ESTEGANOGRAFIA E O MÉTODO DE INSERÇÃO POR MATRIZ

Alexandre Henrique Campos
Universidade de Uberaba - UNIUBE
alexandre@alexandrecampos.com

Guilherme Chaud Tizziotti
Universidade Federal de Uberlândia
guilherme@famat.ufu.br

RESUMO

A Esteganografia é um assunto que ganhou importância rapidamente no contexto da segurança da informação. Ao ser relacionada com a Teoria dos Códigos, que já estava mais desenvolvida, a pesquisa neste mérito ganhou volume. Neste trabalho introduziremos Esteganografia e mostraremos como a Teoria dos Códigos pode facilitar seu estudo; veremos o efeito de código em papel molhado na Esteganografia.

ABSTRACT

Steganography is a subject that has become important very quickly in the security information matter. When it was linked with Coding Theory, which was more developed, its research has increased. In this work we will introduce Steganography and show how the Coding Theory can make its study easier; we will show the efect of wet paper codes in Steganography.

Palavras-chave: Esteganografia, Teoria dos Códigos, Códigos em Papel Molhado.

1 INTRODUÇÃO

Esconder uma mensagem pode ser uma forma eficiente de mantê-la em segredo, já que pode não despertar atenção. É neste processo que entra a esteganografia, ciência que estuda a ocultação de mensagens (informações). Tal nome provém das palavras gregas *estegano* (esconder) e *grafia* (escrita). Não devemos confundir a esteganografia com a criptografia, que oculta o significado da mensagem, e não a mensagem em si, muito menos com códigos corretores de erros, cuja finalidade é detectar e corrigir erros na transmissão de uma mensagem e não ocultá-la.

Basicamente, há quatro fatores principais que influenciam na eficiência da esteganografia, são eles:

1. o tipo de cobertura e a escolha dos lugares que serão usados para esconder a mensagem;
2. o método de inserção da mensagem na cobertura;
3. a quantidade de mudanças que serão feitas na cobertura para a inserção da mensagem;
4. o método usado para recuperar a mensagem.

Atualmente, faz-se o uso da esteganografia (digital) para esconder mensagens em arquivos digitais tais como imagens, áudios ou textos. Um exemplo básico de processo, para se esconder uma informação, usado na esteganografia digital é o LSB (*Least Significant Bit* – Bit Menos Significante). Na forma mais comum, seleciona-se determinado pixel[1] de uma imagem e troca-se o *bit* menos significante por um *bit* de informação. Note que, neste caso, emissor e receptor compartilham o método utilizado e o *canal de seleção*, que são os lugares da cobertura onde a informação está escondida. Vale a pena destacar a existência de dezenas de *softwares* tanto para esconder (inserir) quanto para recuperar mensagens escondidas em arquivos diversos, por exemplo, QuickStego, SecretLayer, SpamMimic ou OpenPuff.

A esteganografia é estudada há séculos e um dos trabalhos mais antigos de que se tem notícia, do qual nasceu o termo esteganografia, é o do alemão Johannes Trithemius [6], publicado postumamente em 1606. Porém, a grande parte dos artigos que tratam de estudos a seu respeito foram publicados nas duas últimas décadas. Neles, novas técnicas e algoritmos eficientes para inserir e extrair as informações das coberturas surgem para garantir uma melhor eficiência na transmissão de mensagens. Uma dessas novas técnicas utiliza ferramentas da Teoria de Códigos Corretores de Erros.

A *eficiência de inserção* – definida como sendo o número de *bits* inseridos por cada alteração feita – é uma maneira de medir a eficiência de um processo esteganográfico. Observe que quanto maior a eficiência de inserção, melhor, já que estaremos inserindo mais *bits* de informação modificando menos a cobertura. Crandall, em [2], descobriu um método, chamado de *inserção por matriz*, que além de ter uma boa eficiência de inserção, o receptor não precisa saber onde o emissor fez as alterações na imagem, ou seja, emissor e receptor não compartilham, ao contrário do LSB, o chamado *canal de seleção* - lugar dentro da cobertura onde ocorrem as mudanças causadas pela inserção. Esse fato é importante, pois ao compartilhar o canal de seleção, emissor e receptor podem cooperar com ataques à mensagem. Westfeld, em [7], foi o primeiro a incorporar o método de inserção por matriz no seu algoritmo F5 e ficou claro que a inserção por matriz poderia ser baseada na estrutura de códigos. Fridrich, Goljan, Lisonek e Soukal [3] introduziram o conceito de *códigos em papel molhado*, em que códigos apropriados são usados no método de inserção por matriz. O uso da matriz de checagem e do processo de decodificação tornam-se importantes ferramentas para o uso da inserção por matriz e melhorias na eficiência de inserção. Isso colocou de vez a teoria de códigos corretores de erros no estudo da esteganografia.

Este trabalho está organizado em três seções. Na primeira, introduzimos conceitos básicos da teoria de códigos corretores de erros. Na segunda, apresentamos conceitos e resultados relacionados à esteganografia e, finalmente, na terceira seção relacionamos os assuntos tratados nas seções anteriores abordando o método de inserção por matriz e os códigos em papel molhado. Encerramos este trabalho com uma conclusão do que foi apresentado.

2 CÓDIGOS CORRETORES DE ERROS

A Teoria de Códigos Corretores de Erros, iniciada por Claude Shannon, Richard Hamming e Marcel Golay no final da década de 1940 e início da década de 1950, é um ramo de pesquisa da matemática e também de outras áreas, como computação e engenharia elétrica. Ela surgiu para estudar transmissões de dados, a fim de encontrar meios de detectar e corrigir os erros causados no processo destas transmissões. De uma maneira resumida, para transmitir uma informação usando a Teoria de Códigos Corretores de Erros, devemos codificar a informação, que será transmitida a partir de um canal, e quando esta chegar em seu destino há que decodificá-la para se obter a informação original. Nesta parte do trabalho faremos uma breve introdução com conceitos e resultados que serão importantes

[1] Menor elemento de uma imagem. São como pequenos quadradinhos coloridos. Cada imagem é formada por uma sucessão de pixeis.

nas seções posteriores. Para mais detalhes sobre esta teoria sugerimos as referências [4] e [5].

Seja A um conjunto finito. Um **código corretor de erro** de comprimento n sobre A (que é chamado de alfabeto) é um subconjunto $C \subseteq A^n$. Geralmente, elementos de C são chamados de *palavras*. O comprimento n e o número de palavras do código C são parâmetros de C. Além deles, há um terceiro parâmetro muito importante, que mede o quão diferentes as palavras são umas das outras e está diretamente relacionado ao número de erros que poderão ser corrigidos no processo de transmissão de uma mensagem. Este parâmetro é a **distância mínima**, definida como

$$d = d(C) = min\{d(x,y)\ ;\ x,y \in C\ ,\ x \neq y\},$$

onde, para quaisquer $x = (x_1,\ldots,x_n), y = (y_1,\ldots,y_n) \in A^n$, $d(x,y) = \sharp\{i : x_i \neq y_i, 1 \leq i \leq n\}$ é a distância de Hamming em A^n. Não é difícil mostrar que a distância de Hamming é uma métrica. Outro conceito importante, relacionado ao de distância mínima, é o peso de um código. Dado $x = (x_1,\ldots,x_n) \in \mathbb{A}_q^n$, define-se o **peso de** x como o inteiro $\omega(x) = \sharp\{i : x_i \neq 0, i = 1,...,n\}$, isto é, $\omega(x) = d(x,0)$. O **peso de um código** C é o inteiro $\omega(C) = min\{\omega(x) : x \in C\backslash\{0\}\}$.

Dois resultados que mostram a importância da distância mínima d de um código C dizem que na transmissão de uma mensagem de C é possível detectar até $d-1$ e corrigir até $\lfloor (d-1)/2 \rfloor$ erros. Assim, quanto maior o valor de d melhor, pois pode-se detectar e corrigir um número maior de erros.

Estamos interessados em códigos corretores de erros sobre um corpo finito $\mathbb{F}_q$ com q elementos. Mais especificamente, em **códigos lineares** que são códigos $C \subset \mathbb{F}_q^n$, em que C é um subespaço vetorial de $\mathbb{F}_q^n$.

Se k é a dimensão do código C como um $\mathbb{F}_q^n$-subespaço vetorial, então escrevemos $dim(C) = k$. Não é difícil ver que $\sharp(C) = q^k$. Um código linear C com comprimento n, dimensão k e distância mínima d é chamado de $[n,k,d]$-código. Quando não for necessário citar a distância mínima, diz-se apenas $[n,k]$-código. Uma relação importante entre estes três parâmetros é a cota de Singleton[2] : $d + k \leq n + 1$.

Seja $\mathscr{B} = \{v_1,...,v_k\}$ uma base para C. A matriz G cujas linhas são os vetores da base $\mathscr{B}$ é chamada de **matriz geradora do código** C.

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$$

A aplicação

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & x & \longmapsto & x \cdot G \end{array}$$

pode ser vista como codificação de elementos de $\mathbb{F}_q^k$ para C. Observamos que $C = Im(T)$.

Definição 2.1: *Seja $C \subset \mathbb{F}_q^n$ um código linear. O **código dual** de C é definido por*

$$C^{\perp} := \{v \in \mathbb{F}_q^n : \langle u,v\rangle = 0, \forall u \in C\},$$

em que $\langle u,v\rangle$ denota o produto interno usual em $\mathbb{F}_q^n$.

Não é difícil mostrar que se C possui comprimento n e dimensão k, então $dim(C^{\perp}) = n-k$. O resultado a seguir, mostra a importância do conhecimento da matriz geradora de $C^{\perp}$. Sua demonstração pode ser facilmente encontrada em qualquer uma das referências sugeridas que tratam sobre este tema.

[2]Ver [5], p. 33.

Proposição 2.1: *Seja C um código linear e $C^{\perp}$ gerado pela matriz H. Então, $w \in C$ se, e somente se, $H \cdot w^t = 0$.*

A matriz H, como acima, é chamada de **matriz teste de paridade** ou **matriz de checagem** do código C. A partir de H, pode-se verificar se uma palavra pertence ou não ao código C. Este fato, como veremos a seguir, é importante no desenvolvimento de um processo de decodificação de C. Para o decorrer deste trabalho, um exemplo importante de código linear será o **código de Hamming**[3], que é o código cuja matriz de checagem, denotada por H_m, é de ordem $(m \times 2^m - 1)$ e apresenta os elementos de $F_2^m \backslash \{0\}$ dispostos em colunas em qualquer ordem.

Sejam $C \subset \mathbb{F}_q^n$ um código linear com matriz teste de paridade H e $x \in \mathbb{F}_q^n$, chamaremos de **síndrome de x em relação a C**, ou simplesmente **síndrome** de x, o vetor Hx^t. Definindo $v + C = \{v + c : c \in C\}$, não é difícil ver que dois vetores $u, v \in \mathbb{F}_q^n$ têm a mesma síndrome se, e somente se, $u \in v + C$. Cada conjunto da forma $v + C$ é chamado de classe lateral de v.

Definição 2.2: *Um vetor de peso mínimo em uma classe lateral é chamado de **elemento líder** dessa classe.*

Encerramos esta seção com um conceito que será muito útil no decorrer deste trabalho. Em geral, dado um código C e uma palavra recebida r, pode-se corrigir r para a palavra em C mais próxima de r, com relação à distância de Hamming. Este tipo de decodificação é chamada de **decodificação por distância mínima**.

3 ESTEGANOGRAFIA

Nesta seção veremos alguns conceitos importantes no tratamento da esteganografia digital.

Sejam $s = (s_1, ..., s_k) \in \mathbb{F}_q^k$ uma mensagem que queremos manter em segredo e $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ a cobertura (ou parte de uma cobertura) onde iremos esconder s.

Definição 3.1: *Um **protocolo esteganográfico de inserção/recuperação** do tipo $[k, n, \rho]$ (ou simplesmente $[k, n, \rho]$-protocolo) sobre $\mathbb{F}_q$, com $k \leq n$ inteiros, é um par de aplicações $\mathscr{P} = (\mathbf{e}, \mathbf{r})$, $\mathbf{e} : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^n$, $\mathbf{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ tal que $\mathbf{r}(\mathbf{e}(s, x)) = s$, para todo $s \in \mathbb{F}_q^k$, $x \in \mathbb{F}_q^n$. As aplicações $\mathbf{e}$ e $\mathbf{r}$ são chamadas de **inserção** e **recuperação**, respectivamente. O número $\rho = max\{d(x, \mathbf{e}(s, x)) : s \in \mathbb{F}_q^k, x \in \mathbb{F}_q^n\}$ é chamado **raio do protocolo**.*

Uma aplicação de inserção de um $[k, n, \rho]$-protocolo permite esconder k símbolos de informação em um vetor de tamanho n trocando, no máximo ρ dos símbolos da cobertura. Quando não for necessário explicitar o valor ρ, escreveremos apenas $[k, n]$-protocolo.

Definição 3.2: *Um protocolo esteganográfico é dito ser **próprio** se $\mathbf{e}(s, x)$ é o elemento mais próximo a x no conjunto $\mathbf{r}^{-1}(s) = \{y \in \mathbb{F}_q^n : \mathbf{r}(y) = s\}$.*

Exemplo 3.1: *Vejamos como definir o protocolo esteganográfico do processo LSB. Suponha que cada pixel seja representado por h bits e que a cobertura é a imagem inteira. O protocolo (para cada pixel) é o par de aplicações $\mathscr{P} = (\mathbf{e}, \mathbf{r})$, em que*

$$\begin{array}{rccc} \mathbf{e}: & \mathbb{F}_2 \times \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^n \\ & (s, (x_1, ..., x_{n-1}, x_n)) & \longmapsto & (x_1, ..., x_{n-1}, s) \end{array}$$

$$\begin{array}{rccc} \mathbf{r}: & \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2 \\ & (y_1, ..., y_n) & \longmapsto & y_n \end{array}$$

Como escondemos 1 bit de informação em uma parte da cobertura de tamanho n e alteramos sempre no máximo 1 desses n elementos, temos um $[1, n, 1]$-protocolo.

[3] Ver [5], p. 23.

Algo que podemos considerar em um protocolo $\mathscr{P} = (\mathbf{e}, \mathbf{r})$, com $\mathbf{e} : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^n$, $\mathbf{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$, é a chamada **média de símbolos modificados**, denotada por $\alpha = \alpha(\mathscr{P})$. Para calculá-la, assumimos que todos os elementos de $\mathbb{F}_q^n$ têm a mesma probabilidade de ser uma cobertura e que todos os elementos de $\mathbb{F}_q^k$ têm a mesma probabilidade de ser uma mensagem. Dessa forma, temos

$$\alpha(\mathscr{P}) = \frac{1}{q^{k+n}} \sum_{s \in \mathbb{F}_q^k} \sum_{x \in \mathbb{F}_q^n} d(x, \mathbf{e}(s, x)).$$

Outros parâmetros que podem ser considerados sobre o protocolo dado acima são os seguintes.

- A **capacidade relativa** k/n: símbolos imersos por símbolo da cobertura;
- A **distorção média** (ou **taxa de mudança**): probabilidade de que determinado símbolo na cobertura seja alterado durante o processo de inserção;
- A **eficiência da inserção**, denotada por e: número de *bits* inseridos para cada *bit* alterado, ou seja, $e = k/\alpha(\mathscr{P})$.

Quanto maior a capacidade relativa, mais informação podemos esconder na cobertura; quanto menor a distorção média, menos alterações fazemos durante a inserção.

Exemplo 3.2: *No caso do $[1, n, 1]$-protocolo $\mathscr{P}$ do LSB temos os seguintes parâmetros:*
- *média de símbolos modificados é $\alpha(\mathscr{P}) = 1/2$;*
- *capacidade relativa é igual a $1/n$;*
- *taxa de mudança será $1/2n$;*
- *eficiência da inserção é 2.*

Para $Y \subseteq \mathbb{F}_q^n$ definimos $d(x, Y) := \min\{d(x, y) : y \in Y\}$.

Lema 3.1: *Seja $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ um $[k, n, \rho]$ protocolo sobre $\mathbb{F}_q$. Então, existe um protocolo próprio $\mathscr{P}' = (\mathbf{e}', \mathbf{r})$ do tipo $[k, n, \rho']$ tal que $\rho' \leq \rho$.*

Demonstração. Tome $\mathbf{e}'$ como a aplicação de decodificação por distância mínima do código (subconjunto de $\mathbb{F}_q^n$) $\mathbf{r}^{-1}(s)$. Como $\mathbf{e}(s, x)$ e $\mathbf{e}'(s, x) \in \mathbf{r}^{-1}(s)$, e $\mathbf{e}'$ foi tomado como distância mínima, temos $d(x, \mathbf{e}'(s, x)) \leq d(x, \mathbf{e}(s, x))$. O resultado segue da Definição 3.2. □

A próxima proposição mostra como uma aplicação de recuperação pode ser obtida.

Proposição 3.1: *Uma aplicação $\mathbf{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ é aplicação de recuperação de um $[k, n]$-protocolo $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ se, e somente se, for sobrejetora. Se este protocolo for próprio, então seu raio é*

$$\rho = \max\{d(x, \mathbf{r}^{-1}(s)) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\}$$

Demonstração. $\Rightarrow$) Seja $s \in \mathbb{F}_q^k$. Como $\mathbf{r}(\mathbf{e}(s, x)) = s$, para qualquer $x \in \mathbb{F}_q^n$, seque que $\mathbf{r}$ é sobrejetora.
$\Leftarrow$) Se $\mathbf{r}$ é sobrejetora, para todo $s \in \mathbb{F}_q^k$, o conjunto $\mathbf{r}^{-1}(s)$ é não vazio. Tome $\mathbf{e}(s, x) = y$, para algum $y \in \mathbf{r}^{-1}(s)$. Então, $\mathbf{r}(\mathbf{e}(s, x)) = \mathbf{r}(y) = s$.

No caso de o protocolo ser próprio, então $\mathbf{e}(x, s)$ é o elemento mais próximo a x em $\mathbf{r}^{-1}(s)$, ou seja, $d(x, \mathbf{e}(s, x)) = d(x, \mathbf{r}^{-1}(s))$ (lembre que $\mathbf{e}(s, x) \in \mathbf{r}^{-1}(s)$). Logo,

$$\begin{aligned} \rho &= \max\{d(x, \mathbf{e}(s, x)) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\} \\ &= \max\{d(x, \mathbf{r}^{-1}(s)) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\} \end{aligned}$$

□

4 INSERÇÃO POR MATRIZ

4.1 O ALGORITMO F5

O algoritmo F5, criado por Westfeld, em [7], permite esconder k bits de informação em $2^k - 1$ *bits* da cobertura alterando no máximo 1 *bit*. Daí, o F5 é um protocolo do tipo $[k, 2^k - 1, 1]$. No que segue, $\langle x \rangle_2$ denota a expressão binária de x e, analogamente, $\langle y \rangle_{10}$ é a forma decimal de y. O i-ésimo vetor da base canônica de $\mathbb{F}_2^{2^k-1}$ é denotado por e_i, e tomamos $e_0 = 0$.

Considere a aplicação (com soma vetorial em $\mathbb{F}_2^k$)

$$\begin{array}{rccc} \eta: & \mathbb{F}_2^k \times \mathbb{F}_2^{2^k-1} & \longrightarrow & \mathbb{N} \\ & (s,x) & \longmapsto & \left\langle s + \sum_{i=1}^{2^k-1} x_i \langle i \rangle_2 \right\rangle_{10} \end{array}$$

As aplicações de inserção e recuperação são dadas, respectivamente, por:

$$\begin{array}{rccc} \mathbf{e}: & \mathbb{F}_2^k \times \mathbb{F}_2^{2^k-1} & \longrightarrow & \mathbb{F}_2^{2^k-1} \\ & (s,x) & \longmapsto & x + e_{\eta(s,x)} \end{array}$$

$$\begin{array}{rccc} \mathbf{r}: & \mathbb{F}_2^{2^k-1} & \longrightarrow & \mathbb{F}_2^k \\ & y & \longmapsto & \sum_{i=1}^{2^k-1} y_i \langle i \rangle_2 \end{array}$$

Vejamos que $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ é de fato um protocolo esteganográfico.

Note que $\mathbf{r}$ é linear, pois se u, $v \in \mathbb{F}_2^{2^k-1}$ e $\alpha \in \mathbb{F}_2$, então, escrevendo $u = (u_1, u_2, ..., u_{2^k-1})$ e $v = (v_1, v_2, ..., v_{2^k-1})$, temos:

$$\mathbf{r}(u + \alpha v) = \mathbf{r}((u_1 + \alpha v_1, u_2 + \alpha v_2, ..., u_{2^k-1} + \alpha v_{2^k-1})) = \sum_{i=1}^{2^k-1} (u_i + \alpha v_i)\langle i \rangle_2 =$$

$$\sum_{i=1}^{2^k-1} u_i \langle i \rangle_2 + \alpha \sum_{i=1}^{2^k-1} v_i \langle i \rangle_2 = \mathbf{r}(u) + \alpha \mathbf{r}(v)$$

Daí,

$$\mathbf{r}(\mathbf{e}(s,x)) = \mathbf{r}(x + e_{\eta(s,x)}) = \mathbf{r}(x) + \mathbf{r}(e_{\eta(s,x)}) = \sum_i x_i \langle i \rangle_2 + \langle \eta(s,x) \rangle_2 \tag{1}$$

Como $\eta(s,x) = \left\langle s + \sum x_i \langle i \rangle_2 \right\rangle_{10}$, temos $\langle \eta(s,x) \rangle_2 = s + \sum x_i \langle i \rangle_2$. Substituindo na equação (1):

$$\mathbf{r}(\mathbf{e}(s,x)) = \sum x_i \langle i \rangle_2 + s + \sum x_i \langle i \rangle_2 = s + 2 \sum x_i \langle i \rangle_2 = s$$

Proposição 4.1: *O F5 possui os seguintes parâmetros:*

- *média de símbolos modificados é* $\alpha(\mathscr{P}) = \frac{2^k-1}{2^k}$*;*
- *capacidade relativa é igual a* $\frac{k}{2^k-1}$*;*
- *taxa de mudança será* $\frac{1}{2^k}$*;*
- *eficiência da inserção é* $\frac{k}{1-2^{-k}}$*.*

Demonstração: Vamos demonstrar o primeiro item. Tome o protocolo F5 com aplicações de imersão $e: \mathbb{F}_2^k \times \mathbb{F}_2^{2^k-1} \longrightarrow \mathbb{F}_2^{2^k-1}$ e recuperação $r: \mathbb{F}_2^{2^k-1} \longrightarrow \mathbb{F}_2^k$. Por simplicidade, chame $n = 2^k - 1$. Temos que

$$\alpha(\mathscr{P}) = \frac{1}{2^k \cdot 2^n} \sum_{s \in \mathbb{F}_2^k} \sum_{x \in \mathbb{F}_2^n} d(x, e(s,x))$$

Para x, temos duas possibilidades: $x \in r^{-1}(x)$ ou $x \notin r^{-1}(s)$.

$$\alpha(\mathscr{P}) = \frac{1}{2^k \cdot 2^n} \sum_{s \in \mathbb{F}_2^k} \left(\sum_{x \in r^{-1}(s)} d(x, e(s,x)) + \sum_{x \notin r^{-1}(s)} d(x, e(s,x)) \right)$$

Se $x \in r^{-1}(x)$, então $x = e(s,x)$ e logo $d(x, e(s,x)) = 0$. Se $x \notin r^{-1}(x)$, para obter $e(s,x)$,o algoritmo F5 faz apenas uma modificação em x e logo $d(x, e(s,x)) = 1$.

$$\alpha(\mathscr{P}) = \frac{1}{2^k \cdot 2^n} \sum_{s \in \mathbb{F}_2^k} \left(\sum_{x \in r^{-1}(s)} 0 + \sum_{x \notin r^{-1}(s)} 1 \right)$$

Em $\mathbb{F}_2^n$, existem 2^n palavras divididas em 2^k classes. Fixado $s \in \mathbb{F}_2^k$, existem $2^k - 1$ classes em $\mathbb{F}_2^n$ tais que $x \notin r^{-1}(s)$, para todo x nessas classes.

$$\alpha(\mathscr{P}) = \frac{1}{2^k \cdot 2^n} \sum_{s \in \mathbb{F}_2^k} (2^k - 1)\frac{2^n}{2^k}$$

$$\alpha(\mathscr{P}) = \frac{1}{2^k \cdot 2^n} 2^k (2^k - 1)\frac{2^n}{2^k} = \frac{2^k - 1}{2^k}$$

■

Exemplo 4.1: *Suponha que queiramos esconder o segredo* $s = 011$ *dentro da cobertura* $x = 1010100$*.*

$$\eta(s,x) = \eta(011, 1010100) = \left\langle s + \sum_{i=1}^{7} x_i \langle i \rangle_2 \right\rangle_{10} =$$

$$\left\langle 011 + 1 \cdot 001 + 0 \cdot 010 + 1 \cdot 011 + 0 \cdot 100 + 1 \cdot 101 + 0 \cdot 110 + 0 \cdot 111 \right\rangle_{10} = \langle 100 \rangle_{10} = 4$$

Portanto, $e_{\eta(s,x)} = 0001000$ *e daí,* $\mathbf{e}(s,x) = 1010100 + 0001000 = 1011100$*.*

Agora,

$$\mathbf{r}(\mathbf{e}(s,x)) = \mathbf{r}(1011100) = \sum_{i=1}^{7} y_i \langle i \rangle_2$$

$$1 \cdot 001 + 0 \cdot 010 + 1 \cdot 011 + 1 \cdot 100 + 1 \cdot 101 + 0 \cdot 110 + 0 \cdot 111 = 011 = s.$$

4.2 RELACIONANDO ESTEGANOGRAFIA E CÓDIGOS CORRETORES DE ERROS

Dada uma aplicação de recuperação $\mathbf{r}$, podemos construir a aplicação de inserção $\mathbf{e}$ utilizando a teoria de códigos corretores de erros. Associado ao protocolo $\mathscr{P} = (\mathbf{e}, \mathbf{r})$, podemos considerar a família de códigos corretores de erros $\mathscr{F}_{\mathscr{P}} := (C_s = \mathbf{r}^{-1}(s) : s \in \mathbb{F}_q^k)$. Como $\mathbf{r}(\mathbf{e}(s,x)) = s$ e $\mathbf{e}(s,x) \in \mathbf{r}^{-1}(s)$, então $\mathbf{e}$ é uma decodificação da palavra x com respeito ao código corretor de erro $\mathbf{r}^{-1}(s)$. Quando o protocolo é próprio, $\mathbf{e}(s,x)$ é o elemento mais próximo à palavra x no conjunto $\mathbf{r}^{-1}(s)$ assim, esta decodificação coincide com a decodificação por distância mínima.

Proposição 4.2: *Seja* $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ *um* $[k,n]$*-protocolo próprio. Se para cada* $s \in \mathbb{F}_q^k$ *considerarmos* $C_s = \{x \in \mathbb{F}_q^n : \mathbf{r}(x) = s\}$*, então a família* $\mathscr{F}_{\mathscr{P}} = \{C_s : s \in \mathbb{F}_q^k\}$ *forma uma partição para* $\mathbb{F}_q^n$*. Além disto, para todo* $s \in \mathbb{F}_q^k$*, a aplicação* $dec_s : \mathbb{F}_q^n \to C_s$ *definida por* $dec_s(x) = \mathbf{e}(s,x)$ *é uma aplicação de decodificação para o código* C_s*.*

Demonstração. Como $\mathbf{r}(\mathbf{e}(s,x)) = s$, $C_s \neq \emptyset$, para qualquer $s \in \mathbb{F}_q^k$. Se $x \in C_s \cap C_{s'}$, então $\mathbf{r}(x) = s$ e $\mathbf{r}(x) = s'$. Como $\mathscr{P}$ é um protocolo, $\mathbf{r}$ está bem definida e $s = s'$. Pela proposição 3.1, r é sobrejetora e logo, para $x \in \mathbb{F}_q^n$, temos $\mathbf{r}(x) = s$, para algum $s \in \mathbb{F}_q^k$ e portanto $x \in C_s$. □

Proposição 4.3: *Seja $\{C_s : s \in \mathbb{F}_q^k\}$ uma família de códigos corretores de erros que formam uma partição para $\mathbb{F}_q^n$. Para cada $s \in \mathbb{F}_q^k$, seja dec_s a decodificação por distância mínima para o código C_s. Considere as aplicações $\mathbf{e} : \mathbb{F}_q^k \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ e $\mathbf{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ definidas, respectivamente, por $\mathbf{e}(s,x) = dec_s(x)$ e $\mathbf{r}(x) = s$ se $x \in C_s$. Nestas condições, $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ é $[k,n]$-protocolo próprio sobre $\mathbb{F}_q$.*

Demonstração. Como $dec_s(x) \in C_s$, temos que $\mathbf{r}(\mathbf{e}(s,x)) = s$. Além do mais, $d(x, \mathbf{e}(s,x)) = d(x, dec_s(x)) = d(x, C_s)$, o que prova que o protocolo é próprio. □

Utilizando estes resultados, podemos construir um protocolo esteganográfico da seguinte maneira:

1. Fixe uma aplicação de recuperação $\mathbf{r} : \mathbb{F}_q^n \to \mathbb{F}_q^k$ e considere a respectiva família[4] de códigos $\mathscr{F}_{\mathscr{P}} = (C_s = \mathbf{r}^{-1}(s) : s \in \mathbb{F}_q^k)$;

2. Para $s \in \mathbb{F}_q^k$, a aplicação de inserção $\mathbf{e}$ será a decodificação por distância mínima para o código $\mathbf{r}^{-1}(s)$.

Justificativa 4.1: *: Como $\mathbf{e}(s,x) \in \mathbf{r}^{-1}(s)$ (pela correção por distância mínima para um elemento de $\mathbf{r}^{-1}(s)$), temos que $\mathbf{r}(\mathbf{e}(s,x)) = s$. Note que poderíamos escolher $\mathbf{e}(s,x)$ como qualquer palavra em $\mathbf{r}^{-1}(s)$. A unicidade, no caso de protocolos, não é importante, apesar de o ser para a teoria dos códigos corretores de erros.*

Apesar da liberdade de poder escolher entre qualquer elemento de $\mathbf{r}^{-1}(s)$, tomamos o mais próximo de x para alterar pouco a cobertura, o que dificulta a detecção da mensagem na cobertura. Um protocolo construído como descrito acima é chamado de **protocolo baseado em códigos**. Esta construção também é conhecida como **matriz de inserção**, apesar do fato de que alguns autores preferem não utilizar este termo, pois podemos não utilizar matriz alguma. Por exemplo, no algoritmo F5 dado anteriormente não foi utilizado nenhuma matriz, porém podemos construir o mesmo utilizando tal recurso. A aplicação de recuperação utilizada no F5 é linear e sua matriz é justamente a matriz de checagem de um código de Hamming de dimensão k. Além disso, a aplicação de inserção é justamente a aplicação de decodificação por distância mínima desse mesmo código.

Exemplo 4.2: *No que segue, H_3 denota o código de Hamming de dimensão 3, ou seja, a matriz de checagem é*

$$M_3 = \begin{pmatrix} 0001111 \\ 0110011 \\ 1010101 \end{pmatrix} \text{ e } \begin{array}{rcl} H_3 & = & \{0000000, 0001111, 0010110, 0011001, \\ & & 0100101, 0101010, 0110011, 0111100, \\ & & 1000011, 1001100, 1010101, 1011010, \\ & & 1100110, 1101001, 1110000, 1111111\} \end{array}$$

Suponha que tenhamos uma aplicação de recuperação $\mathbf{r}$ como no F5 e queiramos encontrar a aplicação de inserção. Os elementos da família de códigos são.

$$\begin{array}{rcl} \mathbf{r}^{-1}(011) & = & \{1011100, 0010000, 0011111, 0000110, \\ & & 0001001, 0110101, 0111010, 0100011, \\ & & 0101100, 1010011, 1000101, 1001010, \\ & & 1110110, 1111001, 1100000, 1101111\} \quad = \quad 0010000 + H_3 \end{array}$$

$$\begin{array}{c} \mathbf{r}^{-1}(000) = H_3 \\ \mathbf{r}^{-1}(001) = 1000000 + H_3 \\ \mathbf{r}^{-1}(010) = 0100000 + H_3 \\ \mathbf{r}^{-1}(100) = 0001000 + H_3 \\ \mathbf{r}^{-1}(101) = 0000100 + H_3 \\ \mathbf{r}^{-1}(110) = 0000010 + H_3 \\ \mathbf{r}^{-1}(111) = 0000001 + H_3 \end{array}$$

[4] Por abuso de notação, nos referimos a $\mathscr{P}$ antes de tê-lo construído efetivamente.

Note que apenas $\mathbf{r}^{-1}(000)$ *é um código linear - os outros são classes laterais. Suponha que queiramos esconder* $s = 011$ *em* $x = 1010100$*, como no exemplo 4.1. Veja que em* $\mathbf{r}^{-1}(011)$*, a palavra mais próxima (distância mínima em* $\mathbf{r}^{-1}(011)$*) a* 1010100 *é* 1011100*. Tomamos* $\mathbf{e}(s, x) = 1011100$ *(na verdade, como está na justificativa 4.1, poderíamos ter escondido* 011 *em* 1010100 *como* 1011100*, ou* 001000*, ou qualquer outra palavra de* $0010000 + H_3$*).*

Mais ainda, a recuperação de qualquer $y \in \mathbf{r}^{-1}(s)$ *coincide com o cálculo da síndrome* $H_3 \cdot y^t$*, com a seguinte ordenação para* H_3*:*

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

O exemplo anterior nos motiva a considerar protocolos $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ em que $\mathbf{r}$ é linear.

Definição 4.1: *Um protocolo esteganográfico* $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ *é dito* ***linear*** *se a aplicação* $\mathbf{r}$ *é linear.*

Proposição 4.4: *Se* $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ *é um* $[k, n]$*-protocolo esteganográfico linear, então* $\mathscr{C} = \mathbf{r}^{-1}(0)$ *é um código linear. Os demais códigos* $C = \mathbf{r}^{-1}(s)$*,* $s \in \mathbb{F}_q^k \setminus \{0\}$*, são classes laterais.*

Demonstração. Pela definição de código linear, precisamos provar que $\mathscr{C}$ é um subespaço vetorial de $\mathbb{F}_q^n$. Por hipótese, $\mathbf{r}$ é linear. Se $\beta \in \mathbb{F}_q$, u e $v \in \mathscr{C}$, então $\mathbf{r}(u) = \mathbf{r}(v) = 0$ e $\mathbf{r}(u + \beta v) = \mathbf{r}(u) + \mathbf{r}(\beta v) = \mathbf{r}(u) + \beta\mathbf{r}(v) = 0 + 0 = 0$. Segue que $u + \beta v \in \mathscr{C}$, daí $\mathscr{C}$ é um código linear.

Dado $s \in \mathbb{F}_q^k$, considere o código $C = \mathbf{r}^{-1}(s)$. Fixamos $u \in C$ e seja $v \in C$ qualquer. Vejamos que $C = u + \mathscr{C}$. Temos $\mathbf{r}(u) = \mathbf{r}(v) = s$. Logo, $\mathbf{r}(u - v) = 0$ e $u - v \in \mathscr{C}$, portanto $C \subseteq u + \mathscr{C}$. Por outro lado, se $y \in u + \mathscr{C}$, então $y = u + c$, com $\mathbf{r}(c) = 0$ e $\mathbf{r}(y) = \mathbf{r}(u) + \mathbf{r}(c) = \mathbf{r}(u) = s$. Segue que $u + \mathscr{C} \in C = \mathbf{r}^{-1}(s)$. □

Definição 4.2: *O código* $\mathscr{C} = \mathbf{r}^{-1}(0)$ *associado a um* $[k, n]$*-protocolo esteganográfico linear* $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ *é chamado de* ***código principal*** *associado a* $\mathscr{P}$ *e denotado por* $C_{\mathscr{P}}$*. Uma matriz* R *de* r *(que é tal que* $\mathbf{r}(x) = Rx^t$ *para qualquer* $x \in \mathbb{F}_q^n$*, existe pois* $\mathbf{r}$ *é linear entre subespaços de dimensão finita e é a matriz teste de paridade de* $C_{\mathscr{P}}$*) é chamada de* ***matriz de recuperação*** *de* $\mathscr{P}$*.*

No Exemplo 4.2 a matriz de recuperação é H_3 como descrita.

Proposição 4.5: *Seja* C *um* $[n, n-k]$*-código e* R *uma matriz teste de paridade de* C*. Seja* $\mathbf{r}$ *a aplicação cuja matriz é* R*. Então,* $\mathbf{r}$ *é uma aplicação de recuperação de um* $[n, k, \rho]$*-protocolo próprio, com* ρ *sendo o raio de cobertura do código* C*.*

Demonstração. Como $\mathbf{r}$ é sobrejetora (pois R é uma matriz teste de paridade), de acordo com o Lema 3.1 e a Proposição 3.1, podemos construir um $[k, n]$-protocolo próprio $\mathscr{P}$. Além disso, $C_{\mathscr{P}} = C$ (pela construção sobre a matriz teste de paridade) e por consequência para todo $s \in \mathbb{F}_q^k$, temos $C_s = y_s + C$, com y_s um elemento fixo de $\mathbf{r}^{-1}(s)$. Vamos calcular o raio $\mathscr{P}$. Pela Proposição 3.1,

$$\begin{aligned} \rho(\mathscr{P}) &= \max\{d(x, \mathbf{r}^{-1}(s)) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\} \\ &= \max\{d(x, y_s + C) : x \in \mathbb{F}_q^n,\ s \in \mathbb{F}_q^k\} \end{aligned}$$

Para $s \in \mathbb{F}_q^k$, seja $\rho_s = \max\{d(x, y_s + C) : x \in \mathbb{F}_q^n\} = d(x, y_s + c)$, para algum $c \in C$. Como a distância de Hamming é invariante pela translação, $\rho_s = d(x, y_s + c) = d(x - y_s, c) \leq \rho_0$; analogamente $\rho_0 \leq \rho_s$. Portanto, $\rho_s = \rho_0$. Finalmente, note que $\rho(\mathscr{P}) = \rho_0 = \max\{d(x, C) : x \in \mathbb{F}_q^n\}$, que é o raio de cobertura do código C. □

Pelos resultados anteriores, para construir um protocolo linear, podemos considerar matrizes teste de paridade de códigos lineares, obter $\mathbf{r}$ e tomar $\mathbf{e}$ como sendo a decodificação do código por distância mínima.

Algoritmo 4.1: *Dada uma matriz teste de paridade R de ordem $k \times n$ com posto tão grande quanto possível, temos uma aplicação de recuperação $\mathbf{r}$, a distância mínima d do código associado (ver Teorema 1.32, em [1]) e κ a capacidade de correção. Queremos construir a aplicação de inserção para $s \in \mathbb{F}_q^k$ e $x \in \mathbb{F}_q^n$.*

1. *Defina $t := \mathbf{r}(x)$;*
2. *Coloque $c := x - \ell_t$, com ℓ_t o elemento de menor peso da classe em que t está em relação ao código;*
3. *Defina $\mathbf{e}(s, x) := \ell_s + c$.*

Justificativa 4.2: *Como $\mathbf{r}$ é linear, $\mathbf{r}(\mathbf{e}(s,x)) = \mathbf{r}(\ell_s + c) = \mathbf{r}(\ell_s) + \mathbf{r}(c) = s + \mathbf{r}(x - \ell_t) = s + \mathbf{r}(x) - \mathbf{r}(\ell_t) = s + \mathbf{r}(x) - \mathbf{r}(x) = s$.*

Apesar de termos escolhido a decodificação por distância mínima, a aplicação de inserção poderia ser tomada segundo qualquer método de decodificação para códigos lineares.

Exemplo 4.3: *Considere a matriz de checagem*

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Defina a aplicação de recuperação $\mathbf{r} : \mathbb{F}_2^7 \to \mathbb{F}_2^3$ por $\mathbf{r}(y) = R \cdot y^t$. Temos que $\mathbf{r}$ é sobrejetora e logo, pela Proposição 3.1, é uma aplicação de recuperação de algum protocolo $\mathscr{P} = (., \mathbf{r})$. Vamos construir a aplicação de inserção. Considere a família de códigos $\mathscr{F} = \{C_s : C_s = \mathbf{r}^{-1}(s),$ para $s \in \mathbb{F}_2^3\}$. Defina $\mathbf{e} : \mathbb{F}_2^3 \times \mathbb{F}_2^7 \to \mathbb{F}_2^7$ por $\mathbf{e}(s,x) = y$, com $y \in \mathbf{r}^{-1}(s) \subset \mathbb{F}_2^7$ tal que $d(x, \mathbf{r}^{-1}(s)) = d(x,y)$.

Neste caso, se quisermos esconder $s = 011$ em 1010100 teremos que $\mathbf{e}(s,x) = 1011100$.

Vale a pena ressaltar que a aplicação de decodificação é usada de uma maneira diferente na Teoria de Códigos Corretores de Erros e na Esteganografia. Na Teoria de Códigos a proposta é corrigir erros (introduzidos pelo canal utilizado na transmissão). Assim, é importante garantir que sob certas condições a palavra original (transmitida) e a decodificada sejam as mesmas. Em particular, quando é usada a decodificação por distância mínima, pode ser que a palavra mais próxima não seja única e, assim, a decodificação falha. Já na Esteganografia a proposta é "introduzir"erros na cobertura, de preferência um número pequeno de erros para dificultar a detecção. Como consequência, a unicidade da palavra mais próxima não é importante: se existir mais que uma palavra mais próxima, simplesmente tomamos uma aleatoriamente.

Lema 4.1: *Seja $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ um $[k,n]$-protocolo próprio sobre $\mathbb{F}_q$ associado ao código C. Então, $\alpha(\mathscr{P}) = \dfrac{1}{q^n} \displaystyle\sum_{x \in \mathbb{F}_q^n} d(x, C)$.*

Demonstração. Como $d(x, \mathbf{e}(s,x)) = d(x, \ell_s + C) = d(x - \ell_s, C)$, temos

$$\sum_{x \in \mathbb{F}_q^n} d(x, \mathbf{e}(s,x)) = \sum_{x \in \mathbb{F}_q^n} d(x, \ell_s + C) = \sum_{y \in \mathbb{F}_q^n} d(y, C)$$

Disto,

$$\alpha(\mathscr{P}) = \frac{1}{q^{k+n}} \sum_{s \in \mathbb{F}_q^k} \sum_{x \in \mathbb{F}_q^n} d(x, \mathbf{e}(s,x)) = \frac{1}{q^{k+n}} \sum_{s \in \mathbb{F}_q^k} \sum_{y \in \mathbb{F}_q^n} d(y, C)$$

Veja que a parte $\displaystyle\sum_{y \in \mathbb{F}_q^n} d(y, C)$ independe de s para cada $s \in \mathbb{F}_q^k$ e portanto,

$$\alpha(\mathscr{P}) = \frac{1}{q^{k+n}} \left(\underbrace{\sum_{y \in \mathbb{F}_q^n} d(y,C) + \cdots + \sum_{y \in \mathbb{F}_q^n} d(y,C)}_{q^k \text{ vezes}} \right) = \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} d(y,C)$$

□

Proposição 4.6: *Seja $\mathscr{P} = (\mathbf{e}, \mathbf{r})$ um $[k,n]$-protocolo próprio sobre $\mathbb{F}_q$ associado a um código C. Para $i = 0, ..., n$, seja α_i o número de líderes (ver Definição 2.2) com peso i com respeito ao código C. Então, $\alpha(\mathscr{P}) = \frac{1}{q^k} \sum_{i=1}^{n} i\alpha_i$.*

Demonstração. Tome $x \in \mathbb{F}_q^n$. Então $x \in \ell_s + C$, para algum $s \in \mathbb{F}_q^k$. Assim, $d(x,C) = \omega(\ell_s)$, pois cada palavra na classe $\ell_s + C$ está a uma mesma distância do código. As q^n palavras de $\mathbb{F}_q^n$ estão igualmente distribuídas em q^k classes, cada uma originada de uma palavra de $\mathbb{F}_q^k$, logo cada classe lateral do código contém q^{n-k} palavras.

$$\sum_{y \in \mathbb{F}_q^n} d(y,C) = q^{n-k} \sum_{y \in \mathbb{F}_q^n / C} d(y,C) = q^{n-k} \sum_{i=1}^{n} i\alpha_i$$

E o resultado segue do lema anterior [5]. □

4.3 CÓDIGOS EM PAPEL MOLHADO

Imagine que se deseje enviar uma mensagem escrita em um papel que foi exposto a chuva e está molhado, exceto por algumas partes, no momento em que o emissor irá escrever. Para minimizar o dano ao papel e evitar que ele rasgue sobre a pressão da caneta, o emissor escolhe os lugares secos como canal de seleção (**canal de seleção** - lugares na cobertura que conterão a mensagem escondida) para colocar a mensagem desejada. Quando o receptor recebe o papel com a mensagem, o papel já está completamente seco e não há como saber quais lugares estavam molhados. Desta forma, emissor e receptor não compartilham o canal de seleção, e diz-se que o emissor está "escrevendo sobre papel molhado".

Quando aplicamos Teoria de Códigos e, por algum motivo, não podemos alterar determinadas posições (como no papel molhado), diz-se que estamos no caso de código em papel molhado. Mais geralmente, chama-se **Código em Papel Molhado** (em inglês, *wet paper code*).

Considere que a imagem de cobertura seja $b = \{b_1, ..., b_n\}$, em que cada b_i é um pixel, para $1 \leq i \leq n$ e o conjunto $J = \{i_1, ..., i_j\} \subset \{1, ..., n\}$ que represente os índices dos pixeis que podem ser modificados. Tome M uma matriz previamente compartilhada entre emissor e receptor, e suponha que a mensagem a ser envidada é $s \in \mathbb{F}_2^k$ escondida em b. O emissor deve então alterar b para b' de tal forma que

$$Mb' = s. \tag{2}$$

Para recuperar a mensagem o receptor precisa resolver um sistema linear em $\mathbb{F}_2$, ou seja, transformamos o problema de inserção em um problema de solução de sistema linear. Chamando $v = b' - b$, os elementos não nulos de v correspondem aos *bits* que devem ser modificados para satisfazer a equação (2). Podemos reescrever o sistema como

$$Mv = s - Mb. \tag{3}$$

[5] O somatório não precisa começar do 0, pois o peso da palavra líder de uma das classes é igual a 0; a saber, a classe $0 + C = C$.

Neste novo sistema, existem j incógnitas v_j, $j \in J$, enquanto os outros $n-j$ valores são iguais a zero. Assim, do lado esquerdo da igualdade, podemos remover de v todas as entradas nulas e de M as $n-j$ colunas correspondentes aos zeros. Desta forma obteremos uma matriz H que é tal que

$$Hv = m - Mb. \tag{4}$$

Mantemos a notação v mesmo após a remoção das entradas nulas. A matriz H possui k linhas e j colunas e o sistema tem solução quando o posto de H for igual a k. Assim, o número mínimo de coordenadas secas necessárias para a inserção de k bits de mensagem usando a matriz H é

$$sec(H) = \text{ min } \{u : \text{toda submatriz de } H \text{ formada por } u \text{ colunas tem posto } k\}.$$

Vejamos como relacionamos este problema com a Teoria de Códigos Corretores de Erros.

Definição 4.3: *Seja J um conjunto de coordenadas que devem ser mantidas fixas durante a inserção, H uma $[n-k, n]$-matriz de checagem de um código C. Considere a matriz H_J obtida de H retirando-se as colunas relativas às posições de J. O código que possui H_J como matriz de checagem é chamado de* ***código reduzido*** *de C e denotado por C_J.*

Considere o conjunto $C'_J = \{c \in C : c_{j_i} = 0 \text{ para todo } j_i \in J\}$.

Proposição 4.7: *As palavras que compõe C_J são as palavras de C'_J deletadas as posições J.*

Demonstração. Seja A o conjunto formado pelas palavras de C'_J deletadas as posições J. Queremos mostrar que $C_J = A$.
$A \subset C_J$: Seja $a = (a_1, ..., a_{n-\sharp(J)}) \in A$. Queremos mostrar que $H_J \cdot a^t = 0$. Ao se completar a com 0 nas posições J, renumeramos e denotamos este novo vetor por $\overline{a}$. Vemos que $\sum_{i=1}^{n}(h_i a_i) = 0$, com $a_j = 0$, para todo $j \in J$ e daí $\overline{a} \in C$. Como nas colunas de J as entradas do vetor são iguais a 0, essas não fazem diferença na combinação linear, $a \in C_J$.
$C_J \subset A$: A matriz teste de paridade de C_J é

$$H_J = \begin{pmatrix} h_1 & h_2 & \cdots & \widehat{h_{J_1}} & \cdots & \widehat{h_{J_2}} \cdots & h_n \end{pmatrix},$$

em que as h_j, $1 \leq j \leq n$, são colunas de H e $\widehat{h_{J_i}}$, $1 \leq i \leq \sharp(J)$, significa a omissão das colunas. Seja $c = (c_1, ..., c_{n-\sharp(J)}) \in C_J$. Após adicionar 0 às posições J e fazer a renumeração, temos $\overline{c} = (c_1, c_2, ..., 0, ..., c_n)$ e daí $H \cdot \overline{c}^t = 0$, ou seja, $\overline{c} \in C'_J$ e $c \in A$. □

Exemplo 4.4: *Considere a matriz de checagem*

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

O código associado a essa matriz é

$$C = \{000000, 001111, 010001, 011110, 100010, 101101, 110011, 111100\}.$$

Tome H_J obtida removendo-se a segunda e a quinta colunas

$$H_J = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

O código reduzido neste caso é $C_J = \{0000, 1111\}$. Note que as únicas palavras de C a possuírem 0 nas segunda e quinta coordenadas eram 000000 e 101101.

O exemplo a seguir nos mostra o uso de códigos em papel molhado.

Exemplo 4.5: *Considere a matriz*

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

O código C associado a essa matriz é dado na Tabela 1 a seguir.

00000000	00011110	00101101	00110011
01001011	01010101	01100110	01111000
10000111	10011001	10101010	10110100
11001100	11010010	11100001	11111111

TABELA 1: Código associado à matriz H.

Suponha que queiramos esconder $s = 1101$ em 11010110. Pela decodificação por distância mínima, poderíamos tomar $\mathbf{e}(s, x)$ como qualquer palavra no conjunto $Y = \{00010110, 11000100, 11011010, 11$ pois estes elementos estão em $\mathbf{r}^{-1}(s)$, dado na Tabela 2, e estão a uma menor distância de x (no caso, $d(y, x) = 2$ para qualquer $y \in Y$).

00001000	00010110	00100101	00111011
01000011	01011101	01101110	01110000
10001111	10010001	10100010	10111100
11000100	11011010	11101001	11110111

TABELA 2: Classe lateral associada a s, ou seja, $\mathbf{r}^{-1}(s)$.

No caso de Código em Papel Molhado em que não podemos, por exemplo, modificar as duas primeiras entradas, as possibilidades se restringiriam ao conjunto $\{11000100, 11011010, 11110111\}$. Se restringirmos até a terceira entrada sem alteração, as possibilidades seriam $\{11000100, 11011010\}$. Se a restrição fosse feita às cinco primeiras entradas, não encontraríamos solução para o sistema como descrito na equação (2).

5 CONCLUSÕES

Vimos que existe uma relação estreita entre protocolos esteganográficos e códigos corretores de erros. Com o grande conhecimento que há sobre a Teoria de Códigos Corretores de Erros pode-se obter propriedades e construções de bons protocolos esteganográficos. Esta relação está só no começo. Uma relação com códigos algébricos geométricos, os quais têm se mostrado eficientes e com boas propriedades, pode ajudar ainda mais no desenvolvimento da esteganografia. E isto serve de motivação para trabalhos futuros.

REFERÊNCIAS

[1] A. H. A. Campos: *Esteganografia do ponto de vista da teoria dos códigos*. Dissertação de Mestrado, Faculdade de Matemática, Universidade Federal de Uberlândia, 2014.

[2] R. Crandall: *Some notes in Steganography*. http://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998.

[3] J. Fridrich, M. Goljan e D. Soukal: *Efficient Wet Paper Codes*. Information Hiding. 7th International Workshop, LNCS , Springer-Verlag, 3727:204–218, 2005.

[4] A. Hefez e M. Villela: *Códigos Corretores de Erros*. IMPA, Rio de Janeiro, fev. 2008.

[5] F. J. MacWilliams e N. J. A. Sloane: *The Theory of Error-Correcting Codes*. North-Holland, New York, 3ª ed., 1977.

[6] J. Trithemius: *Steganographie: Ars per occultam Scripturam animi sui voluntatem absentibus aperiendi certu*. http://www.esotericarchives.com/tritheim/stegano.htm, set. 2013.

[7] A. Westfeld: *F5-A Steganographic Algorithm*. In *Proceedings of the 4th International Workshop on Information Hiding*, pp. 289–302, 2001.