Gulf Journal of Mathematics
Vol 24, Issue 2 (2026) 1-14

ISSN: 2309-4966
https://doi.org/10.56947/x4bnxp71

NON-MONOTONIC XOR VISUAL CRYPTOGRAPHY VIA KRAWTCHOUK NUMBERS

HASNAE CHIHI[1], ASAAD CHAHBOUN[1] and SOUFIANE MEZROUI[2*]

Abstract. Classical visual cryptography is monotonic: once a set of shares reveals the secret, every larger set reveals it too. XOR-based schemes can be non-monotonic, revealing the secret for exactly three of four shares, but such schemes have so far been found only by hand. We show that prescribing the contrast for every number of combined shares reduces to a linear system whose matrix is always invertible, with an explicit inverse given by Krawtchouk numbers. Basis matrices realizing any prescribed behavior follow from one matrix-vector product. We also give integrality conditions and explicit examples.

Keywords. Visual cryptography, XOR-based scheme, non-monotonic access structure, Krawtchouk numbers, basis matrices
2020 Mathematics Subject Classification. Primary 94A60; Secondary 15A06, 05A10

1. Introduction and preliminaries

Visual cryptography, introduced by Naor and Shamir [1], encodes a binary image into n shares in such a way that a qualified collection of shares recovers the image by a purely optical operation, while an unqualified collection reveals nothing. In the classical (k, n)-threshold model the qualified sets are exactly those of size at least k. This access structure is *monotonic*: every superset of a qualified set is qualified. The same monotonicity is built into the general access structures of Ateniese, Blundo, De Santis and Stinson [2].

Monotonicity is natural for secret sharing, where reconstruction should become possible as soon as enough parties cooperate. It is less natural for *authentication*, where a legitimate reconstruction should occur under precisely specified conditions and under no others. Motivated by this, recent work [3, 4] constructs XOR-based four-share schemes in which the secret becomes legible exactly when three shares are combined, while one, two and four shares all give a visually uninformative result. Replacing OR by XOR is what makes this possible: the OR of a superset of a qualified set can only become darker, whereas XOR admits cancellation, so adding a share may destroy the contrast enjoyed by a smaller set.

Date: Received: Aug 25, 2026; Revised: Sep 21, 2026; Accepted: Sep 29, 2026.
* Corresponding author
© The Author(s) 2026. This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of the licence, visit https://creativecommons.org/licenses/by-nc-nd/4.0/.

XOR-based visual cryptography has been studied systematically since the work of Tuyls et al. [5], and linear-algebraic methods have been applied to it before: Shen et al. [6] construct perfect-contrast XOR schemes for general access structures, and Jia et al. [7] study contrast maximization. More broadly, analytic tools continue to yield new cryptographic constructions; for instance, Yilmazer, Yilmaz, Gulsen and Et [8] design an encryption method based on the Laplace transform of the Mittag-Leffler function. The works on XOR-based visual cryptography cited above fix an access structure and optimize the contrast it achieves. Here the contrast profile is the *input*: the designer prescribes a value m_t for every cardinality t, including the value zero at cardinalities above a revealing one, and seeks basis matrices that deliver it.

The schemes of [3, 4] were obtained by exhibiting a pair of 4×6 matrices and checking the required weights by hand. That method does not scale, and it offers no way of aiming at a prescribed behavior. The purpose of this paper is to replace it by a direct computation.

Contributions. We show (Section 2) that the design problem is the linear system $B_n \boldsymbol{c} = \boldsymbol{m}$, where $\boldsymbol{m}$ is the prescribed contrast profile and $\boldsymbol{c}$ records how many copies of each $A_{n,p}$ are placed in each basis matrix. We then determine B_n for every n (Section 3): it satisfies $B_n^2 = 2^{n-2}(I_n + \boldsymbol{e}\boldsymbol{r}^T)$, is therefore invertible, and has the closed-form inverse

$$B_n^{-1} = -2^{1-n} K, \qquad \text{so that} \qquad z_p - y_p = -2^{1-n} \sum_{t=1}^{n} K(p,t)\, m_t,$$

where K is a small integer matrix of Krawtchouk numbers. The inversion is direct: no auxiliary recursive sequence is required at any point.

Section 4 turns this into an elementary construction procedure (multiply $\boldsymbol{m}$ by a tabulated integer matrix, divide by 2^{n-1}, and split the result into positive and negative parts), and states the integrality and non-negativity conditions under which the output is a valid pair of basis matrices. Section 5 carries the procedure out explicitly for a range of non-monotonic behaviors with $4 \le n \le 8$; the known four-share scheme of [3, 4] reappears as the case $\boldsymbol{m} = (0, 0, 4, 0)$.

All schemes reported below were verified by exhaustive enumeration over every $X \subseteq \{1, \dots, n\}$, and all computations were carried out in exact integer arithmetic.

1.1. **Notation.** We use the following conventions throughout. For a binary vector $x = (x_1, \dots, x_N) \in \{0,1\}^N$ we write

$$w(x) := \#\{i : x_i = 1\}, \qquad \operatorname{supp}(x) := \{i : x_i = 1\} \subseteq \{1, \dots, N\}$$

for its *Hamming weight* and its *support*, so that $w(x) = |\operatorname{supp}(x)|$. The same symbol $w(\cdot)$ is used for the weight of a row vector obtained from a matrix.

For $u, v \in \{0,1\}^N$ we write

$$u \cdot v := \sum_{i=1}^{N} u_i v_i \in \mathbb{Z}$$

for the ordinary inner product of u and v regarded as integer vectors. It enters only through the sign $(-1)^{u \cdot v}$, which therefore depends on $u \cdot v$ only modulo 2;

equivalently, $(-1)^{u\cdot v} = +1$ when $|\operatorname{supp}(u) \cap \operatorname{supp}(v)|$ is even and -1 when it is odd. We write $\mathbf{0}$ for the all-zero vector and $u \oplus v$ for coordinatewise XOR.

A subset $Y \subseteq \{1, \dots, N\}$ is identified with its indicator vector in $\{0,1\}^N$; under this identification supp is the inverse map. Finally, $\mathbf{1}[P]$ equals 1 if the statement P holds and 0 otherwise, and $\delta_{p,q} := \mathbf{1}[p = q]$ is the Kronecker delta.

1.2. **Visual cryptography set-up.** Following Lakshmanan and Arumugam [9], let $A_{n,p}$ denote the $n \times \binom{n}{p}$ Boolean matrix whose columns are exactly the vectors of $\{0,1\}^n$ of Hamming weight p; thus every column of a given Hamming weight occurs in $A_{n,p}$ with the same frequency. For $X \subseteq \{1, \dots, n\}$ we write $t = |X|$, let $M[X]$ be the submatrix of M formed by the rows indexed by X, and let M_X denote the XOR of those rows, so that $w(M_X)$ counts the black subpixels it produces.

Basis matrices are built as horizontal concatenations of copies of the $A_{n,p}$,

$$S^0 = (y_1 A_{n,1} \mid \cdots \mid y_n A_{n,n}), \qquad S^1 = (z_1 A_{n,1} \mid \cdots \mid z_n A_{n,n}), \tag{1.1}$$

where $y_p A_{n,p}$ denotes y_p copies of $A_{n,p}$ and $y_p, z_p \in \mathbb{Z}_{\geq 0}$. The shorter matrix is padded with all-zero columns so that both have the same width ℓ, the *pixel expansion*. A zero column never contributes to an XOR weight, so padding does not affect any weight computed below. We write $c_p := z_p - y_p$ and set

$$\boldsymbol{e} = (1, \dots, 1)^T \in \mathbb{R}^n, \qquad \boldsymbol{r} = \left(\tbinom{n}{1}, \dots, \tbinom{n}{n}\right)^T,$$

$$\boldsymbol{c} = (c_1, \dots, c_n)^T, \qquad \boldsymbol{m} = (m_1, \dots, m_n)^T.$$

Each pixel is encoded by choosing S^0 (white) or S^1 (black), applying a uniformly random permutation to its columns, and giving row i of the result to share i; a fresh permutation is drawn for each pixel. The design goal is to prescribe, for every X,

$$w(S^1 X) - w(S^0 X) = m_{|X|}, \tag{1.2}$$

where m_t is the desired contrast at cardinality t. A positive m_t means that sets of size t reveal the secret; $m_t = 0$ means that they do not. As usual [10], the *relative contrast* of the scheme is $\alpha := \min\{m_t : m_t > 0\}/\ell$.

We call the set of cardinalities at which the secret is legible the *access pattern* of the scheme. It is *monotonic* if it consists of all cardinalities from some threshold k upwards, as in the classical (k, n)-threshold model, and *non-monotonic* otherwise. The four-share scheme of [3, 4] is non-monotonic: its secret is legible at cardinality three only.

2. The XOR weight formula and the design system

Proposition 2.1. *For all $1 \leq t, p \leq n$ and every X with $|X| = t$,*

$$w(A_{n,p} X) = \sum_{\substack{j=1 \\ j \text{ odd}}}^{t} \binom{t}{j} \binom{n-t}{p-j}.$$

In particular, $w(A_{n,p}X)$ depends on X only through $t = |X|$.

Proof. Fix X with $|X| = t$ and a column a of weight p. The XOR of the entries of a indexed by X equals 1 precisely when an odd number of the t positions of X carry a 1 in a. For fixed j, the number of weight-p vectors with exactly j ones inside X and $p-j$ ones outside X is $\binom{t}{j}\binom{n-t}{p-j}$. Summing over odd j counts the columns that contribute a 1. □

It is convenient to replace this odd-indexed sum by a signed one.

Definition 2.2. For $0 \le t, p \le n$ set

$$K(t,p) := \sum_{j=0}^{p} (-1)^j \binom{t}{j}\binom{n-t}{p-j}.$$

These are the Krawtchouk numbers of the binary Hamming scheme. Here and below we use the standard convention that $\binom{a}{b} = 0$ unless $0 \le b \le a$, so that terms outside the meaningful range vanish automatically.

These numbers admit a generating-function description, which is also the quickest way to compute them. Generating functions are a standard route to explicit representations of special functions and polynomials; see, for instance, the work of Qureshi and Ali [11] on relatives of the Bessel functions. For a polynomial f we write $[x^p]f$ for the coefficient of x^p in f.

Lemma 2.3. *For all* $0 \le t, p \le n$,

$$K(t,p) = [x^p]\,(1-x)^t(1+x)^{n-t}. \tag{2.1}$$

Proof. This follows from the binomial theorem and the rule for multiplying polynomials. Expanding each factor separately,

$$(1-x)^t = \sum_{j\ge 0}\binom{t}{j}(-x)^j = \sum_{j\ge 0}(-1)^j\binom{t}{j}x^j, \qquad (1+x)^{n-t} = \sum_{k\ge 0}\binom{n-t}{k}x^k.$$

In the product of two polynomials, a term x^p arises from every pair consisting of a term x^j of the first factor and a term x^k of the second with $j+k=p$; hence the coefficient of x^p in the product is the sum of the corresponding products of coefficients (the Cauchy product). Writing $k = p-j$ and letting j run over $0,\dots,p$, we obtain

$$[x^p]\,(1-x)^t(1+x)^{n-t} = \sum_{j=0}^{p}\Big((-1)^j\tbinom{t}{j}\Big)\binom{n-t}{p-j} = K(t,p),$$

which is (2.1). Values of j with $j > t$, and values with $p-j > n-t$, contribute nothing by the convention of Definition 2.2. □

Example. For $n=5$, $t=2$ and $p=3$ we have $(1-x)^2 = 1-2x+x^2$ and $(1+x)^3 = 1+3x+3x^2+x^3$. The term x^3 of the product arises from the pairs $(j,k) = (0,3),(1,2),(2,1)$, which contribute $1\cdot 1$, $(-2)\cdot 3$ and $1\cdot 3$ respectively, so $K(2,3) = 1-6+3 = -2$; expanding $(1-x)^2(1+x)^3 = 1+x-2x^2-2x^3+x^4+x^5$ confirms the coefficient -2.

Corollary 2.4. *For* $1 \le t, p \le n$ *and* $|X| = t$, *we have* $w(A_{n,p}X) = \frac{1}{2}\big[\binom{n}{p} - K(t,p)\big]$.

Proof. By Vandermonde's identity $\binom{n}{p} = \sum_j \binom{t}{j}\binom{n-t}{p-j}$, while $K(t,p)$ is the same sum with alternating signs. The odd-j part is therefore $\frac{1}{2}[\binom{n}{p} - K(t,p)]$, which is the sum in Proposition 2.1. □

Substituting Corollary 2.4 into (1.2), and using the fact that the weight depends only on $|X|$, the requirement becomes the $n \times n$ system

$$B_n \boldsymbol{c} = \boldsymbol{m}, \qquad (B_n)_{t,p} = \tfrac{1}{2}\Big[\tbinom{n}{p} - K(t,p)\Big], \qquad 1 \le t, p \le n. \tag{2.2}$$

For $n = 4$ this is a 4×4 system, which is solved explicitly in Example 5.1.

3. The structure of B_n

All the properties of B_n that we need follow from a single identity, which is most naturally stated in terms of the Fourier transform on the Boolean cube.

3.1. **Fourier transform on the cube.** For a function $g : \{0,1\}^N \to \mathbb{R}$, its *Fourier* (Walsh–Hadamard) *transform* is the function $\widehat{g} : \{0,1\}^N \to \mathbb{R}$ given by

$$\widehat{g}(v) := \sum_{x \in \{0,1\}^N} g(x)\,(-1)^{v \cdot x}, \tag{3.1}$$

where $v \cdot x$ is the inner product of Section 1.1. The vector v is called a *frequency*. We use two standard facts. The first is *character orthogonality*:

$$\sum_{v \in \{0,1\}^N} (-1)^{v \cdot y} = \begin{cases} 2^N, & y = \mathbf{0}, \\ 0, & y \neq \mathbf{0}, \end{cases} \tag{3.2}$$

which holds because, if $y_i = 1$ for some i, pairing each v with $v \oplus e_i$ makes the two corresponding terms cancel. The second is *Fourier inversion*: applying (3.2) to (3.1) gives, for every $u \in \{0,1\}^N$,

$$\sum_{v \in \{0,1\}^N} \widehat{g}(v)\,(-1)^{u \cdot v} = 2^N g(u), \tag{3.3}$$

so that g is determined by $\widehat{g}$.

Lemma 3.1. *For every $v \in \{0,1\}^n$ and every $0 \le p \le n$, writing $t = w(v)$, we have*

$$\sum_{\substack{a \in \{0,1\}^n \\ w(a) = p}} (-1)^{v \cdot a} = K(t,p); \tag{3.4}$$

in particular, the left-hand side depends on v only through its weight. Moreover, for all $0 \le p, q \le n$,

$$\sum_{k=0}^{n} K(q,k)\,K(k,p) = 2^n \delta_{p,q}. \tag{3.5}$$

Proof. Proof of the first identity. Fix v and write $V := \operatorname{supp}(v)$, so that $|V| = t$. The sum runs over the $\binom{n}{p}$ vectors of the weight-p sphere, and we evaluate it in

two steps: we first show that the summand is constant on each part of a suitable partition of that sphere, and then count the size of each part. For $a \in \{0,1\}^n$ put

$$j(a) := |\operatorname{supp}(a) \cap V|,$$

the number of ones of a lying inside V. Since $|V| = t$ and $w(a) = p$, the integer $j(a)$ ranges over $0 \le j \le \min(t, p)$.

Step 1: the summand depends on a only through $j(a)$. The product $v_i a_i$ equals 1 exactly when both $i \in V$ and $a_i = 1$, that is, exactly when $i \in \operatorname{supp}(a) \cap V$, and it equals 0 otherwise. Summing over i therefore counts this intersection:

$$v \cdot a = \sum_{i=1}^{n} v_i a_i = \sum_{i \in V} a_i = |\operatorname{supp}(a) \cap V| = j(a). \tag{3.6}$$

Thus $v \cdot a$ is not merely congruent to $j(a)$ modulo 2 but equal to it as an integer, and consequently

$$(-1)^{v \cdot a} = (-1)^{j(a)}. \tag{3.7}$$

In particular, the summand takes the single value $(-1)^j$ on the whole fiber $\Phi_j := \{a : w(a) = p,\ j(a) = j\}$, so it suffices to count the fibers.

Step 2: the size of each fiber. A vector $a \in \Phi_j$ is obtained by choosing which j of the t positions of V carry a one, and which $p-j$ of the remaining $n-t$ positions outside V carry the other ones; these choices are independent and determine a. Hence

$$|\Phi_j| = \binom{t}{j}\binom{n-t}{p-j}, \tag{3.8}$$

which, by the convention of Definition 2.2, is correct for every j and vanishes outside the admissible range.

Step 3: conclusion. The fibers $\Phi_0, \Phi_1, \dots$ partition the weight-p sphere, and by (3.7) the summand is constant, equal to $(-1)^j$, on Φ_j. Splitting the sum over the fibers and using (3.8),

$$\sum_{\substack{a \in \{0,1\}^n \\ w(a)=p}} (-1)^{v \cdot a} = \sum_{j \ge 0} \sum_{a \in \Phi_j} (-1)^{v \cdot a} = \sum_{j \ge 0} (-1)^j |\Phi_j| = \sum_{j=0}^{p} (-1)^j \binom{t}{j}\binom{n-t}{p-j},$$

which is $K(t,p)$ by definition. Since the right-hand side involves v only through $t = w(v)$, so does the left-hand side.

Example. For $n = 4$, $v = 1100$ (so $V = \{1,2\}$ and $t = 2$) and $p = 2$, the six vectors of weight 2 split into $\Phi_2 = \{1100\}$, $\Phi_1 = \{1010, 1001, 0110, 0101\}$ and $\Phi_0 = \{0011\}$, of sizes $1, 4, 1$, in agreement with $\binom{2}{j}\binom{2}{2-j}$. The sum is $1 - 4 + 1 = -2 = K(2,2)$.

Proof of the second identity. Let $g : \{0,1\}^n \to \mathbb{R}$ be the indicator of the weight-p sphere, $g(x) := \mathbf{1}[w(x) = p]$. By (3.1) and the first identity, its transform is

$$\widehat{g}(v) = \sum_{x} g(x)(-1)^{v \cdot x} = \sum_{\substack{x \\ w(x)=p}} (-1)^{v \cdot x} = K(w(v), p). \tag{3.9}$$

Fix $u \in \{0,1\}^n$ and apply Fourier inversion (3.3) to g:

$$\sum_{v\in\{0,1\}^n} \widehat{g}(v)\,(-1)^{u\cdot v} = 2^n g(u).$$

On the left, group the frequencies v according to their weight $k = w(v)$. By (3.9) the factor $\widehat{g}(v) = K(k,p)$ depends only on k, while the first identity, applied with the roles of the two vectors exchanged, gives

$$\sum_{v:\, w(v)=k} (-1)^{u\cdot v} = K\big(w(u),k\big).$$

Hence the left-hand side equals $\sum_{k=0}^{n} K(w(u),k)\,K(k,p)$, while on the right-hand side $g(u) = \mathbf{1}[w(u)=p]$. Writing $q := w(u)$ and noting that $\mathbf{1}[q=p] = \delta_{p,q}$ gives $\sum_{k=0}^{n} K(q,k)K(k,p) = 2^n\delta_{p,q}$. Since every $q \in \{0,\dots,n\}$ is the weight of some u, the identity holds for all p, q. □

Let K denote the $n \times n$ matrix with entries $K_{t,p} = K(t,p)$ for $1 \le t,p \le n$, and note that $K(t,0) = 1$ and $K(0,p) = \binom{n}{p}$.

Corollary 3.2. $K\boldsymbol{e} = -\boldsymbol{e}, \quad \boldsymbol{r}^T K = -\boldsymbol{r}^T, \quad K^2 = 2^n I_n - \boldsymbol{e}\boldsymbol{r}^T.$

Proof. We specialize (3.5). For $p = 0$ and $q \ge 1$, using $K(k,0) = 1$, we get $K(q,0) + \sum_{k\ge1} K(q,k) = 0$, that is, $\sum_{k\ge1} K(q,k) = -1$, which is $K\boldsymbol{e} = -\boldsymbol{e}$. For $q = 0$ and $p \ge 1$, using $K(0,k) = \binom{n}{k}$, we get $\sum_{k\ge1}\binom{n}{k}K(k,p) = -\binom{n}{p}$, which is $\boldsymbol{r}^T K = -\boldsymbol{r}^T$. For $p, q \ge 1$, separating the term $k = 0$ gives $\binom{n}{p} + (K^2)_{q,p} = 2^n\delta_{pq}$, that is, $K^2 = 2^n I_n - \boldsymbol{e}\boldsymbol{r}^T$. □

Corollary 3.2 already determines the product of K with B_n, which will be the key to Theorem 3.4. Since $B_n = \frac{1}{2}(\boldsymbol{e}\boldsymbol{r}^T - K)$,

$$KB_n = \tfrac{1}{2}\big(K\boldsymbol{e}\boldsymbol{r}^T - K^2\big) = \tfrac{1}{2}\big(-\boldsymbol{e}\boldsymbol{r}^T - 2^n I_n + \boldsymbol{e}\boldsymbol{r}^T\big) = -2^{n-1} I_n. \tag{3.10}$$

In particular, K is invertible, with $K^{-1} = -2^{1-n}B_n$.

Theorem 3.3. *For every $n \ge 1$,*

$$B_n^2 = 2^{n-2}\big(I_n + \boldsymbol{e}\boldsymbol{r}^T\big),$$

$$\det(B_n)^2 = 2^{n(n-1)} \neq 0, \qquad |\det B_n| = 2^{\binom{n}{2}}.$$

In particular, B_n is invertible, so (2.2) has a unique solution for every prescribed $\boldsymbol{m}$.

Proof. Since $B_n = \frac{1}{2}(\boldsymbol{e}\boldsymbol{r}^T - K)$, we have $B_n^2 = \frac{1}{4}[(\boldsymbol{e}\boldsymbol{r}^T)^2 - \boldsymbol{e}\boldsymbol{r}^T K - K\boldsymbol{e}\boldsymbol{r}^T + K^2]$. Now $(\boldsymbol{e}\boldsymbol{r}^T)^2 = (\boldsymbol{r}^T\boldsymbol{e})\boldsymbol{e}\boldsymbol{r}^T = (2^n-1)\boldsymbol{e}\boldsymbol{r}^T$, while $\boldsymbol{e}\boldsymbol{r}^T K = -\boldsymbol{e}\boldsymbol{r}^T$ and $K\boldsymbol{e}\boldsymbol{r}^T = -\boldsymbol{e}\boldsymbol{r}^T$ by Corollary 3.2, and $K^2 = 2^n I_n - \boldsymbol{e}\boldsymbol{r}^T$. Adding these, $B_n^2 = \frac{1}{4}[2^n\boldsymbol{e}\boldsymbol{r}^T + 2^n I_n] = 2^{n-2}(I_n + \boldsymbol{e}\boldsymbol{r}^T)$. The matrix determinant lemma gives $\det(I_n + \boldsymbol{e}\boldsymbol{r}^T) = 1 + \boldsymbol{r}^T\boldsymbol{e} = 2^n$, so $\det(B_n)^2 = 2^{n(n-2)}\cdot 2^n = 2^{n(n-1)}$, and taking square roots gives $|\det B_n| = 2^{n(n-1)/2} = 2^{\binom{n}{2}}$. □

Theorem 3.4. *For every $n \geq 1$ we have $B_n^{-1} = -2^{1-n}K$, so the unique solution of (2.2) is*

$$z_p - y_p = -2^{1-n} \sum_{t=1}^{n} K(p,t)\, m_t, \qquad 1 \leq p \leq n. \tag{3.11}$$

Proof. By (3.10), $KB_n = -2^{n-1}I_n$, so $-2^{1-n}K$ is a left inverse of B_n. Since B_n is invertible by Theorem 3.3, it is the inverse. □

Formula (3.11) requires no auxiliary recursion: the coefficients of the basis matrices are explicit alternating binomial sums of the prescribed contrasts.

4. Constructing schemes

Theorem 3.4 yields a direct construction method. This section states it as an explicit procedure, gives the conditions under which its output is a valid pair of basis matrices, and tabulates the matrix K so that the computation can be carried out by hand.

4.1. The construction procedure.

Given a desired contrast profile $\boldsymbol{m}$, proceed as follows.

- **(R1)** Compute $\boldsymbol{c} = -2^{1-n}K\boldsymbol{m}$, that is, $c_p = -2^{1-n}\sum_{t=1}^{n} K(p,t)m_t$ for $p = 1, \ldots, n$, using the matrix K tabulated in Section 4.5.
- **(R2)** Check that every c_p is an integer (Section 4.3).
- **(R3)** Split $\boldsymbol{c}$ into its positive and negative parts,

$$z_p := \max(c_p, 0), \qquad y_p := \max(-c_p, 0),$$

  so that $z_p, y_p \geq 0$ and $z_p - y_p = c_p$.
- **(R4)** Assemble $S^0 = (y_1 A_{n,1} \mid \cdots \mid y_n A_{n,n})$ and $S^1 = (z_1 A_{n,1} \mid \cdots \mid z_n A_{n,n})$, and pad the shorter one with all-zero columns.

By Theorem 3.4, the resulting matrices satisfy $w(S^1X) - w(S^0X) = m_{|X|}$ for every X, which is exactly the prescribed behavior. The next two subsections make steps (R2) and (R3) precise.

4.2. Non-negativity is automatic.

Step (R3) always succeeds, since any integer splits into its positive and negative parts. We record this explicitly because it isolates integrality as the only genuine obstruction to the procedure.

Proposition 4.1. *If $\boldsymbol{c} \in \mathbb{Z}^n$, then $z_p := \max(c_p, 0)$ and $y_p := \max(-c_p, 0)$ are non-negative integers with $z_p - y_p = c_p$. Hence the only obstruction to carrying out the procedure is the integrality condition of step* (R2).

Note that y_p and z_p are never both nonzero, so each $A_{n,p}$ appears in at most one of the two basis matrices; this feature is visible in every example below.

4.3. **Integrality.** Since K has integer entries, the vector $\boldsymbol{c} = -2^{1-n}K\boldsymbol{m}$ can fail to be integral only because of the divisor 2^{n-1}.

Corollary 4.2. *We have $\boldsymbol{c} \in \mathbb{Z}^n$ if and only if 2^{n-1} divides $\sum_t K(p,t)m_t$ for every p. In particular, if 2^{n-1} divides every m_t, then $\boldsymbol{c} \in \mathbb{Z}^n$.*

Proof. This is immediate from $\boldsymbol{c} = -2^{1-n}K\boldsymbol{m}$ and the integrality of K. □

The sufficient condition is coarse but convenient: *every* profile becomes admissible after multiplication by 2^{n-1}. Since multiplying $\boldsymbol{m}$ by a positive integer multiplies the pixel expansion by the same integer and leaves the relative contrast unchanged, nothing is lost in contrast quality; only pixel expansion is paid. In practice, much smaller profiles are already admissible; for $n = 4$, for instance, $\boldsymbol{m} = (0, 0, 4, 0)$ is admissible, as Example 5.1 shows.

4.4. **What a zero entry delivers.** The entries with $m_t = 0$ are those that the designer intends to be uninformative, so it is worth stating precisely what they guarantee. Because the encryption applies a fresh, uniformly random column permutation to each pixel, the answer is simple.

Proposition 4.3. *Fix X and let π be a uniformly random column permutation. Then the reconstruction $\pi(S^b)_X$ has the same distribution for $b = 0$ and $b = 1$ if and only if $w(S^0X) = w(S^1X)$, that is, if and only if $m_{|X|} = 0$.*

Proof. Permuting columns commutes with XOR-ing rows, so $\pi(S^b)_X = \pi(S^bX)$ is the vector S^bX with its coordinates permuted uniformly at random. Its distribution is therefore uniform on the set of binary vectors of length ℓ with exactly $w(S^bX)$ ones, and this set is determined by, and determines, the number $w(S^bX)$. The two distributions agree exactly when $w(S^0X) = w(S^1X)$, which by (1.2) means $m_{|X|} = 0$. □

Thus $m_t = 0$ means that the recovered image at cardinality t carries no information about the encoded pixel: black and white pixels induce the same distribution on what the viewer sees. This is a statement about the *reconstruction*, which is what the visual protocols of [3, 4] rely on. It is not a statement about the shares themselves: a coalition that holds the actual share matrices, rather than only their XOR, is not constrained by $m_t = 0$ alone, and against such an adversary the guarantee of the present construction extends only below the smallest revealing cardinality.

4.5. **The matrices K for small n.** By Lemma 2.3, $K(p,t) = [x^t](1-x)^p(1+x)^{n-p}$. Writing $K^{(n)}$ for the $n \times n$ array with (p,t) entry $K(p,t)$, step (R1) reads $\boldsymbol{c} = -2^{1-n}K^{(n)}\boldsymbol{m}$. For the sizes used below,

$$K^{(4)} = \begin{pmatrix} 2 & 0 & -2 & -1 \\ 0 & -2 & 0 & 1 \\ -2 & 0 & 2 & -1 \\ -4 & 6 & -4 & 1 \end{pmatrix}, \qquad K^{(5)} = \begin{pmatrix} 3 & 2 & -2 & -3 & -1 \\ 1 & -2 & -2 & 1 & 1 \\ -1 & -2 & 2 & 1 & -1 \\ -3 & 2 & 2 & -3 & 1 \\ -5 & 10 & -10 & 5 & -1 \end{pmatrix},$$

$$K^{(6)} = \begin{pmatrix} 4 & 5 & 0 & -5 & -4 & -1 \\ 2 & -1 & -4 & -1 & 2 & 1 \\ 0 & -3 & 0 & 3 & 0 & -1 \\ -2 & -1 & 4 & -1 & -2 & 1 \\ -4 & 5 & 0 & -5 & 4 & -1 \\ -6 & 15 & -20 & 15 & -6 & 1 \end{pmatrix},$$

with $\boldsymbol{c} = -\frac{1}{8}K^{(4)}\boldsymbol{m}$, $\boldsymbol{c} = -\frac{1}{16}K^{(5)}\boldsymbol{m}$ and $\boldsymbol{c} = -\frac{1}{32}K^{(6)}\boldsymbol{m}$, respectively.

5. Worked examples

Every scheme in this section was verified by exhaustive enumeration over all $X \subseteq \{1, \ldots, n\}$: the reported $\boldsymbol{m}$ is the actual value of $w(S^1X) - w(S^0X)$ at every cardinality, not merely the target.

Example 5.1 ($n = 4$: the published four-share scheme)**.** We ask for a secret that is legible only when three of the four shares are combined, and take $\boldsymbol{m} = (0, 0, 4, 0)$. Step (R1) with $K^{(4)}$ gives

$$K^{(4)}\boldsymbol{m} = \begin{pmatrix} 2 & 0 & -2 & -1 \\ 0 & -2 & 0 & 1 \\ -2 & 0 & 2 & -1 \\ -4 & 6 & -4 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} -8 \\ 0 \\ 8 \\ -16 \end{pmatrix},$$

$$\boldsymbol{c} = -\tfrac{1}{8} \begin{pmatrix} -8 \\ 0 \\ 8 \\ -16 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 2 \end{pmatrix}.$$

The entries are integers, so (R2) holds. Step (R3) gives $z = (1, 0, 0, 2)$ and $y = (0, 0, 1, 0)$: S^1 consists of one copy of $A_{4,1}$ and two copies of $A_{4,4}$, while S^0 consists of one copy of $A_{4,3}$. Padding S^0 to width 6, we obtain

$$S^0 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad S^1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

with pixel expansion $\ell = 6$ and relative contrast $\alpha = 4/6 = 2/3$. These are exactly the basis matrices of [3, 4], obtained here by a few lines of arithmetic rather than by search.

Example 5.2 ($n = 5$, legible for exactly three shares)**.** Now take five shares and require the secret to be legible exactly when three of them are combined: $\boldsymbol{m} = (0, 0, 8, 0, 0)$. Step (R1) with $K^{(5)}$ gives

$$K^{(5)}\boldsymbol{m} = \begin{pmatrix} 3 & 2 & -2 & -3 & -1 \\ 1 & -2 & -2 & 1 & 1 \\ -1 & -2 & 2 & 1 & -1 \\ -3 & 2 & 2 & -3 & 1 \\ -5 & 10 & -10 & 5 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 8 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -16 \\ -16 \\ 16 \\ 16 \\ -80 \end{pmatrix},$$

$$\boldsymbol{c} = -\tfrac{1}{16}\begin{pmatrix} -16 \\ -16 \\ 16 \\ 16 \\ -80 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \\ 5 \end{pmatrix}.$$

The entries are integers, so (R2) holds, and (R3) gives

$$z = (1,1,0,0,5), \qquad y = (0,0,1,1,0).$$

Thus S^1 consists of one copy of $A_{5,1}$, one of $A_{5,2}$ and five copies of the all-ones column $A_{5,5}$, of total width $\binom{5}{1} + \binom{5}{2} + 5 = 20$, while S^0 consists of one copy of $A_{5,3}$ and one of $A_{5,4}$, of width $\binom{5}{3} + \binom{5}{4} = 15$. Padding S^0 with five zero columns, we obtain

$$S^0 = \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&0&1&1&1&0&1&1&1&0&1&0&0&0&0&0 \\ 1&0&0&1&1&0&1&1&0&1&1&1&0&1&1&0&0&0&0&0 \\ 0&1&0&1&0&1&1&0&1&1&1&0&1&1&1&0&0&0&0&0 \\ 0&0&1&0&1&1&0&1&1&1&0&1&1&1&1&0&0&0&0&0 \end{pmatrix},$$

$$S^1 = \begin{pmatrix} 1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1 \\ 0&1&0&0&0&1&0&0&0&1&1&1&0&0&0&1&1&1&1&1 \\ 0&0&1&0&0&0&1&0&0&1&0&0&1&1&0&1&1&1&1&1 \\ 0&0&0&1&0&0&0&1&0&0&1&0&1&0&1&1&1&1&1&1 \\ 0&0&0&0&1&0&0&0&1&0&0&1&0&1&1&1&1&1&1&1 \end{pmatrix},$$

with $\ell = 20$ and $\alpha = 8/20 = 2/5$. In S^0 the first ten columns form $A_{5,3}$ and the next five form $A_{5,4}$; in S^1 the first five columns form $A_{5,1}$, the next ten form $A_{5,2}$, and the last five are the repeated all-ones column. Exactly three of the five shares reveal the secret; one, two, four and five shares do not.

Example 5.3 ($n = 6$, legible for exactly three shares)**.** Take $\boldsymbol{m} = (0,0,8,0,0,0)$. Step (R1) with $K^{(6)}$ gives $K^{(6)}\boldsymbol{m} = (0,-32,0,32,0,-160)^T$, and hence

$$\boldsymbol{c} = -\tfrac{1}{32}(0,-32,0,32,0,-160)^T = (0,1,0,-1,0,5)^T.$$

Therefore $z = (0,1,0,0,0,5)$ and $y = (0,0,0,1,0,0)$: S^1 consists of one copy of $A_{6,2}$ followed by five copies of the all-ones column $A_{6,6}$, of total width $\binom{6}{2}+5 = 20$, while S^0 is one copy of $A_{6,4}$, of width $\binom{6}{4} = 15$. Padding S^0 with five zero columns, we obtain

$$S^0 = \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&0&1&1&1&0&1&1&1&0&1&0&0&0&0&0 \\ 1&0&0&1&1&0&1&1&0&1&1&1&0&1&1&0&0&0&0&0 \\ 0&1&0&1&0&1&1&0&1&1&1&0&1&1&1&0&0&0&0&0 \\ 0&0&1&0&1&1&0&1&1&1&0&1&1&1&1&0&0&0&0&0 \end{pmatrix},$$

$$S^1 = \begin{pmatrix} 1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1 \\ 1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&1&1&1&1&1 \\ 0&1&0&0&0&1&0&0&0&1&1&1&0&0&0&1&1&1&1&1 \\ 0&0&1&0&0&0&1&0&0&1&0&0&1&1&0&1&1&1&1&1 \\ 0&0&0&1&0&0&0&1&0&0&1&0&1&0&1&1&1&1&1&1 \\ 0&0&0&0&1&0&0&0&1&0&0&1&0&1&1&1&1&1&1&1 \end{pmatrix},$$

with $\ell = 20$ and $\alpha = 8/20 = 2/5$. The first fifteen columns of S^0 form $A_{6,4}$ and the last five are padding; the first fifteen columns of S^1 form $A_{6,2}$ and the last five are the repeated all-ones column. Exactly three of the six shares reveal the secret, while one, two, four, five and six shares do not.

Example 5.4 (two revealing cardinalities)**.** Nothing restricts the prescribed profile to a single revealing cardinality. For $n = 6$, take $\boldsymbol{m} = (0, 0, 4, 0, 8, 0)$, which requires legibility for three *and* for five shares, but for no other number. Step (R1) gives $K^{(6)}\boldsymbol{m} = (-32, 0, 0, 0, 32, -128)^T$, hence $\boldsymbol{c} = (1, 0, 0, 0, -1, 4)$, so that $z = (1, 0, 0, 0, 0, 4)$ and $y = (0, 0, 0, 0, 1, 0)$. Thus S^1 consists of $A_{6,1}$ followed by four copies of the all-ones column, of width $\binom{6}{1} + 4 = 10$, and S^0 is $A_{6,5}$, of width $\binom{6}{5} = 6$, padded to 10:

$$S^0 = \begin{pmatrix} 1&1&1&1&1&0&0&0&0&0 \\ 1&1&1&1&0&1&0&0&0&0 \\ 1&1&1&0&1&1&0&0&0&0 \\ 1&1&0&1&1&1&0&0&0&0 \\ 1&0&1&1&1&1&0&0&0&0 \\ 0&1&1&1&1&1&0&0&0&0 \end{pmatrix}, \qquad S^1 = \begin{pmatrix} 1&0&0&0&0&0&1&1&1&1 \\ 0&1&0&0&0&0&1&1&1&1 \\ 0&0&1&0&0&0&1&1&1&1 \\ 0&0&0&1&0&0&1&1&1&1 \\ 0&0&0&0&1&0&1&1&1&1 \\ 0&0&0&0&0&1&1&1&1&1 \end{pmatrix}.$$

Here $\ell = 10$ and $\alpha = 4/10 = 2/5$. Three or five shares reveal the secret, while one, two, four and six shares do not; such a behavior has no counterpart in the threshold model.

6. Conclusion

The problem of designing an XOR-based visual cryptography scheme with a prescribed contrast profile, over the family of matrices in which every column of a given weight occurs equally often, is a linear system, and this system can be solved once and for all. The matrix B_n satisfies $B_n^2 = 2^{n-2}(I_n + \boldsymbol{e}\boldsymbol{r}^T)$, is invertible for every n, and has the closed-form inverse $-2^{1-n}K$. Instead of searching, as was done for the four-share scheme of [3, 4], a designer writes down the desired profile, multiplies it by a tabulated integer matrix, and reads off the basis matrices. The known scheme is recovered as the instance $\boldsymbol{m} = (0, 0, 4, 0)$, and Table 1 shows the same computation producing non-monotonic behaviors up to $n = 8$, including profiles with two separate revealing cardinalities.

Two practical points bound the method. First, integrality: by Corollary 4.2, a profile is admissible once 2^{n-1} divides its entries, and rescaling to achieve this costs pixel expansion but no relative contrast. Second, the pixel expansion grows with n in Table 1, and we make no claim that the values shown are minimal;

TABLE 1. Non-monotonic schemes produced by the procedure of Section 4. Each $\boldsymbol{c}$ is obtained from $\boldsymbol{m}$ by a single matrix–vector product; ℓ is the pixel expansion and α the relative contrast. Upper block: a single revealing cardinality. Lower block: two revealing cardinalities. Every row was verified by exhaustive enumeration over all subsets of shares.

n	legible for $\lvert X\rvert =$	$\boldsymbol{c} = (z_p - y_p)_p$	$\boldsymbol{m}$	$(\ell,\ \alpha)$
4	3	$(1, 0, -1, 2)$	$(0, 0, 4, 0)$	$(6,\ 2/3)$
5	3	$(1, 1, -1, -1, 5)$	$(0, 0, 8, 0, 0)$	$(20,\ 2/5)$
5	4	$(3, -1, -1, 3, -5)$	$(0, 0, 0, 16, 0)$	$(30,\ 8/15)$
6	3	$(0, 1, 0, -1, 0, 5)$	$(0, 0, 8, 0, 0, 0)$	$(20,\ 2/5)$
6	4	$(5, 1, -3, 1, 5, -15)$	$(0, 0, 0, 32, 0, 0)$	$(90,\ 16/45)$
6	5	$(2, -1, 0, 1, -2, 3)$	$(0, 0, 0, 0, 16, 0)$	$(30,\ 8/15)$
7	4	$(5, 5, -3, -3, 5, 5, -35)$	$(0, 0, 0, 64, 0, 0, 0)$	$(280,\ 8/35)$
7	5	$(9, -1, -3, 3, 1, -9, 21)$	$(0, 0, 0, 0, 64, 0, 0)$	$(210,\ 32/105)$
8	5	$(7, 2, -3, 0, 3, -2, -7, 28)$	$(0, 0, 0, 0, 64, 0, 0, 0)$	$(308,\ 16/77)$
5	2, 4	$(0, 1, 1, 0, -10)$	$(0, 12, 0, 8, 0)$	$(20,\ 2/5)$
6	2, 4	$(0, 1, 0, 1, 0, -15)$	$(0, 16, 0, 16, 0, 0)$	$(30,\ 8/15)$
6	3, 5	$(1, 0, 0, 0, -1, 4)$	$(0, 0, 4, 0, 8, 0)$	$(10,\ 2/5)$
7	3, 6	$(5, -1, 5, -1, -11, 15, 21)$	$(0, 0, 64, 0, 0, 128, 0)$	$(336,\ 4/21)$

determining the least expansion attainable for a prescribed profile, and comparing it with the known bounds for XOR-based threshold schemes, is left open.

Finally, Proposition 4.3 records what a zero entry of $\boldsymbol{m}$ guarantees: the reconstruction at that cardinality is distributed identically for black and white pixels, and is therefore uninformative to a viewer who sees only the combined image. Protocols built on non-monotonic schemes should be designed with this scope in mind.

Acknowledgement. The authors thank the editor and the anonymous referees for their careful reading and helpful suggestions, which improved the presentation of the paper.

REFERENCES

1. Naor, M., & Shamir, A. (1995). Visual cryptography. In A. De Santis (Ed.), *Advances in cryptology — EUROCRYPT '94* (Lecture Notes in Computer Science, Vol. 950, pp. 1–12). Springer. https://doi.org/10.1007/BFb0053419
2. Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual cryptography for general access structures. *Information and Computation*, *129*(2), 86–106. https://doi.org/10.1006/inco.1996.0076
3. Chihi, H., Chahboun, A., & Mezroui, S. (2025a). Alternative of traditional password systems using enhanced visual cryptography. *Discover Computing*, *28*(1), Article 287. https://doi.org/10.1007/s10791-025-09802-z

4. Chihi, H., Chahboun, A., & Mezroui, S. (2025b). An enhanced visual cryptography framework for smart lock authentication. *Discover Internet of Things*, *5*(1), Article 136. https://doi.org/10.1007/s43926-025-00248-9
5. Tuyls, P., Hollmann, H. D. L., van Lint, J. H., & Tolhuizen, L. (2005). XOR-based visual cryptography schemes. *Designs, Codes and Cryptography*, *37*, 169–186. https://doi.org/10.1007/s10623-004-3816-4
6. Shen, G., Liu, F., Fu, Z., & Yu, B. (2017). Perfect contrast XOR-based visual cryptography schemes via linear algebra. *Designs, Codes and Cryptography*, *85*(1), 15–37. https://doi.org/10.1007/s10623-016-0285-5
7. Jia, X., Yu, T., Luo, X., Wang, D., & Zhou, H. (2024). Maximizing contrast in XOR-based visual cryptography schemes. *IEEE Transactions on Circuits and Systems for Video Technology*, *34*(12), 12849–12861. https://doi.org/10.1109/TCSVT.2024.3435724
8. Yilmazer, M. C., Yilmaz, E., Gulsen, T., & Et, M. (2023). Laplace transform for Mittag-Leffler function in cryptography. *Gulf Journal of Mathematics*, *15*(2), 81–95. https://doi.org/10.56947/gjom.v15i2.1600
9. Lakshmanan, R., & Arumugam, S. (2017). Construction of a (k, n)-visual cryptography scheme. *Designs, Codes and Cryptography*, *82*(3), 629–645. https://doi.org/10.1007/s10623-016-0181-z
10. Blundo, C., De Santis, A., & Stinson, D. R. (1999). On the contrast in visual cryptography schemes. *Journal of Cryptology*, *12*(4), 261–289. https://doi.org/10.1007/s001459900057
11. Qureshi, M. I., & Ali, M. (2022). Explicit representations of some generalized and mixed relatives of the Bessel functions. *Gulf Journal of Mathematics*, *13*(1), 1–14. https://doi.org/10.56947/gjom.v13i1.923

[1] Abdelmalek Essaadi University, National School of Applied Sciences of Tangier (ENSAT), Mathematics and Intelligent Systems Team (MASI), Route Ziaten, BP 1818, Tanger Principale, Morocco.

Email address: chihi.hasnaa@gmail.com

[2] Abdelmalek Essaadi University, Higher School of Technology of Tetouan (ESTTe), Engineering Laboratory for Intelligent Technologies and Transformation (ELITT-Lab), Tetouan, Morocco.

Email address: smezroui@uae.ac.ma