An Analysis of the F5 Steganographic System

MIDN 1/C Kyle Tucker-Davis

April 26, 2011

Abstract

Steganography, meaning *covered writing*, is the science of secret communication. Ideally, steganographic communications occurs without alerting anyone other than the sender and receiver. The seemingly innocuous medium to carry the information is called the *cover*. With the advent of computers, *digital steganography* refers to secret communication where the cover is a digital media file. In 2001, Westfeld proposed the **F5** steganographic system with the goal of encrypting information in a cover while minimizing the number of changes required. This project investigates the mathematical aspects of the **F5** system.

1 Introduction

Throughout history, many people have found unique and sophisticated ways to encrypt information. There have always been a few who have extended this idea to hiding information within innocuous objects. The goal of steganography, from the Greek words *steganos* and *graphein*, is to hide data from anyone other than the sender and receiver. The main advantage of such systems is that the communication does not garner any attention from an outside party. Cryptography, or the art of secure communication, can ensure privacy, but steganography can ensure absolute secrecy. Early examples include writing on the backing of a wax tablet before covering it, shaving and tattooing the head of a slave, only to let the hair re-grow, or using invisible ink.

Cryptography is widely known as the study of the composition of secret messages. In such a system, two parties Alice and Bob seek to exchange information while a third party Eve tries to learn the contents of the message. Encryption and decryption, respectively, are the processes which yield and decode the secret message. The most effective cryptographic methods are those which are computationally efficient yet secure.

Steganography, on the other hand, aims at allowing Alice and Bob to communicate secretly without Eve even knowing that the communication occurred. A steganographic system involves the message and an arbitrary cover, or the medium on which the message is transmitted. Covers are often tablets, body parts, or in the modern era, text, picture and audio files. Steganographic systems can either be classified as classical or modern, where those considered

modern take advantage of the vast possibilities to hide information in digital files. Consequently, the goal of digital steganography is to embed a message into the redundant data of a cover. The result, after the message has been embedded, is known as the *stego-cover*. The most common digital steganographic systems utilize images, video, or audio files as covers, as they are digital representations of physical quantities that thus contain noise.

One of the most common systems of digital steganography is the Least Significant Bit (LSB) system. In this system, the chosen encoder embeds one bit of information in the least significant bit, often considered redundant, of a given number of pixels of a given image. In this situation, a greyscale image is regarded as an array of pixels, where each pixel is represented by a binary vector. Care must be taken with this system to ensure that the changes made do not betray the stego-cover, while still maximizing the information hidden.

Error-correcting codes are those which utilize redundant data to ensure the original message can be accurately recovered after the introduction of errors. As all forms of media transfer are imperfect, these errors are often introduced as the message is being trasmitted. The use of these codes involves both the detection and the more difficult correction of an error. Simple error-correcting codes rely on some form of parity information as a reference for error detection, where the goal is to both maximize the information sent and the ability to correct errors.

Error-correcting codes are important if the distinction between code words is desired, yet the covering radius is helpful in describing a system's ability to embed a code in a medium. Thus, a covering code is an error-correcting code with a 'good' covering radius. The meaning of 'good' will be discussed later in the paper. The knowledge of error-correcting codes and use of covering codes has the potential to produce effective steganographic systems.

Bierbrauer [B], [BB], Fridrich [BF], Munuera [M], Zhang-Li [ZL] have all published on the advantages of using coding theory to produce steganographic systems, and the aim of this paper will be to combine this work in studying Westfeld's **F5** system.

2 Steganography in the Modern World

Because of its effectiveness, recent history has seen steganography employed by both states and private organizations.

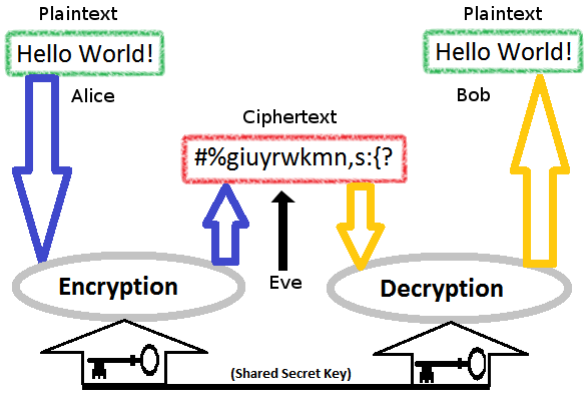
In February 2007, the second isssue of an extremist manual entitled *Technical Mujahid* was released on the internet. This publication is a Jihad technical training manual, intending to increase confidence, knowledge, security, and scientabout:homeific knowledge. One of the six sections references steganography and its potential for effective use. The recognition of the use of steganography by terrorists organizations confirms long standing suspicions of its application.

Cover from Technical Mujahid, Issue #2

In the summer of 2010, 11 suspected Russian spies were arrested in the United States. According to the FBI's charging documents, these individuals used a steganographic system that embedded information into images. Numerous free programs are available online to the casual user, and steganography, while traditionally not considered a severe digital threat, is in practical use.

3 Cryptography vs. Steganography

A *cryptosystem* is a specific method of secure communication. Let Alice and Bob be the sender and receiver, respectively, in such a cryptosystem. Alice starts with a *plaintext*, or unencrypted message. She then uses a *key*, or specific set of rules, to encrypt the message to produce a *ciphertext*. All the while, Eve the evesdropper wants to learn the contents of the plaintext.



Eve Tries to Learn Plaintext from Cryptosystem Used by Alice and Bob

The basic goals of a cryptosystem are computational efficiency and security. Security is the principle desire, and is commonly quantified with four tenents ([HAC], §1.2):

1. *Secrecy*: This objective ensures that the information is available only to those people who are authorized to have it.
2. *Integrity*: This ensures that no third party can make unauthorized alterations to the data.
3. *Non-repudiation*: This prevents the sender of information from denying that they sent that information. This also allows the receiver to prove to a third party that the information was sent by the sender.
4. *Authentication*: Authentication is related to identification. Two parties that are communicating with each other need to be able to identify one another and the receiver can be sure that the person sending the information is who the receiver thinks it is.

Steganography, as a method of secret communication, seeks to maintain the highest levels of security through focusing on imperceptibility to a detector. Similarly to cryptography, steganography is also measured in its integrity, or in this special case, resistance to removal. Unlike most cryptographic systems, however, one component of steganography is the actual size of the message that can be embedded in a cover object while still keeping the changes innocuous.

The ability to detect the manipulation of a cover is related to the length of the message embedded within it, because less changes to the original medium are required. For even the most simple stegosystems, determining the highest amount of information that can be embedded is not trivial. This amount of information is also related to the cover image chosen and the compression format used. Uncompressed files, for example, provide the most redundant space for manipulation, but they are also suspicious. The **F5** system described later in this paper is meant for JPEG images, some of the most abundant.

4 Error-correcting and Covering Codes

We recall some well-known definitions from Hill [H].

Let $GF(q)$ denote a finite field with q elements, where q is a power of a prime. A **linear (error-correcting) code** is a subspace C of $GF(q)^n$ for some $n > 1$, with a fixed basis. This integer n is called the **length** of C. Let C be a linear code of length n over $GF(q)$. If $q = 2$ then the code is called **binary**. Throughout, assume that $GF(q)^n$ has been given the standard basis $e_1 = (1, 0, ..., 0) \in GF(q)^n$, $e_2 = (0, 1, 0, ..., 0) \in GF(q)^n$, ..., $e_n = (0, 0, ..., 0, 1) \in GF(q)^n$. The **dimension** of C is denoted k, so the number of elements of C is equal to q^k.

The **Hamming distance** d is a tool for determining the number of errors a code can, in principle, detect. For any two $x, y \in GF(q)^n$, let $d(x, y)$ denote the number of coordinates where these two vectors differ:

$$d(x, y) = |\{1 \leq i \leq n \mid x_i \neq y_i\}|. \tag{1}$$

Define the **weight** wt of $v \in GF(q)^n$ to be the number of non-zero entries of v. Note, $d(x, y) = \text{wt}(x - y)$ because the vector $x - y$ has non-zero entries only at locations where x and y differ. The smallest distance between distinct codewords in a linear code C is the **minimum distance** of C:

$$d = d(C) = \min_{c \in C,\, c \neq 0} d(0, c). \tag{2}$$

Call a linear code of length n, dimension k, and minimum distance d an $[n, k, d]$ **code**, or $[n, k]$ **code** if the minimum distance is not required. The **Singleton Bound** states that if an $[n, k, d]$ linear code over $GF(q)$ exists, then $k \leq n - d + 1$.

A linear code C of length n and dimension k over $GF(q)$ has a basis of k vectors of length n. If those vectors are arranged as rows of a matrix G, call the $k \times n$ matrix G a **generator matrix** for C. A **check matrix** of C is any full rank matrix whose kernel is equal to C. Thus, a check matrix H is a $(n-k) \times n$ matrix over $GF(q)$.

Definition 1 *Let r be a positive integer and let H be an $r \times (2^r - 1)$ matrix whoses columns are the distinct non-zero vectors of $GF(2)^r$. Then, the code having H as its check matrix is called a binary* **Hamming code** *and is denoted Ham(r,2). [H]*

Example 1 *Let $r = 3$, and let*

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

In this form, namely when the columns of H are arranged in standard form such that the rightmost $k \times k$ entries are the identity matrix I_k, the generator matrix G can be quickly found to be

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

A **coset** is a subset of $GF(q)^n$ of the form $C + v$ for some $v \in GF(q)^n$. Equivalently, a coset is a pre-image of some y in $GF(q)^{n-k}$ under the check matrix $H : GF(q)^n \to GF(q)^{n-k}$. Let S be a coset of C. Then, a **coset leader** of S is an element of S having smallest weight.

Theorem 1 *The coset leaders of a Hamming code are those vectors of* wt ≤ 1.

Proof: Let the Hamming code be defined as a $[n, k, d]$ code as above where for some integer r, $n = 2^r - 1$, $k = 2^r - 1 - r$, and $d = r$. In the binary case, the size of the ambient space is $q^n = 2^n = |GF(q)^n|$ and the size of the code is $q^k = 2^k = |C|$. Thus, the size of any coset S of C is

$$|S| = |GF(q)^n|/|C| = 2^{n-k} = 2^r = n + 1.$$

Claim: Each coset contains a coset leader of wt ≤ 1 and no coset contains more than one vector of wt ≤ 1. *Proof of claim:* Assume that $v_1 + C$ is one such coset with two distinct vectors w_1, w_2 of wt ≤ 1. Then,

$$w_1 = v_1 + c_1, w_2 = v_1 + c_2.$$

So,

$$w_1 - w_2 = c_1 - c_2 \in C.$$

And, since wt$(w_1 - w_2) = 2$ and $d(C) = 3$ for a Hamming code, we have a contradiction. Also, by the Pigeonhole Principle, each coset contains exactly one vector of wt ≤ 1. Thus, the claim holds, and this also proves the theorem. □

Let C be a linear code in $V = GF(q)^n$, as above. We associate to V the usual Euclidean inner product, denoted by a dot $\cdot$ or by brackets $\langle \ldots, \ldots \rangle$. The **dual code** of C is the vector space of all code words in $GF(q)^n$ which are orthogonal (with respect to the given inner product) to each codeword in C:

$$C^{\perp} = \{v \in GF(q)^n \mid \langle v, c \rangle = 0 \ \forall \ c \in C\}. \tag{3}$$

If C is an $[n, k, d]$ code over $GF(q)$, the **covering radius** is defined to be

$$\rho = \max_{x \in GF(q)^n} d(x, C). \tag{4}$$

A **perfect code** is one for which $\rho = [(d-1)/2]$. A **covering code** is a linear error-correcting code having a 'good' covering radius ρ. A 'good' code refers to one which is close to perfect in some sense.

Theorem 2 *Hamming codes are perfect.*

Proof: Since $d(C) = 3$ for Hamming codes, we desire to show that equality holds in

$$\rho = [(d-1)/2] = 1.$$

To attain a contradiction, assume

$$\rho = \max_{x \in GF(q)^n} d(x, C) > 1;$$

then for some $x \in GF(q)^n$, $d(x, C) > 1$. But by the previous theorem, the coset $x + C$ must contain a coset leader of wt ≤ 1, a contradiction to the assumption that $d(x, C) > 1$. Thus, $\rho = 1$. $\square$

5 Steganographic Systems from Error Correcting Codes

Following [M], a **steganographic system** S can be formally defined as

$$S = \{\mathcal{C}, \mathcal{M}, \mathcal{K}, \text{emb}, \text{rec}\},$$

where

(i) $\mathcal{C}$ is a set of all possible covers

(ii) $\mathcal{M}$ is a set of all possible messages

(iii) $\mathcal{K}$ is a set of all possible keys

(iv) $\text{emb} : \mathcal{C} \times \mathcal{M} \times \mathcal{K} \to \mathcal{C}$ is an embedding function

(v) $\text{rec} : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ is a recovery function

and

$$\text{rec}(\text{emb}(c, m, k), k) = m, \tag{5}$$

for all $m \in \mathcal{M}$, $c \in \mathcal{C}$, $k \in \mathcal{K}$. We will assume that a fixed key $k \in \mathcal{K}$ is used, and therefore, the dependence on an element in the keyspace $\mathcal{K}$ can be ignored. The original cover c is called the **plain cover**, m is called the **message**, and $\text{emb}(c, m, k) = \text{emb}(c, m)$ is called the **stegocover**. Let $\mathcal{C}$ be $GF(q)^n$, representing both plain covers and stegocovers. Also, let $\mathcal{M}$ be $GF(q)^k$, where k is a fixed integer such that $0 \leq k \leq n$.

As images are the primary focus of the stegoschemes in this paper, we desire to embed information in the cover image such that its existence is not suspected. Let us start with a picture where the pixels are divided blocks of size n.

An (n, k, t) **stegocoding function** over finite field $GF(q)$ is a vector-valued linear transformation $L(x) = (\ell_1(x), \ell_2(x), \ldots, \ell_k(x)) : GF(q)^n \to GF(q)^k$ satisfying the following condition: For any given $x \in GF(q)^n$ and $y \in GF(q)^k$,

there exists a $z \in GF(q)^n$ such that $\mathrm{wt}(z) \leq t$ and $L(x+z) = y$. We call the matrix L an (n,k,t) **stegocode matrix**.

The mapping that sends (x,y) to z as above defines a $q^n \times q^k$ encoding table B.

Remark 1 *In this case, x is the plain cover, y is the message, $x+z$ is the stegocover, and z is the change made to the plain cover. z is derived from the specific system used, where it is desired that the weight of z is small while still retaining the ability to embed as much information as possible.*

Remark 2 *The stegocoding function in [ZL] corresponds closely to the covering function from [B] and roughly corresponds to the recovering function from Proposition 4.4 in [M].*

We next define the **encoding table** B. For $x \in GF(q)^n$, $y \in GF(q)^k$, define $B_{x,y} = z$ where z satisfies the following conditions: $z \in GF(q)^n$, $wt(z) \leq t$, and $L(x+z) = y$.

For the binary case ($q = 2$), let C be the $[n, n-k, d]$ code given by $C = \ker(L)$, where L is a $k \times n$ matrix of full rank over $GF(2)$. For each $y \in GF(2)^k$, let $v = v(y) \in GF(2)^n$ be such that $L^{-1}(y) = C + v$. Thus, $B_{x,y} = z$ as above means that $x + z \in C + v$ which implies that $z \in C + v + x$. We select z to be an element of $C + v + x$ of smallest weight, i.e. a coset leader. Choose t such that it is the largest weight of all the coset leaders of C. Therefore, the check matrix of the code C above defines an (n,k,t) stegocoding function.

Theorem 3 *Assume L is a $k \times n$ matrix as above. L is a (n,k,t) linear stegocode matrix iff t is the covering radius of the code C whose check matrix is L.*

The proof of the theorem above can be found in [M].

5.1 Practical Aspects of the Encoding Table

The brute force computation of this table involves q^{n+k} calculations. Therefore, the naive implementation of our stegoscheme requires that B is computed beforehand. Unless n and k are relatively small, this computation will be expensive. However, for some codes (those for which an efficient way of computing the coset leader is known), there are more efficient methods of computation.

5.2 Encoding Table Examples

Example 2 *Next we give an example of a $(5,2,1)$ stegocoding function.*

Define the check matrix and generator matrix as follows:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

We have $C = \ker(H) = \mathrm{Row}(G)$. *Since* $\dim(C) = 3$, *this is a* $[5, 3, 2]$ *code. Define the coset space by* $Q = GF(2)^5/\ker(H)$. *Define the syndrome of* $y \in GF(2)^2$ *to be the coset*

$$H^{-1}y = \{v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{pmatrix} \mid Hv = y\}.$$

Now we will compute all the syndromes explicitly. Computing the encoding table amounts to computing all the coset leaders, which are indicated in bold.

$$\begin{aligned}
H^{-1}\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \quad & \{(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0}), (1,0,0,1,0), (1,0,1,0,0), (0,0,1,1,0), \\
& (1,1,0,0,1), (0,1,0,1,1), (0,1,1,0,1), (1,1,1,1,1)\} \\
H^{-1}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \quad & \{(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0}), (1,0,0,0,0), (0,0,1,0,0), (0,1,0,0,1), \\
& (1,0,1,1,0), (1,1,0,1,1), (0,1,1,1,1), (1,1,1,0,1)\} \\
H^{-1}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \quad & \{(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}), (0,1,0,1,0), (1,1,0,0,0), (0,1,1,0,0), \\
& (1,0,0,1,1), (0,0,1,1,1), (1,0,1,0,1), (1,1,1,1,0)\} \\
H^{-1}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \quad & \{(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0}), (0,0,0,1,1), (1,0,0,0,1), (0,0,1,0,1), \\
& (1,1,0,1,0), (0,1,1,1,0), (1,1,1,0,0), (1,0,1,1,1)\}.
\end{aligned}$$

Note that H *is a* $(5, 2, 1)$ *stegocoding function.*

Let C be any Hamming code over $GF(q)$. Then, there is an integer $r \geq 1$ such that C has length $n = q^r - 1$, dimension $k = q^r - r - 1$, and minimum distance $d = 3$.

Example 3 *Let us consider an example of a* **F5** *stegosystem using a* $[7, 4, 3]$ *Hamming code. Define the check matrix and generator matrix as follows:*

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Denote the coset space by $Q = GF(2)^7/C$, *where* $C = \ker(H)$ *is a* $[7, 4, 3]$ *Hamming code.*

The encoding table is a 128×16 *array of vectors. We describe a specific example below. Let* $x = (1, 1, 1, 1, 1, 1, 1)$ *and* $y = (1, 0, 0)$ *We verify that* $B_{x,y} = (0, 0, 0, 0, 1, 0, 0) = z$, *since*

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

Other entries of B can be determined similarly.

For further details, see [B], [BB], [BF], [M], and [ZL].

6 The F5 Stegosystem

This project concerns the **F5** stegosystem, which incorporates linear error-correcting codes. Developed by D. Westfeld in 2001, the system hides k information bits into covers of length $n = 2^k - 1$. More importantly, this embedding is accomplished by changing at most one bit.

Before defining the **F5** stegosystem, new notation must first be defined. For any positive integer m, $[m]_2$ is the binary representation. Similarly, for any binary representation x, $[x]_{10}$ is the associated positive integer. Therefore, for any binary x, $[[x]_{10}]_2 = x$, and for any positive integer m, $[[m]_2]_{10} = m$.

In this system, the embedding map is defined as

$$\text{emb} : GF(2)^n \times GF(2)^k \to GF(2)^n \tag{6}$$

$$\text{emb}(c, m) = c + e(\big[m + \sum_{i=1}^{n} c_i[i]_2\big]_{10}) \ . \tag{7}$$

At this point, note that the message is in $GF(2)^q$, and both the plain text and stegocover are in $GF(2)^n$.

The recovery map is

$$\text{rec} : GF(2)^n \to GF(2)^k \tag{8}$$

$$\text{rec}(c') = \sum_{i=1}^{n} c'_i[i]_2 \ . \tag{9}$$

6.1 Theorem and Proof

Theorem 4 *With* emb *and* rec *as in (7) and (9), respectively, we have* $\text{rec}(\text{emb}(c, m)) = m$.

Proof: If $c' = \text{emb}(c, m)$, where $c' = (c'_1, c'_2, \ldots, c'_n)$, $c = (c_1, c_2, \ldots, c_n)$. Then, for all but one i, $1 \leq i \leq n$, we have

$$c'_i = c_i.$$

Now, suppose $c'_{i_0} \neq c_{i_0}$, $1 \leq i_0 \leq n$. In this case,

$$i_0 = \left[m + \sum_{i=1}^{n} c_i [i]_2 \right]_{10} .$$

In fact, for any $x \in GF(2)^k$, we have

$$[[x]_{10}]_2 = x .$$

Moreover, for any $x \in \{0, 1, \ldots, 2^k - 1\}$, we have

$$[[x]_2]_{10} = x .$$

Therefore,

$$[i_0]_2 = m + \sum_{i=1}^{n} c_i [i]_2 .$$

Thus,

$$\begin{aligned}
\mathrm{rec}(\mathrm{emb}(c, m)) &= \mathrm{rec}(c') \\
&= \sum_{j=1}^{n} c_j [j]_2 \\
&= \sum_{\substack{j=1 \\ j \neq i_0}}^{n} c_j [j]_2 \; + \; c'_{i_0} [i_0]_2 \\
&= \sum_{\substack{j=1 \\ j \neq i_0}}^{n} c_j [j]_2 \; + \; c'_{i_0} (m + \sum_{j=1}^{n} c_j [j]_2) .
\end{aligned}$$

At this point, there are 2 cases: $c'_{i_0} \neq 0$ (i.e. $c'_{i_0} = 1$), and $c'_{i_0} = 0$.
Case 1: Let $c'_{i_0} = 1$. Then, $c_{i_0} = 0$, so the above equation gives

$$\begin{aligned}
\mathrm{rec}(\mathrm{emb}(c, m)) &= \sum_{\substack{j=1 \\ j \neq i_0}}^{n} c_j [j]_2 \; + \; (m + \sum_{j=1}^{n} c_j [j]_2) \\
&= m \; + \; 2 \sum_{j=1}^{n} c_j [j]_2 \\
&= m .
\end{aligned}$$

Case 2: Let $c'_{i_0} = 0$. Then, $c_{i_0} = 1$, so the above equation gives

$$\begin{aligned}
\mathrm{rec}(\mathrm{emb}(c,m)) &= \sum_{\substack{j=1 \\ j \neq i_0}}^{n} c_j[j]_2 \\
&= \sum_{j=1}^{n} c_j[j]_2 + c_{i_0}[i_0]_2 \\
&= \sum_{j=1}^{n} c_j[j]_2 + (m + \sum_{j=1}^{n} c_j[j]_2) \\
&= m + 2\sum_{j=1}^{n} c_j[j]_2 \\
&= m\ .
\end{aligned}$$

□

7 Conclusion

The mating of coding theory's error-correcting and covering codes with digital steganography has the potential to produce effective and efficient new stegoschemes. The relatively low statistical detectability of stegoschemes like the **F5** system still maintain embedding efficiency, thus making them desirable for use.

While the above analysis provides only a narrow view of the methods of digital steganography, it alludes to the power, implications, and importance that it has the potential to occupy in the future. As these stegoschemes continue to become stronger, and therefore less statistically detectible, their use will spread. Several free steganography programs are already accessible, and to date, information transmission between several enemies of the United States has been reported. These include, but are not limited to, terrorist organizations and Russian operatives.

Acknowledgments: I would like to thank Dr. Lisa Marvel from the U.S. Army Research Laboratory for informative discussions and references. I would also like to thank the Honors Advisor for this project, Professor David Joyner.

References

[B] Bierbrauer, Jürgen. *Crandall's Problem.* unpublished. 1998. available: `http://www.ws.binghamton.edu/fridrich/covcodes.pdf`.

[BB] Bierbrauer, Jürgen. **Introduction to Coding Theory**. Chapman and Hall, CRC Press, 2005.

[BF] Bierbrauer, Jürgen and J. Fridrich. *Constructing good covering codes for applications in Steganography*. 2006. available: `http://www.math.mtu.edu/jbierbra/`.

[C] Crandall, Ron. *Some Notes on Steganography*. Posted on Steganography Mailing List, 1998. available: `http://os.inf.tu-dresden.de/westfeld/crandall.pdf`.

[F] Fridrich, Jessica, M. Goljan and D. Hogea. *Steganalysis of JPEG Images: Breaking the F5 Algorithm*. Proceedings of the 5th International Workshop on Information Hiding (IH '02), vol. 2578 of Lecture Notes in Computer Science, pp. 310-323, Noordwijkerhout, The Netherlands, October 2002.

[H] Hill, Raymond. **A First Course in Coding Theory**. Oxford University Press. 1997.

[HAC] Menezes, A, P. van Oorschot, and S. Vanstone. **Handbook of Applied Cryptography**. CRC Press, Inc.; 1997 pp1-4. available: `http://www.cacr.math.uwaterloo.ca/hac/`.

[M] Munuera, Carlos. *Steganography from a Coding Theory Point of View*.

[W] Wayner, Peter. **Disappearing Cryptography**. Morgan Kauffman Publishers. 2009.

[ZL] Zhang, Weiming and S. Li. *Steganographic Codes- a New Problem of Coding Theory*. preprint, 2005. available: `http://arxiv.org/abs/cs/0505072`.