The mΘ Protocol F5 and Hamming mΘ Codes

Pemha Binyam Gabriel Cedric

ABSTRACT

The mΘ structure introduce pure and applied mathematics using the set FpZ ≡ Fp [fxpZ j e(x = 0(mod(p)))g, p prime, to then present mathematical structures resulting from the sets originally introduced F. Ayissi Eteme [6]. This work consists in defining on FpZ the notion of Hamming code according to mΘ set structure. We show a relation between mΘ protocol F5 and Hamming mΘ code. By using this relation, we get a new steganography based on the bit modalities of a code word.

Keywords: mΘ set, Hamming mΘ codes, steganography, mΘ protocol F5.

Classification: LCC: QA76

Language: English

Great Britain Journals Press

LJP Copyright ID: 925633
Print ISSN: 2631-8490
Online ISSN: 2631-8504

London Journal of Research in Science: Natural and Formal

Volume 23 | Issue 13 | Compilation 1.0

The mΘ Protocol F5 and Hamming mΘ Codes

Pemha Binyam Gabriel Cedric

ABSTRACT

The mΘ structure introduce pure and applied mathematics using the set FpZ ≡ Fp [fxpZ j e(x = o(mod(p)))g, p prime, to then present mathematical structures resulting from the sets originally introduced F. Ayissi Eteme [6]. This work consists in defining on FpZ the notion of Hamming code according to mΘ set structure. We show a relation between mΘ protocol F5 and Hamming mΘ code. By using this relation, we get a new steganography based on the bit modalities of a code word.

Keywords: mΘ set, Hamming mΘ codes, steganography, mΘ protocol F5.

I. INTRODUCTION

Steganography [5, 7] can be comparable to protection of communication, as it is known as a technique being used in order to protect some information to be exchanged by hiding its original existence, onto some digital files, could it be a photographies or videograms. As we know of cryptography as the technique and science behind the protection of messages and information to be transmitted, the idea for steganography is actually to prevent a nasty observer to even detect the need for that protection firstly, and it is also depending on the situations, as for instance in places where cryptography cannot be used.

Sometimes, it is also possible to mix together both techniques for protection of communication and information. The classic example known to illustrate use of a steganographic scheme is the prisoners problem exchanging messages under the surveillance of a warden. Crandall [10] was the first to suggest it and later Westfeld [11] applied it.

The $m\Theta$ codes [2, 12, 13, 14] present an enrichment from the logical viewpoint and we can mathematically express that an information is lightly, partially or greatly damaged.

Let E be a finite $m\Theta$ set. A non-empty subset $\mathcal{C}$ of E is called a $m\Theta$ code. E is the $m\Theta$ set of n-tuples from a finite $m\Theta$ set $\mathbb{F}_{p\mathbb{Z}}$ with p^2 elements. Each element of E is called $m\Theta$ words and the elements of $\mathcal{C}$, $m\Theta$ codewords. E is an n-dimensional vector space over $\mathbb{F}_{p\mathbb{Z}}$, so $E = V(n, p\mathbb{Z})$.

London Journal of Research in Science: Natural and Formal

Section 2 define firstly the modal Θ-valent set structure and the algebra of $(\mathbb{F}_{p\mathbb{Z}},\, F_\alpha)$, secondly the linear $m\Theta$ codes and lastly the Hamming $m\Theta$-distance of $(\mathcal{C},\, F^n_{\alpha|\mathcal{C}})$. Section 3 presents the Hamming codes on $V(n,\, 2\mathbb{Z})$. Section 4 is devoted to the $m\Theta$ steganographic protocol $F5$ and Hamming $m\Theta$ codes.

II. PRELIMINARIES

2.1 The modalΘ-valent set structure and the algebra of (FpZ; Fa)

Definition 0.1. *[15] Let $E \neq \emptyset$, I be a chain whose first and last elements are 0 and 1 respectively, $(F_\alpha)_{\alpha\in I_*}$ where $I_* = I \setminus \{0\} = \{f : E \longrightarrow E \mid f \text{ application}\}$.*

A $m\Theta$ set is the pair $\left(E,\, (F_\alpha)_{\alpha\in I_*}\right)$ or $(E,\, F_\alpha)$ such that :

- $\underset{\alpha}{\cap} F_\alpha(E) = \underset{\alpha\in I_*}{\cap} \{F_\alpha(x) : x \in E\} \neq \emptyset$;
- $\forall \alpha, \beta \in I_*$, *if* $\alpha \neq \beta$ *then* $F_\alpha \neq F_\beta$;
- $\forall \alpha, \beta \in I_*$, $F_\alpha \circ F_\beta = F_\beta$;
- $\forall x, y \in E$, *if* $\forall \alpha \in I_*, F_\alpha(x) = F_\alpha(y)$ *then* $x = y$.

Theorem 0.1. *[8]*

Let (E, F_α) be a $m\Theta$ set.

$$\forall x,\, y \in E,\, x =_\Theta y \iff \forall \alpha \in I_*,\, F_\alpha(x) = F_\alpha(y).$$

Proof 0.1. *[8]*

Definition 0.2. *[12] Let $\mathrm{C}(E, F_\alpha) = \underset{\alpha\in I_*}{\cap} F_\alpha(E)$. We call $\mathrm{C}(E, F_\alpha)$ the set of $m\Theta$ invariant elements of the $m\Theta$ set (E, F_α).*

Proposition 0.1. *[8] Let (E, F_α) be a $m\Theta$ set. The following properties are equivalent:*

1. $x \in \underset{\alpha\in I_*}{\cap} F_\alpha(E)$;
2. $\forall \alpha \in I_*,\, F_\alpha(x) = x$;
3. $\forall \alpha, \beta \in I_*,\, F_\alpha(x) = F_\beta(x)$;
4. $\exists \mu \in I_*,\, x = F_\mu(x)$.

London Journal of Research in Science: Natural and Formal

Proof 0.2. *[8]*

Definition 0.3. *[1]*
Let (E, F_α) and (E', F'_α) be two $m\Theta$ sets. We shall call

1. *(E', F'_α) a $m\Theta$ subset of (E, F_α) if the structure of $m\Theta$ set (E', F'_α) is the restriction to E' of the structure of the $m\Theta$ set (E, F_α), that means:*
   - $E' \subseteq E$;
   - $\forall \alpha : \alpha \in I_*,\ F'_\alpha = F_{\alpha|_{E'}}$.
2. *Let X be a non-empty set. X a $m\Theta$ subset of (E, F_α) if:*
   - $X \subseteq E$;
   - *$(X, F_{\alpha|_X})$ is a $m\Theta s$ which is a $m\Theta$ subset of (E, F_α).*

Let p be a prime number. Let us recall that if $a \in \mathbb{F}_{p\mathbb{Z}}$.

$$\mathbb{F}_{p\mathbb{Z}} = \mathbb{F}_p \cup \{x_{p\mathbb{Z}} : \neg\,(x \equiv 0\,(mod p))\}\,; \quad \mathbb{F}_p = \{0,\, 1,\, 2,\, \cdots,\, p-1\}.$$

Let us define $s(a)$ the $m\Theta$ support of a as follows:

$$s\,(a) = \begin{cases} a & if\ a \in \mathbb{F}_p; \\ x & if\ a = x_{p\mathbb{Z}}\ with\ \rceil(x \equiv 0\,(mod\, p))\,. \end{cases}$$

Thus $s\,(a) \in \mathbb{F}_p$.

Definition 0.4. *[15] Let $\perp$ be a binary operation on $\mathbb{F}_p$. So, $\forall a,\, b \in \mathbb{F}_p$, $a \perp b \in \mathbb{F}_p$. Let $x,\, y \in \mathbb{F}_{p\mathbb{Z}}$. We define a binary operation $\perp^*$ on $\mathbb{F}_{p\mathbb{Z}}$ as follows :*

$$x \perp^* y = \begin{cases} s(x) \perp s(y) & if \begin{cases} x, y \in \mathbb{F}_p \\ (s(x) \perp s(y)) \equiv 0\,(mod\, p) \quad otherwise \end{cases} \\ (s(x) \perp s(y))_{p\mathbb{Z}} & otherwise. \end{cases}$$

$\perp^*$ as defined above on $\mathbb{F}_{p\mathbb{Z}}$ will be called a $m\Theta$ law on $\mathbb{F}_{p\mathbb{Z}}$ $\forall x, y \in \mathbb{F}_{p\mathbb{Z}}$. So we can define $x + y \in \mathbb{F}_{p\mathbb{Z}}$ and $x \times y \in \mathbb{F}_{p\mathbb{Z}}$ $\forall x, y \in \mathbb{F}_{p\mathbb{Z}}$.

Theorem 0.2. *[1] $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha, +, \times)$ is a $m\Theta$ ring of unity 1 and of $m\Theta$ unity $\frac{1}{p\mathbb{Z}}$.*

Proof 0.3. *[1]*

Remark 0.1. *Since p is prime, $(\mathbb{F}_{p\mathbb{Z}},\, F_\alpha)$ is a $m\Theta$ field.*

Definition 0.5. *[6] x is a divisor of zero in $(\mathbb{F}_{p\mathbb{Z}},\, F_\alpha)$ if $\exists y \in \mathbb{F}_{p\mathbb{Z}}$ verifying $x \times y = 0$*

Example 0.1. *[6] By this example, we show that $\mathbb{F}_{p\mathbb{Z}}$, p prime, is a $m\Theta$ field of p^2 elements.*
$p = 2$, we have $\mathbb{F}_{2\mathbb{Z}} = \{0,\, 1,\, 1_{2\mathbb{Z}},\, 3_{2\mathbb{Z}}\}$

The table of $m\Theta$ determination and tables laws of $\mathbb{F}_{2\mathbb{Z}}$.

London Journal of Research in Science: Natural and Formal

$\mathbb{F}_{2\mathbb{Z}}$	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
F_1	0	1	1	*0*
F_2	0	1	0	*1*

$+^{\Theta}$	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
1	*1*	*0*	*0*	*0*
$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	*0*	*0*	*0*
$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	*0*	*0*	*0*

$\times^{\Theta}$	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	*0*	*0*	*0*	*0*
1	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$1_{2\mathbb{Z}}$	*0*	$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$3_{2\mathbb{Z}}$	*0*	$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$

2.2 Linear mΘ codes

Let (A, F_α) be a finite $m\Theta$ set. $\forall n \in \mathbb{N}^*$, we will denote in what follows the $m\Theta$ set product of (A, F_α) by (A^n, F_α^n); where F_α^n is the product on A^n of F_α. By definition, we have:

$$F_\alpha^n : A^n \longrightarrow A^n; \quad (a_1, \cdots, a_n) \longmapsto F_\alpha^n(a_1, \cdots, a_n) = (F_\alpha(a_1), \cdots, F_\alpha(a_n))$$

$k, n \in \mathbb{N}^*$ such that $k \leq n$.

Definition 0.6. *[14] Let us set $\mathcal{C} = f(E)$ the image of f. As f is injective, f is a $m\Theta$ bijection from E to $\mathcal{C}$. $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$ is considered as the $m\Theta$ set of all possible $m\Theta$ messages.*

1. *A $m\Theta$ code of length n and of alphabet (A, F_α), the $m\Theta$ set $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$.*
2. *Elements of $\mathcal{C}$, $m\Theta$ messages or $m\Theta$ words of the $m\Theta$ code $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$.*
3. *Elements of $\mathcal{C}$, $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}}) = \cap_{\alpha \in I_*} F_\alpha^n|_{\mathcal{C}}(\mathcal{C})$, messages or words of the $m\Theta$ code $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$.*

Proposition 0.2. *[12] $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$ is a $m\Theta$ part of (A^n, F_α^n).*

Proof 0.4. *[12]*

Proposition 0.3. *[12] Let $(\mathcal{C}, F_\alpha^n|_{\mathcal{C}})$ be a $m\Theta$ code of length n on (A, F_α). The set $C(\mathcal{C}, F_\alpha^n|_{\mathcal{C}}) = \cap_{\alpha \in I_*} F_\alpha^n|_{\mathcal{C}}(\mathcal{C})$ is a classical code of length n on $\cap_{\alpha \in I_*} F_\alpha(A) = C(A, F_\alpha)$.*

Definition 0.7. *[13] Let $(\mathbb{F}_{2\mathbb{Z}}, F_\alpha)$ be the $m\Theta$ field with $Card\,(\mathbb{F}_{2\mathbb{Z}}, F_\alpha) = 4$ $\forall \alpha \in I_*$,*

1. *Hamming α-weight of $x = (x_1, \cdots, x_n) \in (V(n, 2\mathbb{Z}), F_\alpha^n)$ is the number $\omega_{H_\alpha}(x) = \omega(F_\alpha^n(x))$, of non zero coordinates of $F_\alpha^n(x)$.*

$$\omega_{H_\alpha}(x) = \omega(F_\alpha^n(x)) = Card\{i \mid F_\alpha(x_i) \neq 0;\ i = 1, \cdots, n\}.$$

London Journal of Research in Science: Natural and Formal

2. *Hamming $m\Theta$-weight of $x = (x_1, \cdots, x_n) \in (V(n, 2\mathbb{Z}), F_\alpha^n)$ is the number $\omega_{H_\Theta}(x)$ and defined by:*

$$\omega_{H_\Theta}(x) = \begin{cases} \omega(x) & x \in \mathbb{F}_2^n; \\ \sum_{\alpha \in I_*} \omega_{H_\alpha}(x) = \sum_{\alpha \in I_*} \omega(F_\alpha^n(x)) & otherwise. \end{cases}$$

The alphabet used is the $m\Theta$ field $(\mathbb{F}_{p\mathbb{Z}} = (\frac{\mathbb{Z}_{p\mathbb{Z}}}{p\mathbb{Z}_{p\mathbb{Z}}}, F_\alpha))$.

Proposition 0.4. *[6] We set $E = V(k, p\mathbb{Z})$ and $\mathcal{C} = f(E)$. Let (E, F_α^k) be the $m\Theta$ set of $m\Theta$ message and f a linear $m\Theta$ encoder of (E, F_α^k) in $(V(n, p\mathbb{Z}), F_\alpha^n)$.*
Then, the $m\Theta$ code $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ is a $m\Theta$ vector subspace of $(V(n, p\mathbb{Z}), F_\alpha^n)$ over $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$.

Proof 0.6. *[6]*

Definition 0.8. *[14] A $m\Theta$ linear code of length n and of $m\Theta$ dimension k on $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$ is a $m\Theta$ vector subspace of $(V(n, p\mathbb{Z}), F_\alpha^n)$ of $m\Theta$ dimension k. .*

Proposition 0.5. *[6] Let $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ be a linear $m\Theta$ code of length n and of $m\Theta$ dimension k.*
Then $C(\mathcal{C}, F_{\alpha|\mathcal{C}}^n) = \cap_{\alpha \in I_*} F_\alpha^n(\mathcal{C})$ is a linear code of length n and of dimension k.

Proof 0.7. *[6]*

As $C(V(k, p\mathbb{Z}), F_\alpha^k)$ is a $\mathbb{F}_p$-vector space of dimension k, so $C(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ is a linear code of length n and $dim\,(C(V(k, p\mathbb{Z}), F_\alpha^k)) = dim\,(C(\mathcal{C}, F_{\alpha|\mathcal{C}}^n))$.

2.3 The Hamming $m\Theta$-distance of $(C; F\frac{n}{a}C)$

Let $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$ be a $m\Theta$ or a pseudo $m\Theta$ code on (A, F_α) of length n. In $(\mathcal{C}, F_{\alpha|\mathcal{C}}^n)$, let us define a notion compatible with the structure of $m\Theta$ code called $m\Theta$ distance.

$\forall \alpha \in I_*$, d_{H_α} on $A^n \times A^n$ is defined by:

$$\begin{aligned} d_{H_\alpha}(x, y) &= d_H(F_\alpha^n x, F_\alpha^n y) \\ &= card\{i : F_\alpha x_i \neq F_\alpha y_i\,;\, i = 1, \cdots, n\}. \end{aligned}$$

Where $x = (x_1, \cdots, x_n)$; $y = (y_1, \cdots, y_n)$ and d_H is the Hamming distance on $(C(A, F_\alpha))^n$.

Proposition 0.6. *If (A, F_α) is a $m\Theta$ set and $(\mathcal{C}, F_\alpha)$ is a $m\Theta$ code on (A, F_α), then*
$\forall x, y \in A^n$, d_{H_Θ} on $A^n \times A^n$ is defined by:

$$d_{H_\Theta}(x, y) = \begin{cases} d_H(x, y) & \text{if } x \text{ and } y \in (C(A, F_\alpha))^n; \\ \sum_{\alpha \in I_*} d_{H_\alpha}(x, y) = \sum_{\alpha \in I_*} d_H(F_\alpha x, F_\alpha y) & \text{otherwise.} \end{cases}$$

$F_\alpha^n x = (F_\alpha x_1, \cdots, F_\alpha x_n)$; $F_\alpha^n y = (F_\alpha y_1, \cdots, F_\alpha y_n)$. Then d_{H_Θ} is a $m\Theta$ distance on (A^n, F_α^n).

Proof 0.8. *[12]*

Definition 0.9. *d_{H_Θ} will be called the Hamming $m\Theta$ distance on (A^n, F_α^n).*

Definition 0.10. *Let $(\mathcal{C}, F_\alpha)$ be a $m\Theta$ code; d_{H_Θ} is the $m\Theta$ Hamming distance. We define δ^Θ as follows:*

$$\delta^\Theta = \min \{d_{H_\Theta}(x, y) : x, y \in \mathcal{C}; x \neq y\}.$$

δ^Θ is the minimal $m\Theta$ distance of the $m\Theta$ code $(\mathcal{C}, F_\alpha)$.

III. THE HAMMING MΘ CODES

3.1 Dual mΘ codes

Let $(\mathcal{C}, F_\alpha)$, $\forall \alpha \in I_*$, be a linear $m\Theta$ code in $V(n, p\mathbb{Z})$. Let G be a $m\Theta$ matrix whose rows generate $(\mathcal{C}, F_\alpha)$. Let G be a generating $m\Theta$ matrix of $(\mathcal{C}, F_\alpha)$.

The dual $m\Theta$ code of $(\mathcal{C}, F_\alpha)$, denoted $\mathcal{C}^\perp$, is defined as follows

$$\mathcal{C}^\perp = \{x \in V(n, p\mathbb{Z});\ \forall \alpha \in I_*\ , \langle F_\alpha x, F_\alpha c\rangle = 0,\ \forall c \in (\mathcal{C}, F_\alpha)\}$$

$\forall u, v \in V(n, p\mathbb{Z})$ $\langle u, v\rangle := u_1v_1 + u_2v_2 + \cdots + u_nv_n$. $\mathcal{C}^\perp$ is clearly also a linear $m\Theta$ code, and has a generating $m\Theta$ matrix H. By the definition of $\mathcal{C}^\perp$,

$$\mathcal{C} = \{c \in V(n, p\mathbb{Z})/\ \forall \alpha \in I_*,\ F_\alpha(c)H^t = 0\}.$$

Where H is a parity check $m\Theta$ matrix for $(\mathcal{C}, F_\alpha)$. If a $m\Theta$ word u is received, then it can be verified that u is a $m\Theta$ codeword such that $uH^t = 0$, i.e, $\forall \alpha \in I_*, F_\alpha(u)H^t = 0$.

London Journal of Research in Science: Natural and Formal

3.2 Hamming Codes on V (n; 2Z)

Hamming $m\Theta$ code is a linear $m\Theta$ code in $V(n, 2\mathbb{Z})$ for some $n \geq 2$. Let $\mathbb{F}_{2\mathbb{Z}}$ be the $m\Theta$ field of four elements and let H be the matrix whose columns are all the non-zero $m\Theta$ vectors of length k over $\mathbb{F}_{2\mathbb{Z}}$, $\forall k \leq n$. Note that there will be $2^k - 1$ of these. We define the Hamming $m\Theta$ code as follows:

Definition 0.11. *Let $k \geq 2$ and $n = 2^k - 1$. Let H denote the $k \times n$ $m\Theta$ matrix. The Hamming $m\Theta$ code, $Ham_{2\mathbb{Z}}(n)$, is the linear $m\Theta$ subspace of $V(n, 2\mathbb{Z})$ consisting of the set of all α-vectors, $\alpha \in I_*$, orthogonal to all the rows of H.*

$$Ham_{2\mathbb{Z}}(n) = \{v \in V(n, 2\mathbb{Z}) \,/\, \forall \alpha \in I_*,\, F_\alpha(v) \times H^t = 0\}.$$

Proposition 0.7. *The Hamming $m\Theta$ code $Ham_{2\mathbb{Z}}(n)$ is a $(2^k - 1, 2^k - k - 1, 3)$-code with $k \times (2^k - 1)$ parity check $m\Theta$ matrix .*

Proof 0.9. *[3]*

IV. THE MΘ STEGANOGRAPHIC PROTOCOL F5 AND HAMMING MΘ CODES

4.1 The mΘ protocol F5

$F5$ is a steganographic system developed by Westfeld in 2001 [11]. The $m\Theta$ protocol $F5$ over $\mathbb{F}_{2\mathbb{Z}}$ permits to hide $m\Theta$ messages of length k in cover $m\Theta$ words of length $n = 2^k - 1$ by partially or totally changing more than one of them .

Let $< F_\alpha^k m >_2$ be the α-binary word of m with k bits, $< m >_2 \in V(k, 2\mathbb{Z})$. Conversely, for $z \in V(k, 2\mathbb{Z})$, $\forall \alpha \in I_*$, let $< F_\alpha^k z >_{10}$ be an element of $\mathbb{F}_2^k$ which has $F_\alpha^k z$ as α-binary word, so $1 \leq < F_\alpha^k(z) >_{10} \leq 2^k - 1$.

Lastly, let e_i be the i^{th} α-vector of the canonical basis of $V(2^k - 1, 2)$; $e_0 = 0_{V(2^k-1,2)}$.

Proposition 0.8. *The $m\Theta$ maps $\gamma_{2\mathbb{Z}}$, $e_{2\mathbb{Z}}$, and $r_{2\mathbb{Z}}$ as follows define:*

(i)
$$\begin{array}{rcl} \gamma_{2\mathbb{Z}} : V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z}) & \longrightarrow & (\mathbb{N}_{2\mathbb{Z}}, F'_\alpha) \\ (x, m) & \longmapsto & (< F_\alpha^k(m) + \sum_{i=1}^{2^k-1} F_\alpha(x_i) < i >_2 >_{10})_{\alpha \in I_*} \end{array}$$

(ii)
$$\begin{array}{rcl} e_{2\mathbb{Z}} : V(2^k - 1, 2\mathbb{Z}) \times V(k, 2\mathbb{Z}) & \longrightarrow & V(2^k - 1, 2\mathbb{Z}) \\ (x, m) & \longmapsto & (F_\alpha^{2^k-1}(u) + e_{F'_\alpha(\gamma_{2\mathbb{Z}}(x,m))})_{\alpha \in I_*} \end{array}$$

(iii)
$$\begin{array}{rcl} r_{2\mathbb{Z}} : V(2^k - 1, 2\mathbb{Z}) & \longrightarrow & V(k, 2\mathbb{Z}) \\ x & \longmapsto & (\sum_{i=1}^{2^k-1} F_\alpha(x_i) < i >_2)_{\alpha \in I_*} \end{array}$$

are well defined and $m\Theta$.

London Journal of Research in Science: Natural and Formal

Proof 0.10.

(i) • *Let* $(x,\, m),\, (x',\, m') \in V(2^k-1,\, 2\mathbb{Z}) \times V(k,\, 2\mathbb{Z})$

let us suppose that $(x,\, m) = (x',\, m')$ *(* $x = x'$ *and* $m = m'$*) and let us show that* $\gamma_{2\mathbb{Z}}(x,\, m) = \gamma_{2\mathbb{Z}}(x',\, m')$.

$$(x,\, m) = (x',\, m') \Longrightarrow \forall \alpha \in I_* \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^k m = F_\alpha^k m' \end{cases}$$

$\forall \alpha \in I_*$;

$$F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 = F_\alpha^k t + \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2$$

$$\Longrightarrow < F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10} = < F_\alpha^k m' + \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2 >_{10}$$

$$\Longrightarrow (< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*} = (< F_\alpha^k m' + \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2 >_{10})_{\alpha \in I_*}$$

$$\Longrightarrow \gamma_{2\mathbb{Z}}(x,\, m) = \gamma_{2\mathbb{Z}}(x',\, t)$$

Therefore the map $\gamma_{2\mathbb{Z}}$ *is well defined.*

• *Let us verify* $\gamma_{2\mathbb{Z}}$ *is* $m\Theta$ *map.*

Let $(x,\, m),\, (x',\, m') \in V(2^k-1,\, 2\mathbb{Z}) \times V(k,\, 2\mathbb{Z})$
$\forall \alpha \in I_*$,

$$\begin{aligned} \gamma_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k)(x,\, m) &= \gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m) \\ &= (< F_\alpha^k(F_\alpha^k m) + \sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1}x)_i) < i >_2 >_{10})_{\alpha \in I_*} \\ &= (< F_\alpha^k m + \sum_{i=1}^{2^k-1} (F_\alpha^{2^k-1}x)_i < i >_2 >_{10})_{\alpha \in I_*} \\ &= (< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*} \\ F_\alpha' \circ \gamma_{2\mathbb{Z}}(x,\, m) &= F_\alpha'(< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*} \\ &= (< F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 >_{10})_{\alpha \in I_*} \end{aligned}$$

Therefore $\gamma_{2\mathbb{Z}}$ *is a* $m\Theta$ *map.*

London Journal of Research in Science: Natural and Formal

(ii) • $(x,\, m),\, (x',\, m') \in V(2^k-1,\, 2\mathbb{Z}) \times V(k,\, 2\mathbb{Z})$ *such that* $(x,\, m) = (x',\, m')$ *(* $x = x'$ *and* $m = m'$*), let's show that* $e_{2\mathbb{Z}}(x,\, m) = e_{2\mathbb{Z}}(x',\, m')$.

$$(x,\, m) = (x',\, m') \Longrightarrow \forall \alpha \in I_*,\ \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^k m = F_\alpha^k m' \end{cases}$$

$$\begin{aligned} \forall \alpha \in I_*,\ \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^k m = F_\alpha^k m' \end{cases} &\Rightarrow \quad \forall \alpha \in I_*,\ \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ \gamma_{2\mathbb{Z}}(x,\, m) = \gamma_{2\mathbb{Z}}(x',\, m') \end{cases} \\ &\Rightarrow \quad \forall \alpha \in I_*,\ \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ F_\alpha^{'}\gamma_{2\mathbb{Z}}(x,\, m) = F_\alpha^{'}\gamma_{2\mathbb{Z}}(x',\, m') \end{cases} \\ &\Rightarrow \quad \forall \alpha \in I_*,\ \begin{cases} F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x' \\ e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x,\, m)} = e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x',\, m')} \end{cases} \end{aligned}$$

$$\Rightarrow \quad \forall_\alpha^{I_*};\ F_\alpha^{2^k-1}x + e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x,\, m)} = F_\alpha^{2^k-1}x' + e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x',\, m')}$$

$$\Rightarrow \quad (F_\alpha^{2^k-1}x + e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x,\, m)} = F_\alpha^{2^k-1}x' + e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x',\, m')})_{\alpha \in I_*}$$

$$\Rightarrow \quad e_{2\mathbb{Z}}(x,\, m) = e_{2\mathbb{Z}}(x',\, m').$$

Therefore $e_{2\mathbb{Z}}$ *is well defined.*

- *Let us verify* $e_{2\mathbb{Z}}$ *is a* $m\Theta$ *map.*

Let $(x,\, m) \in V(2^k-1,\, 2\mathbb{Z}) \times V(k,\, 2\mathbb{Z})$

$$\begin{aligned} e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k)(x,\, m) &= e_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m) \\ &= (F_\alpha^{2^k-1}(F_\alpha^{2^k-1}x) + e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m)})_{\alpha \in I_*} \\ &= (F_\alpha^{2^k-1}x + e_{F_\alpha^{'}\gamma_{2\mathbb{Z}}(x,\, m)})_{\alpha \in I_*} \quad (\ \gamma_{2\mathbb{Z}} \text{ is } m\Theta \text{ map}). \end{aligned}$$

$$\begin{aligned} F_\alpha^{'} \circ e_{2\mathbb{Z}}(x,\, m) &= F_\alpha^{'}(F_\alpha^{2^k-1}x + e_{F_\alpha^{'}(\gamma_{2\mathbb{Z}}(x,\, m))})_{\alpha \in I_*} \\ &= (F_\alpha^{2^k-1}x + e_{F_\alpha^{'}(\gamma_{2\mathbb{Z}}(x,\, m))})_{\alpha \in I_*}. \end{aligned}$$

Therefore;

$$e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k) = F_\alpha^{'} \circ e_{2\mathbb{Z}}.$$

(iii) • *Let us show that* $r_{2\mathbb{Z}}$ *is well defined.*

Let us suppose that $x = x'$ *(* $F_\alpha^{2^k-1}x = F_\alpha^{2^k-1}x'$*) and let us show that* $r_{2\mathbb{Z}}x = r_{2\mathbb{Z}}x'$.
Let $\alpha \in I_*$;

$$\begin{aligned} F_\alpha^{2^k-1}(x) = F_\alpha^{2^k-1}(x') &\Rightarrow F_\alpha x_i = F_\alpha x_i' \\ &\Rightarrow F_\alpha x_i < i >_2 = F_\alpha y_i < i >_2 \\ &\Rightarrow \sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2 = \sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2 \\ &\Rightarrow (\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha \in I_*} = (\sum_{i=1}^{2^k-1} F_\alpha x_i' < i >_2)_{\alpha \in I_*} \\ &\Rightarrow r_{2\mathbb{Z}}(x) = r_{2\mathbb{Z}}(x') \end{aligned}$$

Therefore $r_{2\mathbb{Z}}$ is a $m\Theta$ map.

- *Let us show that $r_{2\mathbb{Z}}$ is $m\Theta$ map.*

  Let $x \in V(2^k-1,\, 2\mathbb{Z})$, let $\alpha \in I_*$.

$$\begin{aligned} r_{2\mathbb{Z}} \circ F_\alpha^{2^k-1}(x) &= r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x) \\ &= (\sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1}x)_i) < i >_2)_{\alpha\in I_*} \\ &= (\sum_{i=1}^{2^k-1} F_\alpha(F_\alpha x_i) < i >_2)_{\alpha\in I_*} \\ &= (\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha\in I_*} \end{aligned}$$

$$\begin{aligned} F_\alpha^{'} \circ r_{2\mathbb{Z}}(x,\, m) &= F_\alpha^{'}((\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha\in I_*}) \\ &= (\sum_{i=1}^{2^k-1} F_\alpha x_i < i >_2)_{\alpha\in I_*} \end{aligned}$$

Therefore $r_{2\mathbb{Z}}$ is a $m\Theta$ map.

Proposition 0.9. *$(e_{2\mathbb{Z}},\, r_{2\mathbb{Z}})$ before define in the proposition 0.8 is a $m\Theta$ steganographic protocols.*

Proof 0.11. *Let's show that $(e_{2\mathbb{Z}},\, r_{2\mathbb{Z}})$ is a $m\Theta$ steganographic protocol. In other words, $r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x,\, m)) = m$, for any $m \in \mathbb{F}_{2\mathbb{Z}}^k$ and for any $x \in V(2^k-1,\, 2\mathbb{Z})$.*
So, $\forall \alpha \in I_*$, $F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x,\, m))) = F_\alpha^k(m)$.

1.

$$\begin{aligned} F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x,\, m))) &= r_{2\mathbb{Z}}(F_\alpha^{2^k-1} \circ e_{2\mathbb{Z}}(x,\, m))\ (r_{2\mathbb{Z}} \text{ is } m\Theta \text{ map}) \\ &= r_{2\mathbb{Z}}(e_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k))(x,\, m)\ (e_{2\mathbb{Z}} \text{ is a } m\Theta \text{ map}) \\ &= r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m)) \\ &= r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_{F_\alpha^{'}(\gamma_{2\mathbb{Z}}(x,\, m))}). \end{aligned}$$

London Journal of Research in Science: Natural and Formal

we put

$$\begin{aligned} j = F'_\alpha(\gamma_{2\mathbb{Z}}(x,\, m)) &= \gamma_{2\mathbb{Z}} \circ (F_\alpha^{2^k-1},\, F_\alpha^k)(x,\, m) \\ &= \gamma_{2\mathbb{Z}}(F_\alpha^{2^k-1}x,\, F_\alpha^k m) \\ &= < F_\alpha^k(F_\alpha^k m) + \sum_{i=1}^{2^k-1} F_\alpha((F_\alpha^{2^k-1}x)_i) < i >_2 >_{10} \\ &= < F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha(F_\alpha x_i) < i >_2 >_{10} \\ &= < F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha(x_i) < i >_2 >_{10} \end{aligned}$$

$$\textit{then} < j >_2 = F_\alpha^k m + \sum_{i=1}^{2^k-1} F_\alpha(x) < i >_2 \qquad (*)$$

2.

$$\begin{aligned} r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_j) &= r_{2\mathbb{Z}}(F_\alpha x_1,\, F_\alpha x_2, \cdots, F_\alpha x_j + 1, \cdots, F_\alpha x_n) \\ &= \sum_{i=1,\, i\neq j}^{2^k-1} \{F_\alpha(F_\alpha x_i) < i >_2 + (F_\alpha x_j + 1) < j >_2\} \\ &= \sum_{i=1,\, i\neq j}^{2^k-1} \{F_\alpha(x_i) < i >_2 + (F_\alpha x_j + 1) < j >_2\} \end{aligned}$$

changing $< j >_2$ *by expression given in* $(*)$ *we get:*
$r_{2\mathbb{Z}}(F_\alpha^{2^k-1}x + e_j) = F_\alpha^k m$; *so*

$$\forall \alpha \in I_*,\, F_\alpha^k(r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x,\, m))) = F_\alpha^k(x,\, m).$$

Therefore, $r_{2\mathbb{Z}}(e_{2\mathbb{Z}}(x,\, m)) = (x,\, m)$. *Thus* $m\Theta$ *protocol* $F5$ *is a* $m\Theta$ *steganographic protocol.*

Remark 0.2. *1. Embed a* $m\Theta$ *message* s *by the* $m\Theta$ *steganographic protocol* $F5$ *in a* $m\Theta$ *cover* u *consists to swap the* $m\Theta$ *coordinate number* $\gamma_{2\mathbb{Z}}(u,\, s)$.

2. *mΘ extraction consists to add all products of each α-component, $\forall \alpha \in I_*$, to the value of the $F_{2\mathbb{Z}}$ expression of the index. In other words,*

$$r_{2\mathbb{Z}}(u) = \sum_{i=1}^{2^k-1} F_\alpha u_i < i >_2 .$$

Example 0.2. *Let $[7, 4]_{2\mathbb{Z}}$ be a Hamming code, $k = 3$. We want to insert $m = 01_{2\mathbb{Z}}1_{2\mathbb{Z}}$ into $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$ by the mΘ steganographic protocol F5.*
$F_1^3 m = 011$, $F_2^3 m = 000$, $F_1^7 x = 1100001$, $F_2^7 x = 0000100$.
So, how to calculate $e_{2\mathbb{Z}}(01_{2\mathbb{Z}}1_{2\mathbb{Z}}, 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}})$.

$$\begin{aligned}\gamma_{2\mathbb{Z}}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}, 01_{2\mathbb{Z}}1_{2\mathbb{Z}}) &= (< F_1^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_1 x_i < i >_2 >_{10}, \\ &\quad < F_2^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_2 x_i < i >_2 >_{10})\end{aligned}$$

$$\begin{aligned}< F_1^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_1 x_i < i >_2 >_{10} &= < 011 + 1(001) + 1(010) + 1(111) >_{10} \\ &= 7\end{aligned}$$

and

$$\begin{aligned}< F_2^3(01_{2\mathbb{Z}}1_{2\mathbb{Z}}) + \sum_{i=1}^{7} F_2 x_i < i >_2 >_{10} &= < 000 + 1(101) >_{10} \\ &= 5.\end{aligned}$$

$$\gamma_{2\mathbb{Z}}(x, m) = (7; 5) = (F_1^{'}(\gamma_{2\mathbb{Z}}(x, m)); F_2^{'}(\gamma_{2\mathbb{Z}}(x, m))).$$

$$e_{2\mathbb{Z}}(x, m) = (F_1^7 x + e_{F_1^{'}(\gamma_{2\mathbb{Z}}(x,m))}; F_2^7 x + e_{F_2^{'}(\gamma_{2\mathbb{Z}}(x,m))})$$

$$F_1^7 x + e_{F_1^{'}(\gamma_{2\mathbb{Z}}(x,m))} = 1100001 + e_7 = 1100001 + 0000001 = 1100000.$$

$$F_2^7 x + e_{F_2^{'}(\gamma_{2\mathbb{Z}}(x,m))} = 0000100 + e_5 = 0000100 + 0000100 = 0000000.$$

$$\begin{aligned}e_{2\mathbb{Z}}(x, m) &= (1100000, 0000000) \\ &= 1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000 \\ &= v.\end{aligned}$$

London Journal of Research in Science: Natural and Formal

Now, we will extract the $m\Theta$ message hidden m in the $m\Theta$ stego-word $y = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000$.

In other words, how to calculate $r_{2\mathbb{Z}}(1_{2\mathbb{Z}}1_{2\mathbb{Z}}00000)$? By definition of $r_{2\mathbb{Z}}$ given in the remark 0.3.:

$$r_{2\mathbb{Z}}(y) = (\sum_{i=1}^{7} F_1 y_i < i >_2, \sum_{i=1}^{7} F_2 y_i < i >_2)$$

$$\begin{aligned} r_{2\mathbb{Z}}(y) &= (1(001) + 1(010);\ 1(000)) \\ &= (011;\ 000) \\ &= 01_{2\mathbb{Z}}1_{2\mathbb{Z}} \\ &= m. \end{aligned}$$

4.2 The F5 mΘ Algorithm

To increase embedding efficiency, the $F5$ algorithm introduces for the first time the concept of matrix embedding technique for embedding in the context of using Hamming codes.

More formally, the desired purpose of the matrix $m\Theta$ embedding technique is to communicate a $m\Theta$ message $m \in V(n-k,\ p\mathbb{Z})$ through the cover $m\Theta$ vector $x \in V(n,\ p\mathbb{Z})$, modifying it as little as possible.
The principle is to change the cover $m\Theta$ vector x to stego $m\Theta$ vector y, such that:

$$H(F_\alpha y)_{\alpha \in I_*} = (F_\alpha m)_{\alpha \in I_*},$$

with $H \in \mathcal{M}_{n-k,n}$ the parity check matrix of Hamming $m\Theta$ code. The $m\Theta$ transformation of the cover $m\Theta$ vector x into y is then carried out by seeking the $m\Theta$ vector of modification $e \in V(n,\ p\mathbb{Z})$:

$$(F_\alpha y)_{\alpha \in I_*} = (F_\alpha(x+e))_{\alpha \in I_*};$$

$$H(F_\alpha(x+e))_{\alpha \in I_*} = (F_\alpha m)_{\alpha \in I_*} \Longleftrightarrow H(F_\alpha e)_{\alpha \in I_*} = (F_\alpha m)_{\alpha \in I_*} - H(F_\alpha x)_{\alpha \in I_*}.$$

Example 0.3. *Taking $[7,\ 4]$ Hamming $m\Theta$ code, we explain how to embed 3 $m\Theta$ bits of $\mathbb{F}_{2\mathbb{Z}}$ into 7 pixels. Let $m = 01_{2\mathbb{Z}}1_{2\mathbb{Z}}$ be the $m\Theta$ message that we want to insert in the cover $m\Theta$ vector $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$. The parity check matrix is therefore in the following form:*

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

The purpose is to find the α*-vector* $e = (e_1, e_2, e_3, e_4, e_5, e_6, e_7)$ *such that* $H(x + e) = m$.
Otherwise,

$$\begin{cases} F_1(m) = 0\,1\,1, \quad F_2(m) = 0\,0\,0. \\ F_1(x) = 1\,1\,0\,0\,0\,0\,1, \quad F_2(x) = 0\,0\,0\,0\,1\,0\,1. \end{cases}$$

So,

$$\begin{aligned} F_1(m) - H \times F_1(x) &= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}. \end{aligned}$$

Thus, the modification α*-vector is* $F_1(e) = (0, 0, 0, 0, 0, 0, 1)$.

$$\begin{aligned} F_2(m) - H \times F_2(x) &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}. \end{aligned}$$

Thus, $F_2(e) = (0, 1, 0, 0, 0, 0, 0)$.

$$e = (F_1(e), F_2(e)) = (0, 3_{2\mathbb{Z}}, 0, 0, 0, 0, 1_{2\mathbb{Z}}).$$

London Journal of Research in Science: Natural and Formal

The cover $m\Theta$ vector x is then transformed into

$$\begin{aligned} y = x + e &= 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}} + 03_{2\mathbb{Z}}00001_{2\mathbb{Z}} \\ &= 1_{2\mathbb{Z}}0003_{2\mathbb{Z}}00 \end{aligned}$$

We have the cover $m\Theta$ vector $x = 1_{2\mathbb{Z}}1_{2\mathbb{Z}}003_{2\mathbb{Z}}01_{2\mathbb{Z}}$ and the stego $m\Theta$ vector $y = 1_{2\mathbb{Z}}0003_{2\mathbb{Z}}00$. When embedding m into x, it appears that 2 pixels of x have been partially damaged, namely the second and the last component of x. Indeed,

$$\begin{cases} 1_{2\mathbb{Z}} = (F_\alpha 1_{2\mathbb{Z}})_{\alpha\in I_*} = (F_1 1_{2\mathbb{Z}},\ F_2 1_{2\mathbb{Z}}) = (1,\ 0) \\ 0 = (F_\alpha 0)_{\alpha\in I_*} = (F_1 0,\ F_2 0) = (0,\ 0) \end{cases}$$

The passage from $1_{2\mathbb{Z}}$ to 0 shows that the pixels has been partially damaged.

V. CONCLUSION

This note shows that the Hamming $m\Theta$ code is a $\mathbb{F}_{2\mathbb{Z}}$-vector subspace of $V(n,\ 2\mathbb{Z})$ of dimension n. It appears that there exists a close relation between the $m\Theta$ protocols $F5$ and the Hamming $m\Theta$ code. The embedding of a $m\Theta$ message of k bits into the cover $m\Theta$ vector of n pixels changes at the level of the α-modalities because it partially or totally damages at most one pixel of the cover $m\Theta$ vector.

REFERENCES

1. F. Ayissi Eteme, chrm_ introducing pure and applied mathematics, Lambert academic publishing saarbruken, Germany, 2015.
2. J.A. Tsimi and Rose Youdom, The modal _Θvalent extensions of BCH codes, Journal of Interdisciplinary mathematics, May 2021.
3. Sky McKinley, The Hamming codes and Delsarte's Linear Programming Bound, Master thesis at Portland State University, 2003.
4. J.A. Tsimi and G. Pemha, A mΘ spectrum of Reed-Muller codes, Journal of Discrete Mathematical Sciences and Cryptography (JDMSC), 2021.
5. F. Petitcolas, R. Anderson, M. Kuhn,Information hiding. A survey, Proc. IEEE 87 (1999) 1062 - 1078.
6. F.A. Eteme and J.A. Tsimi, A mΘ approach of the algebraic theory of linear codes, Journal of Discrete Mathematical Sciences and Cryptography, vol.14 (2011), N_. 6, pp. 559-581.
7. W. Bender et al., Applications for data hiding, IBM Systems J 39 (2000) 547- 568.
8. F. Ayissi Eteme, Logique et Algèbre de structure mathé matiques modales _Θvalentes chrysippiennes, Edition Hermann, Paris, 2009.
9. F. Ayissi Eteme, Complétion chrysippienne d'une algèbre de Lukasiewicz _Θvalent CRAS Paris, 299, série 1(3), 1984, pp. 69 - 72.
10. R. Crandall, Some notes on steganography, 1998.
11. A. Westfeld, F5. High capacity despite better steganalysis, in: Lecture Notes in Computer Science, vol. 2137, Springer, New York, 2001, pp. 289 - 302.

This page is intentionally left blank