International Journal of Applied Mathematics

Volume 31 No. 2 2018, 279-288
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v31i2.9

IMAGE ENCRYPTION USING THE INCIDENCE MATRIX

Abdelghni Lakehal[1] §, Abdelkarim Boua[2]

[1]Abdelmalek Essaadi University
Polydisciplinary Faculty
MAE2D, Larache, MOROCCO

[2]Sidi Mohammed Ben Abdellah University
Polydisciplinary Faculty
LSI, Taza – MOROCCO

Abstract: The purpose of this article is to indicate the importance of using close planar rings in the construction of high efficiency balanced incomplete block (BIBD) plans, and how these can be used to encrypting the image. Therefore, an algorithm of a program to compute the incidence matrix plays a very important role in encrypting and decrypting images.

AMS Subject Classification: 16N60, 16W25, 16U80
Key Words: planar near-ring, BIBD, image encrypting

1. Introduction and motivation

Near-rings are one of the generalized structures of rings. The study and research on near-rings is very systematic and continuous. Near-ring have been used since the development of calculus, but the key idea behind near-rings was formalized in 1905 by Dickson who defined the near-fields. Veblin and Wedderburn used Dickson's near-field to give examples of Nondesarguesian planes. In late 1930s, Wieland studied near-rings, which were not near-fields. Extensive studies about the subject can be found in two famous books on near-rings (see [7]). Near-rings abound in all directions of mathematics and continuous research is being

Received: February 18, 2018

§Correspondence author

conducted, which shows that their structure has power and beauty in all its own. Importantly, the study of the theory of planar near-rings has received momentum in the last decades. Various applications of planar near-rings have been applied in different fields (see [4], [7]).

The combinatorial design theory may seem like an area of math for solving puzzles or brainteasers. However, what if the theory itself had various applications in encrypting and decrypting images.? The aim of this essay was to determine how could balanced incomplete block designs be applied in in encrypting and decrypting images.

After the fundamentals theory had been established, a method for transforming (BIBD) into an incidence matrix was outlined. This transformation allowed the matrix to contain only binary digits while retaining the properties of (BIBD), allowing the rows or the columns of the matrix to be used as codes. These properties were later utilized to depict that error detection and correction can be done at a faster and efficient rate when the codes were generated from (BIBD).

2. Definitions and terminology

Recall that a right (resp. left) near-ring is a set $\mathcal{N}$ together with two binary operations " + " and "." such that

(i) $\mathcal{N}$ is a group (not necessarily abelian).

(ii) $\mathcal{N}$ is a semigroup.

(iii) For all $x, y, z \in \mathcal{N}$, $(x + y)z = xw + yz$ (resp. $z(x + y)z = zx + zy$).

Now we remind some definitions and properties of near-rings, for details see [4].

Definition 1. For a near-ring $(\mathcal{N}, +, .)$ and $a, b \in \mathcal{N}$, define an equivalence relation $\Re$ on $\mathcal{N}$ by:

$$a\Re b \Leftrightarrow xa = xb \quad \text{for all} \quad x \in \mathcal{N}.$$

If $a\Re b$, we say that a and b are equivalent multipliers.

Definition 2. A near-ring $(\mathcal{N}, +, .)$ is said to be planar if:

(i) has at least three equivalence classes, i.e., $N/\Re \geq 3$.

(ii) For constants $a, b, c \in \mathcal{N}$ where a is not equivalent to b, the equation $x.a + x.b = c$ has a unique solution for $x \in \mathcal{N}$.

The theory of codes and design has developed dramatically for the past few decades having vast amount of applications in current technology. Combinatorial design theory lies in heart of coding theory. There exists various designs but this essay would only consider one of its fundamental design, balanced incomplete block designs, as the concepts of designs are new. Before the research question "How could balanced incomplete block designs be applied in error detection and correction" is answered, what are error detection and correction and balanced incomplete block designs?

Definition 3. A balanced incomplete block design (BIBD) with parameters (v, b, r, k, λ) is a pair (P, B) with the following properties:

(i) P is a set with v elements.

(ii) $B = \{B_1, B_2, ..., B_b\}$ is a subset of P with b elements are called the blocks a (BIBD).

(iii) Each B_i has exactly k elements where $k < v$ each unordered pair (p, q) with $p, q \in P$, $p \neq q$ occurs in exactly λ elements in B.

Each $a \in P$ occurs in exactly r sets of B. The term balance indicates that each pair of elements occurs in exactly the same number of block, the term incomplete means that each block contains less than v elements.

The main parameters of a (BIBD) are (v, b, r, k, λ) and the parameters satisfy the following necessary conditions for existence.

(1) $vr = kb$;

(2) $\lambda(k-1) = v(k-1)$.

There are good construction methods for obtaining planar near-rings. We exhibit the following one, due to Clay (see [2], [3], [4], [5]), which is both easy and most useful.

Theorem 4. *Let F be a field of order p^n, where p is a prime and let t be a nontrivial divisor of $p^n - 1$, so $st = p^n - 1$ for some s. Choose a generator g of the multiplicative group of F. Define $g^a ._t g^b = g^{a+b-[b]_s}$, where $[b]_s$ denotes the residue class of a modulo s. Then $(F, +, ._t)$ is a planar near-ring with $N^* = N - \{0\}$.*

3. Construction the incidence matrix from planar near-rings

The planar near-rings theory is also used in the construction of balanced incomplete block designs (BIBD) of high efficiency where by high efficiency "E" we mean $E = \frac{\lambda v}{rk}$, this E is a number between 0 and 1 and it estimates the quality of any statistical analysis if $E \geq 0,75$ the quality is good. According to [3], the construction of a (BIBD) from a planar near-ring can be obtained as follows:

Theorem 5. *Let $\mathcal{N}$ be a finite planar near-ring and $B = \{a\mathcal{N}^* + b \mid a, b \in \mathcal{N}, a \neq 0\}$, then $(\mathcal{N}, B)$ is a (BIBD) with parameters $(v, \frac{v(v-1}{k}, v-1, k, k-1)$, where $v = |N|$ and k is the cardinality of each aN^* with $a \neq 0$.*

It is often convenient to represent a (BIBD) by means of an incidence matrix. This is especially useful for computer programs. Here we recall the definition of an incidence matrix.

Definition 6. Let (P, B) be a (BIBD) where $P = \{p_1, ..., p_v\}$ and $B = \{B_1, ..., B_b\}$. The incidence matrix of (P, B) is the $v \times b$ matrix $M = m_{ij}$ defined by the rule

$$m_{ij} = \begin{cases} 1, & \text{if } p_i \in B_j; \\ 0, & \text{otherwise.} \end{cases}$$

The incidence matrix M of a (v, b, r, k, λ)-BIBD satisfies the following properties:

(i) every column of M contains exactly k"1" s.

(ii) every row if M contains exactly r"1" s.

(iii) two distinct rows of M both contain "1" s in exactly λ columns.

Now using the planar near-rings one can construct error correcting codes from (BIBD). Indeed, by taking either the rows or columns of the incidence matrix of such a (BIBD) one can obtain binary codes called the row code C_{rowB} or (column code C_{colB}, respectively) of B with several features.

Proposition 7. ([6]). *Let the notation be as in Definition 3.*

(i) *C_{rowB} has v codewords of length b, equal weight r and minimal distance $2(r - \lambda)$.*

(ii) *C has b codewords of length v, equal weight k and minimal distance* $(k-m)$*, where* $m = max_{i \neq j}|B_i \cap B_j|$.

(iii) *Neither* C_{rowB} *nor* C_{colB} *can be linear.*

Algorithm [1]:
Input: m integer number
Output: incidence matrix.
If $m = p^n$, then:
1. Define a field F of order p^n.
i) t : divisor of $p^n - 1$ such that $st = p^n - 1$.
ii) g : multiplicative generator of F.
2. Define law "$._t$" Such that: $g^a ._t g^b = g^{a+b-[b]_s}$, where $[b]_s$ denotes the residue class of b modulo s. Then $N = (F, +, ._t)$ is a planar near-ring.
3. The construction of "BIBD".

- $B = \{\alpha N^* + \beta \mid \alpha, \beta \in N, \alpha \neq 0\}$.
- $v \longleftarrow card(N)$;
- $k \longleftarrow card(\alpha N^*)$;
- $b \longleftarrow \frac{v(v-1)}{k}$;
- $r \longleftarrow v - 1$;
- $\lambda \longleftarrow k - 1$;

(v, b, r, k, λ) (BIBD) parameters of (N, B).
4. The construction of the incidence matrix.
For $i = 1 : v$
For $j = 1 : b$
$m_{i,j} = \begin{cases} 1, & \text{if } i \in B_j \text{ or } i \in N \text{ and } B_j \in B \ ; \\ 0, & \text{if not.} \end{cases}$
End for.
End for.
Otherwise, we take the largest prime divisor of n and we apply the same algorithm.

Example: Using this algorithm where $p = 11$, then $t = 5$, $s = 2$ and $g = 2$. The incidence matrix of order 11×22 is giving by:

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

From this matrix we extract 11 codewords and each codewords is row of the incidence matrix of length 22, weight 10 and minimum distance is 12. Similarly, we extract a column code with 22 codewords, and each codewords represents a column of the incidence matrix of length 11, and its weight 5 and minimum distance is 2. Hence the row code can detect 11 errors and correct 5 errors, and the column code can detect a single error but it doesn't correct any error. On the other hand we found that the effectiveness of this (BIBD), $E = 0.88 \geq 0.75$, thus indicating that its quality is good.

4. Encryption and decryption by line codes and column codes of the incidence matrix

The idea of our method is to build a mask based on the incidence matrix presented in Section 3. Given an image I to be encrypted, from the incidence matrix we construct the mask M with the same size as the target image I, the encrypted image R is obtained by the logical connector "*xor*" between the image I and the mask M as follow:

$$R = I \; xor \; M \, . \tag{1}$$

The mask obtained from the incidence matrix is binary, this requires that the image to been crypt is also obinary, for this reason the encryption of a binary image is done in a systematic manner using the equation (1). In **Fig. 1**, the sub-figure (a) represents a binary image, the sub-figure (b) represents the mask constructed by the incidence matrix of size $7 * 14$ and as a result, the encrypted image is obtained in the sub-figure (c). In this case, the incidence matrix is constructed by the line codewords. **Fig. 2** shows the same target image but the mask is obtained by the column code words.

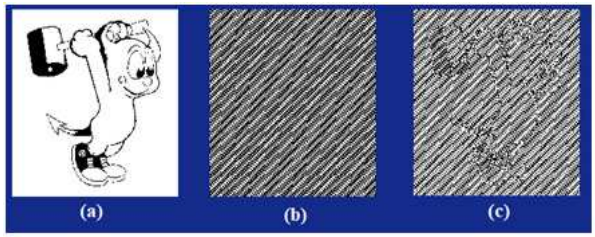

Fig. 1: Encryption with the code lines of the incidence matrix.

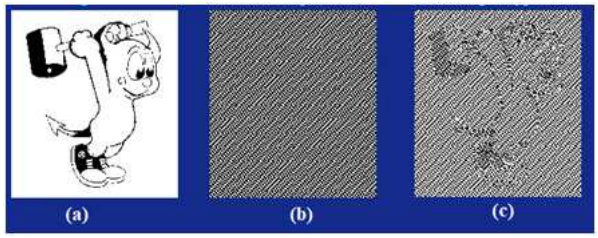

Fig. 2: Encryption with the code column of the incidence matrix.

The next figure (**Fig. 3**) represents the encryption of an image with different masks. As this figure shows, the degree of encryption increases proportionally with the group order n. This figure represents 3 cases according to the group order, in $(A1)$ the mask constructed from the incidence matrix using a group of order 5, the image $B1$ represents the encrypted image of the target image the same for the other two where $n = 13$ and $n = 29$ respectively. We can easily notice that the image becomes totally hidden when the group order is increased, for $n = 29$ the encrypted image becomes perfectly hidden.

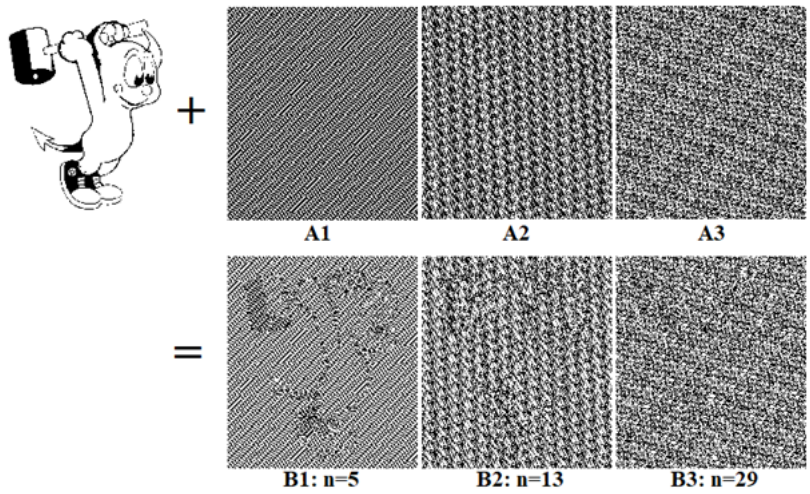

Fig. 3: Encryption according to different masks.

As we have mentioned, the encryption of a binary image is done in a systematic way by the "*xor*" logical connector between the mask and the target image, on the other hand in the case where the image is in gray level, the encryption process is done by the following steps:

(1) we decompose the grayscale images into 8 binary images where each pixel in the image breaks down into 8 bits and each bit corresponds to a binary image.

(2) The encryption of the 8 binary images is done by the same mask

(3) The encrypted image is constructed by assembling the eight encrypted images obtained using the inverse operation of the (phase I), the figure (**Fig. 4**) summarizes this procedure.

In the case of grayscale image there is no need for a high group order for encryption, just use an order greater than or equal to 7 to have a totally hidden encrypted image. In **Fig. 4**, the target image is decomposed into eight binary images (phase I) and then the encrypted images are obtained by the "*xor*" logical operation of the mask with each image (phase II), the assembly of these images encrypted by the reverse operation of (phase I) gives the encrypted image (phase III).

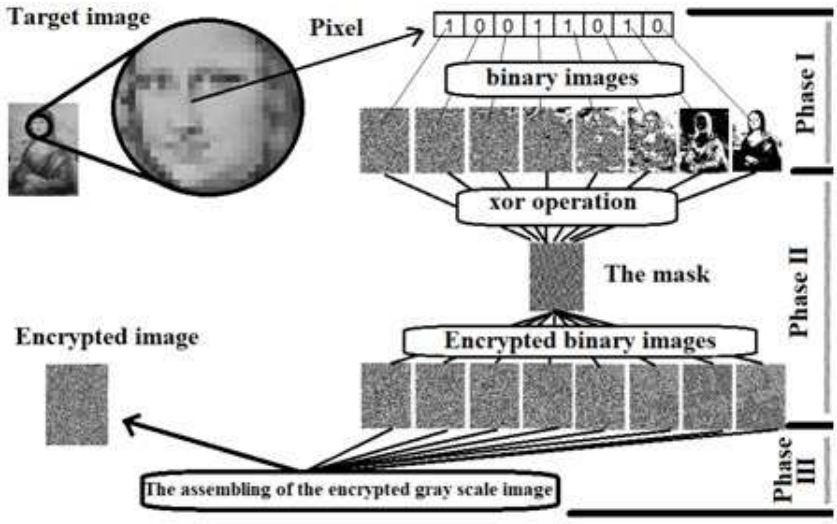

Fig. 4: Grayscale image encryption with group order $n = 7$.

In the case of a color image, the image is decomposed into three images, red, green, blue, then the method used in the case of grayscale image for each of these three images is used to obtain the encrypted image.

5. Conclusion

In these papers we presented a method to encrypt a binary image, gray level or color image, the method is based on the incidences matrix obtained by the (BIBD) of a planar nears-ring. Among the strong points of our method is the difficulty of decrypting the encrypted images without having the mask used in encryption or even impossible as well as the calculations in the encryption phase are very small which makes the complexity of the algorithm is polynomial all it gives our proposed method efficiency and robustness.

References

[1] A. Boua, L. Oukhtite, A. Raji & O. Ait Zemzami, An algorithm to construct error correcting codes from planar near-rings, *Inter. J. of Math. Engineering & Sci.*, **3**, No 1, (2014), 14-23.

[2] J.R. Clay, Generating balanced incomplete block designs from planar near-rings, *J. Algebra*, **22** (1972), 319-331.

[3] J.R. Clay, Geometric and combinatorial ideas related to circular planar nearrings, *Bull. of the Institute of Math. Academia Sinica*, **16** (1988), 275-283.

[4] J.R. Clay, *Near-rings: Geneses and Applications*, Oxford University Press, 1992.

[5] J.R. Clay, Geometry in fields, *Algebra Colloq.*, **1**, No 4 (1994), 289-306.

[6] P. Fuchs, G. Hofer & G. Pilz, Codes from planar near-rings, *IEEE Trans. Inform. Theory*, **36** (1990), 647-651.

[7] G. Pilz, *Near-rings*, North Holland and American Elsevier, Amsterdam, 2nd Revis. Ed. (1983).