(T \mid M, C, S, K) \\ &\quad - H(T) - H(K), \end{aligned}$$

and

$$I(M; S, C) = H(C \mid S) - I(K; M, S, C) - I(T; M, C, S, K).$$

Thus,

$$I(T; M, C, S, K) \ge \phi(n, q),$$

$$I(K; M, S, C) \ge I(K; M, C),$$

$$\begin{aligned} I(M; S, C) &\le H(C \mid S) - I(K; M, S, C) - \phi(n, q) \\ &\le H(C \mid S) - I(K; M, C) - \phi(n, q). \end{aligned}$$

According to Theorem 2 in [15], for the uniform permutation model,

$$I(K; M, C) = q - 2^{-n} q.$$

Thus,

$$I(M; S, C) \le H(C \mid S) - q + 2^{-n} q - \phi(n, q).$$

For the Bernoulli key model,

$$I(K;M,C) \approx 2^{-n} nqH_2(p).$$

Thus,

$$I(M;S,C) \le H(C \mid S) - 2^{-n} nqH_2(p) - \phi(n,q),$$

where $p = \Pr(K_{ij} = 1) = 1 - \Pr(K_{ij} = 0)$.

Theorem 6 indicates that for both the uniform permutation model and the Bernoulli key model, the message equivocation achieves the upper bound when the embedding rate $r \to 0$.

3.4. Differential attack

Theorem 7. *Under the condition of chosen-stego attack, the attacker can recover the key by using n groups of differential equations.*

Proof. Assume that by some way the attacker has already known that wet paper codes are used to transfer the secret message, and can be viewed as an encryption algorithm. Take the message block as plaintext and the stego block as cipher text, wet paper codes can be viewed as a block cipher, because the sender uses the same key $\mathbf{k}$ to encrypt different blocks of plaintexts. The only goal of the attacker is to recover the key $\mathbf{k}$. Assume that the attacker has already had many plaintext-cipher text pairs, and could choose the needful stego block $\mathbf{c}$ and the corresponding message group $\mathbf{m}$, which amounts to making a chosen-cipher text attack.

Then an attack is given under the above condition that some information of the key is obtained by using differential attack and a group of equivalent keys are found by solving a group of linear equations.

The following operations are discussed on F_2^n. Because the attacker can choose stego objects, he can get two stego objects $\mathbf{c}_1$ and $\mathbf{c}_1'$, where $\mathbf{c}_1 - \mathbf{c}_1' = (1,0,0,\cdots,0)^{\mathbf{T}}$. Let the corresponding messages of two stego objects be $\mathbf{m}_1$ and $\mathbf{m}_1'$ separately, so differential equations can be obtained by

$$\mathbf{kc}_1 - \mathbf{kc}_1' = \mathbf{m}_1 - \mathbf{m}_1'.$$

Since $\mathbf{c}_1 - \mathbf{c}_1' = (1,0,0,\cdots,0)^{\mathbf{T}}$, we have

$$\mathbf{k}(\mathbf{c}_1 - \mathbf{c}_1') = \mathbf{k}_{j,1} = \mathbf{m}_1 - \mathbf{m}_1'.$$

Similarly, for $\mathbf{c}_i - \mathbf{c}_i' = (0,0,\cdots\bar{1},\cdots,0)^{\mathbf{T}}$, we can get differential equations

$$\mathbf{k}_{j,i} = \mathbf{m}_i - \mathbf{m}_i',$$

where $i = 1,2,\cdots,n$. Because the attacker can get q bits of $\mathbf{k}$ by solving a group of equations, only n groups of differential equations need to be constructed, and then the key $\mathbf{k}$ is obtained.

For example, assume that the attacker wants to recover the key $\mathbf{k}$ of matrix embedding under the condition of chosen-stego attack, where

$$\mathbf{k} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Then the attacker could firstly choose two stego sequences $\mathbf{c}_1$ and $\mathbf{c}_1'$, where their differential vector is $(1,0,0,0)^T$. For instance, $\mathbf{c}_1 = (1,1,1,1)^T$ and $\mathbf{c}_1' = (0,1,1,1)^T$. Then, find the corresponding message sequence of $\mathbf{c}_1$ and $\mathbf{c}_1'$. Note that $\mathbf{m}_1 = (0,0,1)^T$ $\mathbf{m}_1' = (1,1,1)^T$. Finally, calculate $\mathbf{m}_1 - \mathbf{m}_1' = (1,1,0)^T$, where $(1,1,0)^T$ the first group of is $\mathbf{k}$. Similarly, $\mathbf{k}$ can be completely recovered by 4 groups of differential equations.

Theorem 7 indicates that secrecy security of matrix embedding is weak under the condition of chosen-stego attack.

4. Conclusion

This paper studies the secrecy security of the matrix embedding schemes under the conditions of known-cover attack by concerning about the message equivocation, key equivocation and unicity distance functions, as well as the relationship among the wet rate, embedding rate and the key equivocation. But it should be pointed out that the mimic cover can not be exactly estimated, and in fact, the restoration of cover object is a difficult problem in information hiding. We also point out that matrix embedding is not secrecy secure under the condition of chosen-stego attack. The current used schemes of fixed shared key for matrix embedding have weak secrecy security against stronger attackers.

Acknowledgments

This work is supported by the Natural Science Foundation of China under Grant [61170234, 60803155], the Strategic Priority Research Program of the Chinese Academy of Sciences [XDA06030601], the National Science and Technology Major Project of China [2010ZX03004-003], Science and Technology Innovation Team of Zhengzhou [10CXTD150].

References

1. V. Oleshchuk, Internet of things and privacy preserving technologies, in *proc. 1st Int. Conf. Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology,* eds. K.E. Skouby(Grimstad, Norway, 2009), pp. 336–340.
2. C.M. Medaglia and A. Serbanati, An Overview of Privacy and Security Issues in the Internet of Things, (Springer, New York, 2010).
3. J. Banks, Understanding RFID Part 9: RFID Privacy and Security, Accessed on February 1, 2009. Available online at http://www. rfidnews.org, 2008.
4. A.N.M. Noman, K. Curran, and T. Lunney, ID modulation: embedding sensor data in an RFID time series, in *Proc. 7th Int. Conf. Information Hiding*, eds. R. J. Anderson(Barcelona, Spain, 2005), pp. 234–246.
5. A.N.M. Noman, K. Curran, and T. Lunney, A watermarking based tamper detection solution for RFID tags, in *Proc. 6th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processin*g, eds. L.C. Jain. (Darmstadt, Germany, 2010), pp. 98-101.
6. R. Crandall, Some Notes on Steganography, *Posted on Steganography Mailing List*, Available online at http://os.inf.tu-dresden.de/~westfeld/crandall.pdf, 1998.
7. A .Westfeld, F5: a steganographic algorithm, in *Proc. 4th Int. Conf. Information Hiding*, eds. I.S. Moskowitz (Pittsburgh, PA, USA, 2001), pp. 289-302.
8. F. Galand and Kabatiansky G, Information hiding by coverings, in *Proc. 3rd Int. Conf. IEEE Information Theory*, eds. S.W. Golomb, G. Gong, T. Helleseth and H.Y. Song (Paris, France, 2003), pp. 151-154.
9. J. Fridrich, P. Lisonek, and D. Soukal, On steganographic embedding efficiency, in *Proc. 8th Int. Conf. Information Hiding*, eds. M. G. Nigotia. (Toronto, Canada, 2006), pp. 282–296.
10. Y.K. Gao, X.L Li and B. Yang, Employing optimal matrix for efficient matrix embedding, in *Proc. 5th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing*, eds. E. Joelianto (Kyoto, Japan, 2009), pp. 161-165.
11. C.L. Hou, C.C. Lu, S.C. Tsai and W.G. Tzeng, An optimal data hiding scheme with tree-based parity check, *J.IEEE Transactions on Image Processing*, 99(9)(2010) 1-7.
12. J. Fridrich and D. Soukal, Matrix embedding for large payloads, *J. IEEE Transactions on Information Forensics Security*, 1(3) (2006) 390–394.
13. J. Fridrich, M. Goljan, and D. Soukal, Wet paper codes with improved embedding efficiency, *J. IEEE Transactions on Information Forensics Security*, 1(1)(2006) 102–110.
14. J. Fridrich, T. Pevny, and J. Kodovsky, Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities, in *Proc. 9th Int. Conf. ACM Multimedia & Security*, eds. J. Dittmann, J. Fridrich (Dallas, TX, USA, 2007) 3-14.
15. P.A. Regalia, Cryptographic Secrecy of steganographic matrix embedding, *J. IEEE Transactions on Information Forensics Security*, 3(4) (2008) 768-791.
16. N. Shachtman, FBI: Spies Hid Secret Messages on Public Websites, Accessed on August 22, 2012. Available online at http://www.wired.com/dangerroom/2010/06/alleged-spies-hid-secret-messages-on-public-websites/.
17. C. Stier, Russian spy ring hid secret messages on the web, Accessed on August 22, 2012. Available online at http://www.newscientist.com/article/dn19126-russian-spy-ring-hid-secret-messages-on-the-web.html.
18. T.M. Cover, J.A. Thomas, Elements of Information Theory. Amarica:Wiley- Interscience, 1991, 35-45.