Threshold Visual Cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels

Philip A. Eisen * Douglas R. Stinson †

October 29, 1999

Abstract

In 1994, Naor and Shamir introduced an unconditionally secure method for encoding black and white images. This method, known as a threshold visual cryptography scheme (VCS), has the benefit of requiring no cryptographic computation on the part of the decoders. In a (k, n)-VCS, a share, in the form of a transparency, is given to n users. Any k users can recover the secret simply by stacking transparencies, but $k-1$ users can gain no information about the secret whatsoever.

In this paper, we first explore the issue of contrast, by demonstrating that the current definitions are inadequate, and by providing an alternative definition. This new definition motivates an examination of minimizing pixel expansion subject to fixing the VCS parameters h and l. New bounds on pixel expansion are introduced, and connections between these bounds are examined. The best bound presented is tighter than any previous bound. An analysis of connections between $(2, n)$ schemes and designs such as BIBD's, PBD's, and (r, λ)-designs is performed. Also, an integer linear program is provided whose solution exactly determines the minimum pixel expansion of a $(2, n)$-VCS with specified h and l.

1 Introduction

Visual cryptography was first introduced by Naor and Shamir. In [11], the authors proposed a method for encoding black and white images in an unconditionally secure way. This method has the additional feature that it requires no cryptographic computation on the part of the decoders. In a visual cryptography scheme (VCS), the decoding is done entirely by the human eye. Such schemes have the benefit that they can be used by people without any background knowledge in mathematics, and can also be used where access to computers is not possible.

As described in [11], in a (k, n)-threshold VCS, the secret is an image, consisting of a collection of black and white pixels. Each share is also a collection of pixels, or more specifically, subpixels. In order to decode the message, each participant (where n is the total number of participants) photocopies their share onto a transparency, thus transforming white subpixels to clear. If k participants stack their transparencies together, the image will be revealed, but if fewer than k participants stack shares, the resulting image will be indistinguishable from random noise. More generally, any set of $k-1$ participants can analyze their collection of shares by any means, but they will obtain no information about the secret.

Later papers discussed visual cryptography for general access structures (see [2],[7]), as well as methods for encoding colour images (see [12],[4]). Naor and Shamir also briefly discussed a VCS where each share is itself a meaningful, but innocent-looking image. When k such shares are combined, the true secret is

*Department of Combinatorics and Optimization, University of Waterloo, Waterloo Ontario, N2L 3G1, Canada. E-mail: nthornhill@sympatico.ca.

†Department of Combinatorics and Optimization, University of Waterloo Waterloo Ontario, N2L 3G1, Canada. E-mail: dstinson@cacr.math.uwaterloo.ca. Research supported by NSERC grants IRC #216431-96 and RGPIN # 203114-98.

revealed without any trace of the original images. Such schemes, which later were named extended visual cryptography schemes (EVCS), were further elaborated on in [1].

The paper is organized into the following sections. In Section 2, we introduce the model for visual cryptography schemes, including the use of basis matrices and the notion of canonical schemes. In Section 3, we explain the current measurements for contrast, and demonstrate why they are inadequate. We then introduce a new measurement. Section 4 provides some preliminary results regarding schemes with specified values of h and l, which are the whiteness levels of reconstructed white and black pixels, respectively. Specifically, we show that for any meaningful values of k, n, h and l, a scheme with these parameter values exists. In Section 5, we construct $(2,n)$ schemes for a certain set of values of h and l. This construction is optimal with respect to pixel expansion.

Section 6 introduces the main result of this paper, a new bound on m, the pixel expansion of $(2,n)$ schemes with specified values of h and l. This bound, which in general is an implicit bound on m, is tighter than any previously described bound. In Section 7, we consider the effect of forcing the rows of the basis matrix for encoding white pixels to have weight $m-h$. This allows us to reduce our three part bound of Section 6 to a single bound on m. Section 8 enforces a restriction on the basis matrix for the encoding of black pixels, and establishes a connection between such schemes and (r,λ)-designs.

In Section 9, we take a different approach, and find an integer linear program whose solution allows us to exactly compute the minimum pixel expansion of a $(2,n)$ schemes with specified h and l values. This program allows us to find two additional classes of pixel expansion optimal $(2,n)$ schemes. Section 10 uses the linear program to determine how well the bounds of Section 6 and Section 7 predict the actual minimum pixel expansion. Also, the bounds are compared, and the bound of Section 7 is found to be tighter in general. Section 11 provides conclusions and open problems.

Appendix A provides a table of solutions to the integer linear program of Section 9, for various values of n. Finally, Appendix B provides a detailed proof of some important properties of the function used in the proof of our main bound.

2 The Model

We consider each pixel to be a collection of m subpixels. In practice, this can be accomplished by expanding the original image by a factor of m prior to encoding. We therefore define multisets $\mathcal{C}_0, \mathcal{C}_1 \subset \{0,1\}^{n\times m}$, $\mathcal{C}_0 \cap \mathcal{C}_1 = \emptyset$. To encode a white pixel we choose a random $C \in \mathcal{C}_0$, and on share i we place m subpixels with colours listed in row i of C. To encode a black pixel we choose a random $C \in \mathcal{C}_1$, and perform the same operation.

The viability of the scheme lies in the way the multisets $\mathcal{C}_0$ and $\mathcal{C}_1$ are chosen. Suppose we consider s participants $X = \{i_1, \ldots, i_s\}$, where $s < k$, and imagine once again that our secret image consists of a single pixel. The s participants can "combine" their shares to obtain an $s \times m$ matrix D representing s rows of the encoding matrix chosen. The security requirement therefore mandates that if we define new multisets $\mathcal{D}_0, \mathcal{D}_1$ given by the restriction of $\mathcal{C}_0, \mathcal{C}_1$ respectively to rows $i_1, \ldots, i_s$, the matrix D should appear with equal frequency in both $\mathcal{D}_0$ and $\mathcal{D}_1$. If this is the case, then to the participants in X, the image could be black or white with equal likelihood.

Any set of k participants, however, should be able to determine the secret image. This can be accomplished if a reconstructed white pixel appears "whiter" than a reconstructed black pixel. In other words, the "or" of k rows of any $C \in \mathcal{C}_0$ should have more zeroes than the "or" of k rows of any $C \in \mathcal{C}_1$.

We formalize these requirements in the following definition of a VCS, which is equivalent to that given in [11], and is paraphrased from Verheul & Van Tilborg [12].

Definition 2.1. *A (k,n) visual cryptography scheme S consists of two collections of $n \times m$ $\{0,1\}$ matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. The scheme is considered valid if for some nonnegative integers h and l, $h > l$, the following conditions are met:*

1. *For any $C \in \mathcal{C}_0$, the "or" $\overrightarrow{v}$ of any k of the n rows of C satisfies $w(\overrightarrow{v}) \leq m - h$, where $w(\overrightarrow{v})$ is the Hamming weight of $\overrightarrow{v}$.*

2. *For any $C \in \mathcal{C}_1$, the "or" $\overrightarrow{v}$ of any k of the n rows of C satisfies $w(\overrightarrow{v}) \geq m - l$.*

3. *For any $i_1 < i_2 < \ldots < i_s$ in $\{1, 2, \ldots, n\}$ with $s < k$, the two collections of $s \times m$ matrices $\mathcal{D}_j$ for $j \in \{0, 1\}$ obtained by restricting each matrix in $\mathcal{C}_j$ (where $j = 0, 1$) to rows $i_1, i_2, \ldots, i_s$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

Properties 1 and 2 are collectively called the *contrast conditions*, and property 3 is called the *security condition.*

A few observations are in order:

1. The reconstruction of an image is not perfect. White pixels will not be all white upon reconstruction, and in general, black pixels will not be all black upon reconstruction. All that is guaranteed is that reconstructed white will appear lighter than reconstructed black.

2. Certainly, any subset X of participants with $|X| > k$ can reconstruct the image by stacking any k of their shares. However, the definition of a VCS does not guarantee that if more than k shares are stacked, the image will be obtained. We call a scheme with the property that the image can be recovered if *k or more* shares are stacked a *strong* VCS [4].

2.1 Basis Matrices

Constructing the families $\mathcal{C}_0$ and $\mathcal{C}_1$ may seem a daunting task. However, it can be made considerably simpler with the use of basis matrices. $\mathcal{C}_0$ and $\mathcal{C}_1$ can be constructed by taking every column permutation of the basis matrices S_0 and S_1, respectively. S_0 and S_1 must satisfy properties very similar to those in Definition 2.1; these are detailed below.

Definition 2.2. *A (k, n) visual cryptography scheme S based on basis matrices consists of two $n \times m$ $\{0, 1\}$ matrices S_0 and S_1. The scheme is considered valid if for some nonnegative integers h and l, $h > l$, the following conditions are met:*

1. *The "or" $\overrightarrow{v}$ of any k of the n rows in S_0 satisfies $w(\overrightarrow{v}) \leq m - h$, where $w(\overrightarrow{v})$ is the Hamming weight of $\overrightarrow{v}$.*

2. *The "or" $\overrightarrow{v}$ of any k of the n rows in S_1 satisfies $w(\overrightarrow{v}) \geq m - l$.*

3. *For any $i_1 < i_2 < \ldots < i_s$ in $\{1, 2, \ldots, n\}$ with $s < k$, the matrices obtained by restricting S_0 and S_1 to rows $i_1, i_2, \ldots, i_s$ are equal up to column permutation.*

2.2 VCS Parameters

A VCS is characterized by many different parameters. Finding the balance between these parameters is the main challenge in creating a working scheme.

1. n: The number of participants. Usually this is a fixed, predetermined value.

2. k: The threshold. This is determined by security needs.

3. h: The "whiteness" of a white pixel. For fixed l, the larger the value of h is, the clearer the reconstructed image is.

4. l: The "whiteness" of a black pixel. For fixed h, the smaller the value of l is, the clearer the reconstructed image is.

5. r: The size of sets $\mathcal{C}_0$ and $\mathcal{C}_1$, which WLOG are equinumerous [2]. In general, a large value of r would translate into a large requirement of storage space. However, the use of basis matrices reduces the storage requirements to just two matrices, making this parameter of low importance.

6. m: The pixel expansion. This represents the factor by which each share is larger than the original image, and so it is desirable to make m as small as possible.

7. α: The contrast. A measurement of how clear a reconstructed image is, or how distinguishable black is from white. The meaning and measurement of contrast is highly disputed. We will discuss this further in the next section.

2.3 Canonical Schemes

Throughout the literature, certain visual cryptography schemes are described which have the property that all columns of a given weight appear with equal frequency in the basis matrices (see [11], [9], [2], [12], [7], [10], [5], [4], [6], [3]). Such schemes are referred to as *canonical*. The formal definition is as follows. (Note that in [5], canonical schemes are defined differently.)

Definition 2.3. *[4] Let (S_0, S_1) be the basis matrices of a (k,n)-VCS. They are in canonical form if, for $i = 0, 1$ and for any columns c and c' with equal weight, it is the case that $f_{c,i} = f_{c',i}$, where $f_{c,i}$ represents the frequency with which column c occurs in S_i. A (k,n)-VCS whose basis matrices are in canonical form is referred to as a canonical (k,n)-VCS.*

In order to specify the basis matrices of a canonical (k,n)-VCS, we need simply specify the frequency with which the columns of weight i appear in each basis matrix, for $i = 0, \dots, n$. The multiplicity of weight i columns in basis matrix S_j is denoted by $\mu_{i,j}$.

Example 2.1. *A canonical* $(4,4)$-*VCS*
As per [11], we can define a pixel-expansion optimal $(4,4)$-VCS as follows:

$$\mu_{0,0} = 1, \qquad \mu_{2,0} = 1, \qquad \mu_{4,0} = 1,$$
$$\mu_{1,1} = 1, \qquad \mu_{3,0} = 1.$$

The basis matrices are thus:

$$S_0 = \begin{bmatrix} 01110001 \\ 01001101 \\ 00101011 \\ 00010111 \end{bmatrix},$$
$$S_1 = \begin{bmatrix} 10001110 \\ 01001101 \\ 00101011 \\ 00010111 \end{bmatrix}.$$

3 Contrast

Of all the parameters which characterize a VCS, none causes as much difficulty as contrast. Indeed, not only is there no consensus on the definition of contrast, there is not even agreement about the name. What certain papers refer to as contrast ([9], [10], [5]), other papers refer to as loss of contrast ([11], [12], [4]); in this second set of papers contrast is given another meaning. Here, the word contrast will be used in the former sense.

The contrast of a scheme is a measurement of readability. Since reconstructed black and reconstructed white both appear as collections of black and white subpixels, the reconstructed image is less clear to the human eye than is the original image. Contrast gives a measurement of how clear the reconstructed image is in relation to the original. Thus, a perfect reconstruction (which, of course, is impossible) would have a contrast of 1, and contrast is always positive.

In working towards a definition of contrast, we consider the effect of keeping all VCS parameters but one fixed, and see how contrast changes with the lone varying parameter. It is important to note that contrast is relevant only in the reconstructed image, so the values of k, n and r are not important.

Intuitively, we can see that as we increase m, the contrast drops. Likewise, it is clear that contrast increases with an increase in h, and decreases with an increase in l. Armed with this knowledge, we are ready to examine the competing definitions of contrast.

3.1 Defining Contrast

3.1.1 The Naor and Shamir Definition

Naor and Shamir defined contrast to be

$$\alpha_{NS} = \frac{h-l}{m}.$$

Naor and Shamir's definition has clear intuitive appeal, as it varies with h, l and m exactly as described above. Also, a scheme with $l = 0$, $h = m$, i.e., perfect reconstruction, would have contrast 1. Unfortunately, experimentation shows that the intuitive notions are insufficient. α_{NS} depends only on the difference between h and l. In reality, the actual values of h and l are important as well. A demonstration of this is given in Figure 2. (The original image is shown in Figure 1.) The top scheme has parameters $h = 2$, $l = 0$, $m = 9$, thus giving $\alpha_{NS} = 2/9$. The bottom scheme has parameters $h = 6$, $l = 4$, $m = 9$, so $\alpha_{NS} = 2/9$ again. However, the top image is clearly more identifiable. Naor and Shamir's definition appears to be inadequate for this reason.

3.1.2 The Verheul and Van Tilborg Definition

In [12], Verheul and Van Tilborg reached the above conclusion about α_{NS}, and so they sought to provide a definition which more closely modelled reality. They suggested the following definition:

$$\alpha_{VV} = \frac{h-l}{m(h+l)}.$$

In this new definition, the actual values of h and l are important, as is the difference between them. Again, however, this definition fails to match reality in the case where $l = 0$, i.e., when black pixels are perfectly reconstructed. In this situation, we see that α_{VV} reduces to $1/m$. This is troublesome for two reasons.

1. h has disappeared from the definition. This means that all schemes with fixed m and $l = 0$, have the same value of α_{VV}. In other words, if reconstructed black is perfectly black, then this definition implies that it does not matter how white reconstructed white is! As Figure 3 shows, this is simply not true in practice. In the figure, the top scheme's parameters are $h = 1$, $l = 0$, $m = 9$, giving $\alpha_{VV} = 1/9$. For the bottom scheme, the parameters are $h = 5$, $l = 0$, $m = 9$, so again, $\alpha_{VV} = 1/9$. Here, the bottom image is obviously clearer.

2. The only way to achieve $\alpha_{VV} = 1$ is when $m = 1$. This implies that for $m > 1$, even if white were perfectly reconstructed as white, and black were perfectly reconstructed as black, the reconstructed image (according to α_{VV}) would be less clear than the original.

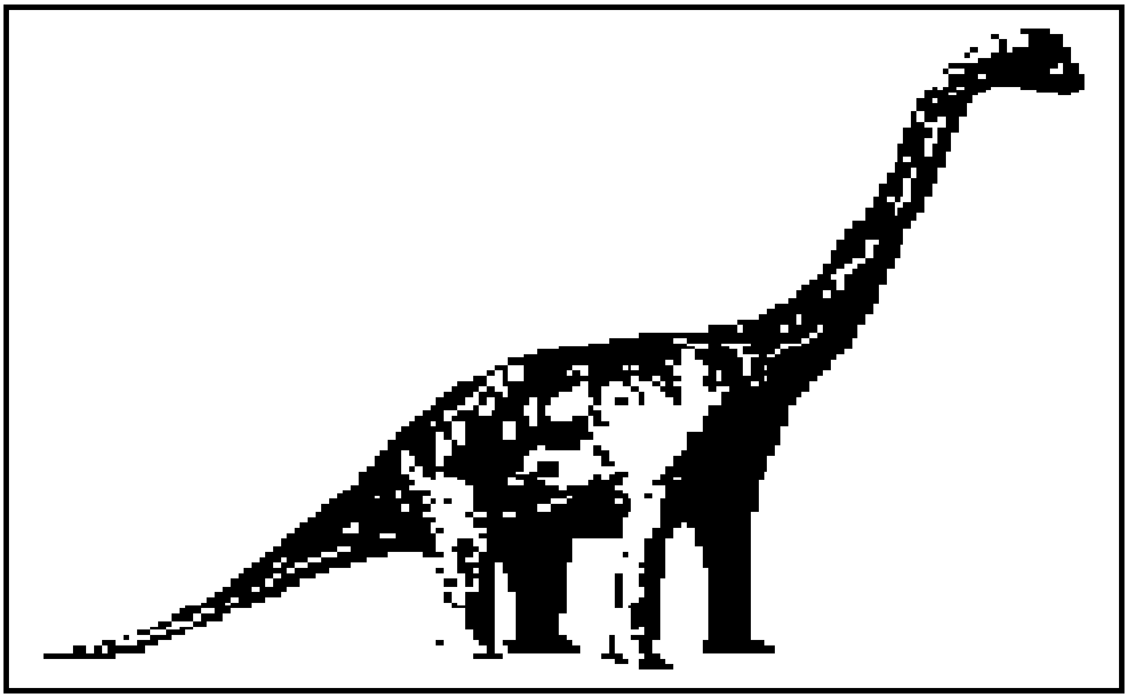

Figure 1: The original image.

3.1.3 A New Definition

We propose the following new definition for contrast:

$$\alpha_T = \frac{h-l}{m+l}.$$

This new definition combines the positive features of the previous two.

1. It varies in the desired way with m, h and l.
2. Given a constant value of $h-l$, contrast decreases as l increases, coinciding with experimental results.
3. When $l=0$, α_T reduces to h/m, meaning that the contrast is still dependent on h. Furthermore, when $h=m$, we have a perfect reconstruction with a contrast of 1, as desired.

An example of schemes with equal values of α_T is shown in Figure 4. The top scheme has $h=3$, $l=0$, $m=9$, while the bottom scheme has $h=7$, $l=3$, $m=9$. Thus, both schemes have $\alpha_T = 1/3$.

3.2 Optimizing α_T

In the historical definitions of contrast, the interplay between h, l, and m is not very evident. Indeed, we could write

$$\alpha_{NS} = \frac{1}{m} \times (h-l), \qquad \alpha_{VV} = \frac{1}{m} \times \frac{h-l}{h+l},$$

making the three parameters appear completely independent. But this is most definitely not the case. The most obvious demonstration of this fact is that by the very definition of h, it must be that $m \geq h+1$. α_T

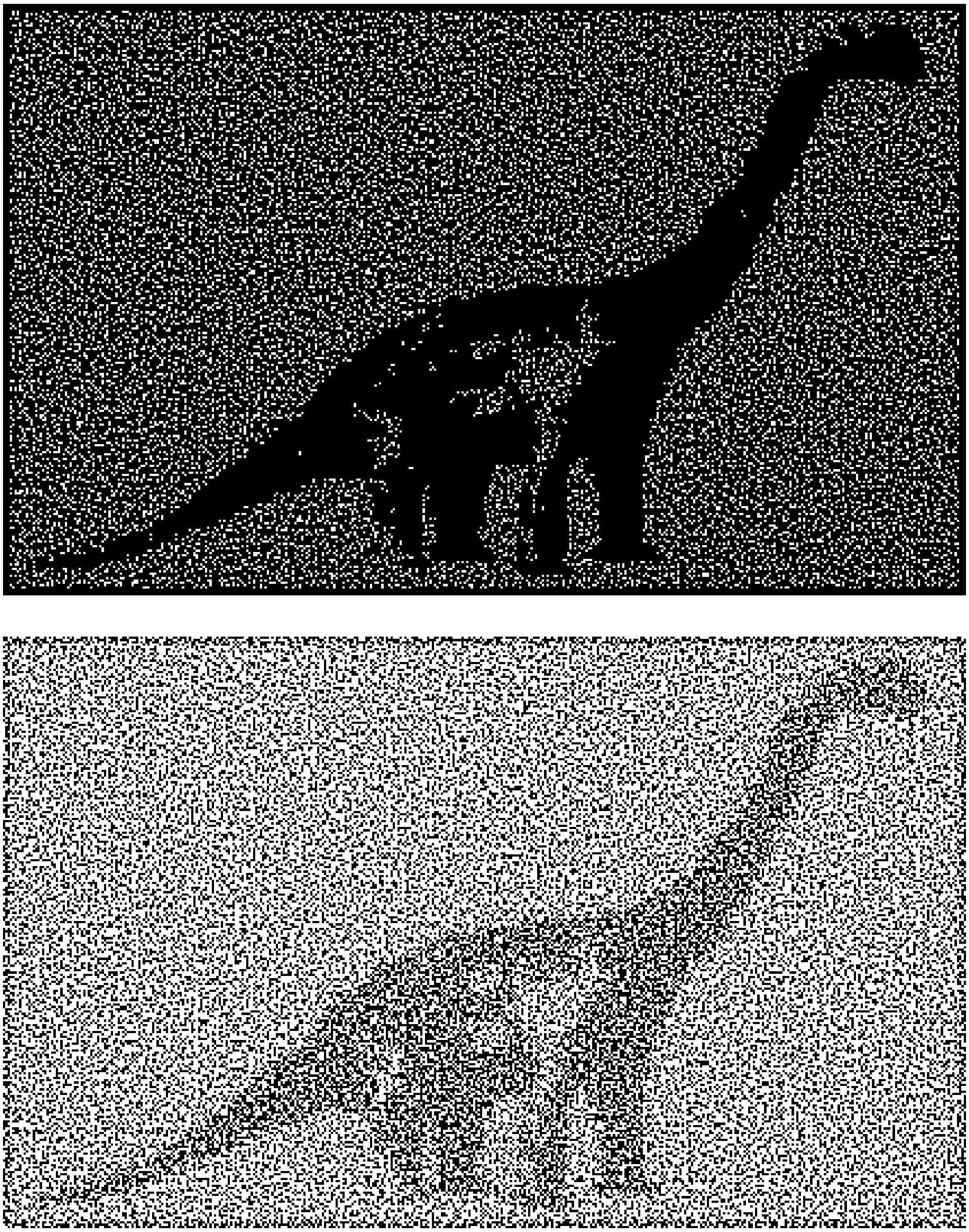

Figure 2: Two schemes with equal values of α_{NS}.

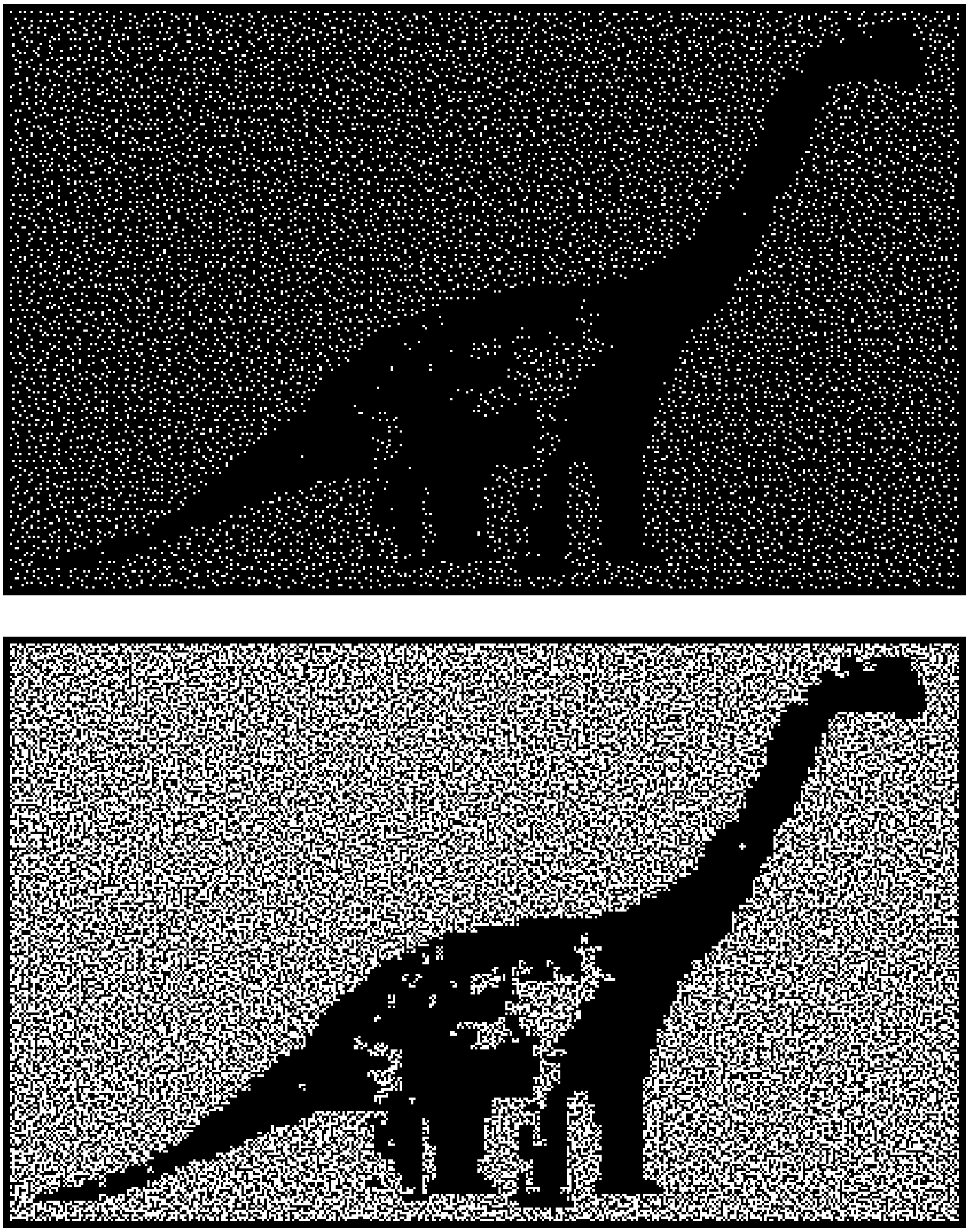

Figure 3: Two schemes with equal values of α_{VV}.

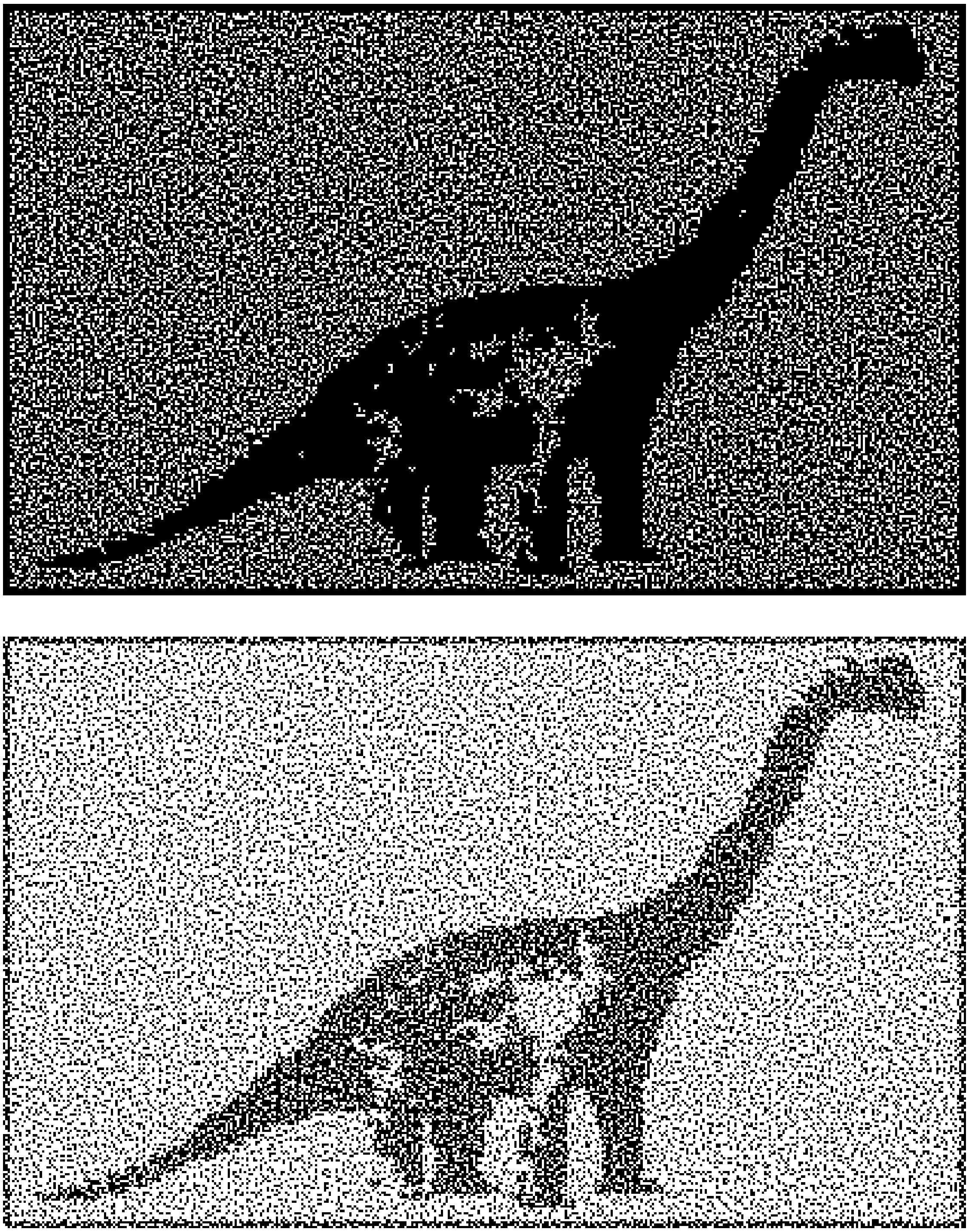

Figure 4: Two schemes with equal values of α_T.

brings the interplay between h, l and m to the forefront. Thus, an approach for optimizing α_T would be to analyze this connection.

Clearly, though, m does not vary as a function of h and l alone. k and n are equally important parameters, as the historical bounds show. In particular, what is interesting is the minimum value of m given choices for k, n, h and l. Calling this m_{min}, we arrive at a central question of VCS optimization:

What is $m_{min}(k, n, h, l)$?

Note that this question is not just important for α_T. Indeed, if $m_{min}(k, n, h, l)$ can be determined, it becomes a straightforward matter to find contrast optimal, minimum pixel expansion schemes for **any** definition of contrast! The only parameters of relevance in determining contrast are h, l, and m. Determining $m_{min}(k, n, h, l)$ allows us to express m as a function of the independent parameters h and l. Given a definition of contrast, denoted α, optimizing is then simply a matter of maximizing the function $\alpha(h, l)$, which can be done using calculus.

The rest of this paper considers (k, n) schemes in which the parameters h and l are specified. As an extension of the basic notation for threshold schemes, we write a (k, n)-VCS with specified parameters h and l as a (k, n, h, l)-VCS. Similarly, when the pixel expansion m is also specified, we write this as a (k, n, h, l, m)-VCS.

4 Preliminaries

We begin our discussion with two simple but important results.

Theorem 4.1. *If there exists a (k, n, h, l, m)-VCS $(\mathcal{C}_0, \mathcal{C}_1)$, there exists a $(k, n, h, l, m+1)$-VCS $(\mathcal{C}'_0, \mathcal{C}'_1)$.*

Proof: Let X_n be the column vector consisting of n 1's. Consider $\mathcal{C}'_j = \{C \oplus X_n : C \in \mathcal{C}_j\}, j = 0, 1$, where $\oplus$ represents concatenation. This is a $(k, n, h, l, m+1)$-VCS, as required. ■

Note that in a (k, n, h, l, m)-VCS constructed with basis matrices, appending X_n to S_0 and S_1 will also create a $(k, n, h, l, m+1)$-VCS.

Theorem 4.1 shows that if a (k, n, h, l)-VCS exists at all, then the determination of $m_{min}(k, n, h, l)$ exactly determines for which m a (k, n, h, l, m) scheme exists. Both implicit and explicit in Definition 2.1 are necessary conditions on k, n, h and l to have a meaningful VCS. These conditions are enumerated in Fact 4.1.

Fact 4.1. *The following are necessary conditions for the existence of a (k, n, h, l)-VCS.*

1. $k \in \mathbb{Z}, k \geq 2$.
2. $n \in \mathbb{Z}, n \geq 2$.
3. $k \leq n$.
4. $h \in \mathbb{Z}, h \geq 1$.
5. $l \in \mathbb{Z}, l \geq 0$.
6. $h > l$.

Theorem 4.2 shows that the above conditions are also sufficient.

Theorem 4.2. *If k, n, h and l meet the conditions of Fact 4.1, then a (k, n, h, l)-VCS exists.*

Proof: WLOG, we will construct schemes based on basis matrices. First, we make two observations.

1. If (S_0, S_1) defines a (k,n,h,l)-VCS and (S_0', S_1') defines a (k,n,h',l')-VCS, then $(S_0 \oplus S_0', S_1 \oplus S_1')$ defines a $(k,n,h+h',l+l')$-VCS.
2. If (S_0, S_1) defines a (k,n,h,l)-VCS, then $(S_0 \oplus Y_n, S_1 \oplus Y_n)$ defines a $(k,n,h+1,l+1)$-VCS, where Y_n is the column vector consisting of n 0's.

In [12], [4], $(k,n,1,0)$ schemes are constructed for all valid k and n (as in Fact 4.1.) We thus get the following algorithm for constructing a (k,n,h,l)-VCS.

1. Construct a $(k,n,h-l,0)$-VCS by concatenating $h-l$ copies of each basis matrix in the $(k,n,1,0)$ scheme specified in [12] or [4], viz. observation 1.
2. Append l copies of Y_n to each basis matrix in the scheme from step 1, creating a (k,n,h,l)-VCS, viz. observation 2.

Note that the algorithm works for any scheme satisfying the conditions of Fact 4.1. ■

Example 4.1. *A (3,4,3,1)-VCS*
To begin with, we need a $(3,4,1,0)$-VCS. By [4], such a scheme is given by the following basis matrices:

$$S_0' = \begin{bmatrix} 011111100 \\ 011110011 \\ 011001111 \\ 000111111 \end{bmatrix} \qquad S_1' = \begin{bmatrix} 111111000 \\ 111100110 \\ 111010101 \\ 111001011 \end{bmatrix}.$$

We concatenate two copies of each basis matrix to obtain a $(3,4,2,0)$-VCS:

$$S_0'' = \begin{bmatrix} 011111100011111100 \\ 011110011011110011 \\ 011001111011001111 \\ 000111111000111111 \end{bmatrix} \qquad S_1'' = \begin{bmatrix} 111111000111111000 \\ 111100110111100110 \\ 111010101111010101 \\ 111001011111001011 \end{bmatrix}.$$

Finally, we append a copy of Y_4 to each basis matrix to create our $(3,4,3,1)$-VCS:

$$S_0 = \begin{bmatrix} 0111111000111111000 \\ 0111100110111100110 \\ 0110011110110011110 \\ 0001111110001111110 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 1111110001111110000 \\ 1111001101111001100 \\ 1110101011110101010 \\ 1110010111110010110 \end{bmatrix}.$$

5 An Optimal Construction for Some $(2,n,h,l)$ Schemes

In this section, we will explicitly find m_{min} for a certain class of schemes.

Theorem 5.1. *If*

$$h \leq l\frac{n-1}{n-2}, \tag{1}$$

then $m_{min}(2,n,h,l) = 2h - l$.

Proof: We first describe a canonical $(2,n,h,l)$-VCS for h and l satisfying (1). The scheme has:

$$\mu_{0,0} = h, \qquad \mu_{n,0} = h - l,$$
$$\mu_{0,1} = (2-n)h + (n-1)l, \qquad \mu_{1,1} = h - l.$$

Note that $\mu_{0,1} \geq 0$ if and only if (1) holds.

Firstly,

$$\begin{aligned}
\sum_{j=0}^{n} \mu_{j,0} \binom{n}{j} &= h\binom{n}{0} + (h-l)\binom{n}{n} \\
&= 2h - l, \\
\sum_{j=0}^{n} \mu_{j,1} \binom{n}{j} &= ((2-n)h + (n-1)l)) \binom{n}{0} + (h-l)\binom{n}{1} \\
&= (2-n+n)h + (n-1-n)l \\
&= 2h - l,
\end{aligned}$$

so $m = 2h - l$.

The weight of any row of S_0 is clearly equal to $\mu_{n,0}$, or $h-l$. The weight of any row of S_1 is $\binom{1}{0} \times \mu_{1,1} = h-l$, so the security condition is satisfied.

The "or" of any two rows of S_0 has weight equal to $\mu_{n,0}$, or $h-l$, as well. Noting that $h - l = m - h$, the first of the contrast conditions is satisfied. The "or" of any two rows of S_1 has weight equal to $2\mu_{1,1} = 2h - 2l = m - l$, so the second contrast condition is satisfied, and we have a $(2, n, h, l, 2h-l)$-VCS. Thus, if (1) holds, $m_{min}(2, n, h, l) \leq 2h - l$.

Now, every row of S_0, and therefore S_1, has at least h 0's. Also, since the "or" of any two rows of S_1 has weight $\geq m - l$, and each row of S_1 has weight $\leq m - h$, each row of S_1 must have at least $(m - l) - (m - h) = h - l$ 1's. Thus, $m_{min}(2, n, h, l) \geq 2h - l$.

Combining the two inequalities, we have the desired result. ■

Example 5.1. *A* $(2, 5, 7, 6)$*-VCS*

We first note that

$$7 \leq 6\frac{5-1}{5-2},$$

so (1) holds. The basis matrices obtained by the construction are:

$$S_0 = \begin{bmatrix} 10000000 \\ 10000000 \\ 10000000 \\ 10000000 \\ 10000000 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \end{bmatrix}.$$

This scheme has $m = 2h - l = 8$.

6 A New Bound

6.1 A Proof of the Bound

In this section, we generalize the bound on $(2, n)$ schemes proven in [7] to include the parameters h and l. We begin by considering an arbitrary $(2, n, h, l, m)$-VCS $(\mathcal{C}_0, \mathcal{C}_1)$. In such a scheme, the "or" of any two rows of $C \in \mathcal{C}_0$ has weight $\leq m - h$, which implies any one row of C has weight $\leq m - h$. Also, the "or" of any two rows of $C \in \mathcal{C}_1$ has weight $\geq m - l$.

Let $C \in \mathcal{C}_1$. We define

$$T(C) = \left|\{(x, y, z) : c_{xz} = 1, c_{yz} = 0\}\right|.$$

If we examine any two rows of C, we will find a column permutation of the following situation:

$$\left[\begin{array}{ccc|ccc|ccc|ccc} 1 & \cdots & 1 & \overbrace{1 \; \cdots \; 1}^{\geq h-l} & & & \overbrace{0 \; \cdots \; 0}^{\geq h-l} & & & \overbrace{0 \; \cdots \; 0}^{\leq l} & & \\ 1 & \cdots & 1 & 0 \; \cdots \; 0 & & & 1 \; \cdots \; 1 & & & 0 \; \cdots \; 0 & & \end{array}\right]$$

It follows that

$$\begin{aligned} T(C) &\geq \binom{n}{2} \times (h-l) \times 2 \\ &= n(n-1)(h-l). \end{aligned} \tag{2}$$

Suppose we define the number of 1's in column z of C, $1 \leq z \leq m$, to be w_z. Then

$$T(C) = \sum_{z=1}^{m} w_z(n - w_z). \tag{3}$$

We can derive an upper bound on (3). We define

$$\bar{w} = \frac{\sum_{z=1}^{m} w_z}{m}.$$

The bound is stated as a lemma with accompanying proof.

Lemma 6.1. *If $w_z, z = 1, \ldots, m$, are real numbers, and $\bar{w}$ is defined as above, then*

$$\sum_{z=1}^{m} w_z(n - w_z) \leq m\bar{w}(n - \bar{w}). \tag{4}$$

Proof: Let $Z = \{(x, y) : x, y \in \{1, \ldots, m\}, w_y \neq w_x\}$. Suppose that $Z \neq \emptyset$, let $(x, y) \in Z$, and consider what happens if we let $w'_x = (w_x + w_y)/2$, $w'_y = (w_x + w_y)/2$. Looking at the portion of (4) involving w'_x and w'_y, we get the following:

$$\begin{aligned} w'_x(n - w'_x) + w'_y(n - w'_y) &= 2(\frac{w_x + w_y}{2})(n - \frac{w_x + w_y}{2}) \\ &= (w_x + w_y)(\frac{2n - w_x - w_y}{2}) \\ &= nw_x + nw_y - \frac{w_x^2}{2} - \frac{w_y^2}{2} - w_x w_y \\ &= nw_x - w_x^2 + nw_y - w_y^2 + \frac{w_x^2}{2} + \frac{w_y^2}{2} - w_x w_y \\ &= w_x(n - w_x) + w_y(n - w_y) + \frac{1}{2}(w_x - w_y)^2 \\ &> w_x(n - w_x) + w_y(n - w_y). \end{aligned}$$

Thus, if Z is non-empty, we can increase the value of (4).

Now $Z = \emptyset$ precisely when $w_z = \bar{w}$ for all $z \in \{1, \ldots, m\}$. So we have

$$\begin{aligned} \sum_{z=1}^{m} w_z(n - w_z) &\leq \sum_{z=1}^{m} \bar{w}(n - \bar{w}) \\ &= m\bar{w}(n - \bar{w}). \blacksquare \end{aligned}$$

As an aside, we note that this lemma is also a direct application of Jensen's inequality.

Since there are n rows in C with weight $\leq m-h$, we have

$$\sum_{z=1}^{m} w_z \leq n(m-h).$$

To determine a lower bound on $\sum_{z=1}^{m} w_z$, we will use the following lemma.

Lemma 6.2. *Let $x_1, \ldots, x_n$ be real numbers satisfying the condition $x_i + x_j \geq N$, $i = 1, \ldots, n$, $j = 1, \ldots, n$, $i \neq j$. Then*

$$\sum_{i=1}^{n} x_i \geq \frac{nN}{2}.$$

Proof: Consider the following sum:

$$\sum_{i=1}^{n} \sum_{\substack{j=1,\ldots,n \\ j>i}} x_i + x_j.$$

This is a sum of $\binom{n}{2}$ pairs, each of which are $\geq N$. Thus,

$$\sum_{i=1}^{n} \sum_{\substack{j=1,\ldots,n \\ j>i}} x_i + x_j \geq \frac{n(n-1)N}{2}.$$

However, the sum can be rearranged, noting that each number x_i, $i = 1, \ldots, n$ appears exactly $n-1$ times. This implies

$$(n-1)\sum_{i=1}^{n} x_i \geq \frac{n(n-1)N}{2},$$

and so

$$\sum_{i=1}^{n} x_i \geq \frac{nN}{2}. \blacksquare$$

Letting x_i be the weight of row i of C, and $N = m - l$, we find that the lemma applies. Since the total weight of all rows of C is the same as the total weight of all columns of C, we have

$$\sum_{z=1}^{m} w_z \geq \frac{n(m-l)}{2}.$$

Thus,

$$\frac{n(m-l)}{2m} \leq \bar{w} \leq \frac{n(m-h)}{m}. \tag{5}$$

Consider the function $f(x) = mx(n-x)$. f attains its maximum at $x = n/2$, $f'(x) > 0$ for $x < n/2$ and $f'(x) < 0$ for $x > n/2$. Combining this with (5), we examine three cases.

Case 1 This case is characterized by the following inequality:

$$\boxed{\frac{n(m-l)}{2m} \geq \frac{n}{2}.}$$

This is equivalent to

$$\frac{m-l}{m} \geq 1,$$

which occurs if and only if $l \leq 0$. The only possibility, due to Fact 4.1, is $l = 0$. Then

$$\begin{aligned} m\bar{w}(n-\bar{w}) &\leq m(\frac{n(m-l)}{2m})(n - \frac{n(m-l)}{2m}) \\ &= m\frac{n}{2}\frac{n}{2}. \end{aligned}$$

Combining this with (2), we obtain

$$n(n-1)(h-l) \leq \frac{mn^2}{4},$$

and hence

$$m \geq \frac{4(n-1)h}{n}. \tag{6}$$

Case 2 Case 2 occurs when we have

$$\boxed{\frac{n(m-h)}{m} \leq \frac{n}{2}.}$$

This is equivalent to

$$h \geq \frac{m}{2}.$$

Then

$$m\bar{w}(n-\bar{w}) \leq m(\frac{n(m-h)}{m})(\frac{nh}{m}),$$

giving

$$n(n-1)(h-l) \leq \frac{(m-h)hn^2}{m}$$

whence

$$m \geq \frac{nh^2}{ln+h-l}. \tag{7}$$

Case 3 This case corresponds to

$$\boxed{\frac{n(m-l)}{2m} \leq \frac{n}{2} \leq \frac{n(m-h)}{m}.}$$

Then

$$m\bar{w}(n-\bar{w}) \leq m(\frac{n}{2})(\frac{n}{2})$$

which implies

$$n(n-1)(h-l) \leq \frac{mn^2}{4}$$

and thus

$$m \geq \frac{4(h-l)(n-1)}{n}. \tag{8}$$

Theorem 4.2 of [7] states that in any $(2,n)$-VCS,

$$\alpha_{NS} \leq \frac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}.$$

Recalling the definition of α_{NS}, and rearranging, we find

Theorem 6.1.

$$m_{min}(2,n,h,l) \geq \frac{n(n-1)}{\lfloor n/2 \rfloor \lceil n/2 \rceil}(h-l).$$

Note that (8) is equivalent to the above when n is even, and only slightly weaker when n is odd.

The bound proven in Case 1 tends asymptotically to $m \geq 4h$. This is quite weak. We have a much stronger bound, which follows directly from Theorem 5.5 of [12], letting $k=2$.

Theorem 6.2. *[12] In a $(2,n,h,0)$-VCS $(\mathcal{C}_0, \mathcal{C}_1)$, $m \geq nh$.*

We now describe a canonical $(2,n,h,0)$-VCS which meets this bound with equality. The multiplicities are:

$$\mu_{0,0} = h, \qquad \mu_{n,0} = (n-1)h, \qquad \mu_{n-1,1} = h.$$

We have

$$\begin{aligned}
\sum_{i=0}^{n} \mu_{i,1}\binom{n}{i} &= \mu_{n-1,1}\binom{n}{n-1} \\
&= hn, \\
\sum_{i=0}^{n} \mu_{i,0}\binom{n}{i} &= \mu_{0,0}\binom{n}{0} + \mu_{n,0}\binom{n}{n} \\
&= h + (n-1)h \\
&= nh,
\end{aligned}$$

so $m = nh$. To prove that we have a $(2,n,h,0)$-VCS, we simply note that the basis matrices described above simply consist of h concatenations of the basis matrices for the $(k,n,1,0)$-VCS described in [4], when $k=2$. Therefore, the fact that we have described a $(2,n,h,0)$-VCS follows directly from Theorem 3.1 of [4]. We have proven the following result.

Theorem 6.3. *$m_{min}(2,n,h,0) = nh$.*

In summary, we have the following.

Theorem 6.4. *The following are necessary conditions for the existence of a* $(2, n, h, l, m)$*-VCS:*

$$m \geq \begin{cases} nh, & \text{if } l = 0 \\ \frac{nh^2}{ln+h-l}, & \text{if } h \geq m/2 \\ \frac{4(h-l)(n-1)}{n}, & \text{otherwise.} \end{cases}$$

6.2 A Strengthening of the Bound

A key simplification above was (4). It removed the need to examine the complicated expression $\sum_{z=1}^{m} w_z(n-w_z)$. However, (4) can be met with equality only if $\bar{w}$ is an integer. Here, we attempt to find a stronger inequality in the case where $\bar{w}$ is not an integer. The following lemma is invaluable to this analysis.

Lemma 6.3. *If* $w_z, z = 1, \ldots, m$, *are all integers, and* $\bar{w}$ *is defined as above, then the value of*

$$\sum_{z=1}^{m} w_z(n - w_z) \tag{9}$$

is maximized when every w_z *is equal to* $\lfloor \bar{w} \rfloor$ *or* $\lceil \bar{w} \rceil$.

Proof: Let $Z = \{(x, y) : x, y \in \{1, \ldots, m\}, w_y - w_x \geq 2\}$. Suppose $Z \neq \emptyset$, let $(x, y) \in Z$, and consider what happens if we let $w'_x = w_x + 1$, $w'_y = w_y - 1$. Looking at the portion of (9) involving w'_x and w'_y, we get the following:

$$\begin{aligned} w'_x(n - w'_x) + w'_y(n - w'_y) &= (w_x + 1)(n - w_x - 1) + (w_y - 1)(n - w_y + 1) \\ &= w_x n - w_x^2 - w_x + n - w_x - 1 + \\ &\quad\; w_y n - w_y^2 + w_y - n + w_y - 1 \\ &= w_x(n - w_x) + w_y(n - w_y) + 2w_y - 2w_x - 2 \\ &> w_x(n - w_x) + w_y(n - w_y). \end{aligned}$$

Thus, if Z is non-empty, we can increase the value of (9).

If $\bar{w}$ is integral, then $Z = \emptyset$ precisely when $w_z = \bar{w}$ for all $z \in \{1, \ldots, m\}$. Since $\bar{w} = \lfloor \bar{w} \rfloor = \lceil \bar{w} \rceil$ in this case, we have the desired result.

Otherwise, $Z = \emptyset$ when every w_z is within 1 of $\bar{w}$, meaning $w_z = \lfloor \bar{w} \rfloor$ or $w_z = \lceil \bar{w} \rceil$, $z = 1, \ldots, m$. ■

In fact, by the definition of $\bar{w}$, we can see that the maximum value of (9) is obtained when we have $m(\bar{w} - \lfloor \bar{w} \rfloor)$ w_z's with weight $\lceil \bar{w} \rceil$, and $m(1 - \bar{w} + \lfloor \bar{w} \rfloor)$ w_z's with weight $\lfloor \bar{w} \rfloor$. (Note that if $\bar{w}$ is an integer, this simply says that all m w_z's have value $\bar{w}$.) Combining this analysis with (3), we obtain the following strengthening of (4):

$$T(C) \leq m\big(\lceil \bar{w} \rceil (n - \lceil \bar{w} \rceil)(\bar{w} - \lfloor \bar{w} \rfloor) + \lfloor \bar{w} \rfloor (n - \lfloor \bar{w} \rfloor)(1 - \bar{w} + \lfloor \bar{w} \rfloor)\big). \tag{10}$$

Now, consider the function

$$f^*(x) = m\big(\lceil x \rceil (n - \lceil x \rceil)(x - \lfloor x \rfloor) + \lfloor x \rfloor (n - \lfloor x \rfloor)(1 - x + \lfloor x \rfloor)\big).$$

f^* attains its maximum at every point on the interval $[\lfloor n/2 \rfloor, \lceil n/2 \rceil)$. Further, f^* is strictly increasing over the interval $[0, \lfloor n/2 \rfloor)$ and strictly decreasing over the interval $[\lceil n/2 \rceil, n]$. (A detailed proof of these facts is left to Appendix B.) Combining this with (5), we once again have three cases.

Case 1 This case is characterized by the following inequality:

$$\boxed{\frac{n(m-l)}{2m} \geq \lceil \frac{n}{2} \rceil.}$$

We note that if n is odd, the above inequality is satisfied if and only if $l < 0$. By Fact 4.1, this cannot occur, so Case 1 never occurs if n is odd. (It is, however, important to realize that this does not say $(2, n, h, 0)$ schemes with n odd do not exist, but rather that these schemes fall into the other two cases.) If n is even, the only valid situation is $l = 0$. Then

$$\begin{aligned} f^*(\bar{w}) &\leq m\big(\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor (\frac{n}{2} - \lfloor \frac{n}{2} \rfloor) + \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil (1 - \frac{n}{2} + \lfloor \frac{n}{2} \rfloor)\big) \\ &= m \frac{n}{2} \frac{n}{2}. \end{aligned}$$

Combining this with (2), we obtain

$$n(n-1)(h-l) \leq \frac{mn^2}{4}$$

giving

$$m \geq \frac{4(n-1)h}{n}. \tag{11}$$

This bound is equivalent to (6).
Case 2 Case 2 occurs when we have

$$\boxed{\frac{n(m-h)}{m} < \lfloor \frac{n}{2} \rfloor.}$$

This is equivalent to

$$h > \frac{m}{2} + (\frac{n}{2} - \lfloor \frac{n}{2} \rfloor)(\frac{m}{n}).$$

Then

$$\begin{aligned} f^*(\bar{w}) &\leq m\big(\lceil \frac{n(m-h)}{m} \rceil (n - \lceil \frac{n(m-h)}{m} \rceil)(\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor) + \\ &\quad \lfloor \frac{n(m-h)}{m} \rfloor (n - \lfloor \frac{n(m-h)}{m} \rfloor)(1 - \frac{n(m-h)}{m} + \lfloor \frac{n(m-h)}{m} \rfloor)\big) \\ &= m\big(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor (\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor) + \\ &\quad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil (1 - \frac{n(m-h)}{m} + \lfloor \frac{n(m-h)}{m} \rfloor)\big). \end{aligned}$$

It is not clear how to further simplify this. So we have the following bound:

$$\begin{aligned} n(n-1)(h-l) &\leq m\big(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor (\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor) + \\ &\quad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil (1 - \frac{n(m-h)}{m} \lfloor \frac{n(m-h)}{m} \rfloor)\big). \end{aligned} \tag{12}$$

Case 3 This case corresponds to

$$\boxed{\frac{n(m-l)}{2m} \leq x \leq \frac{n(m-h)}{m},}$$

for some $x \in [\lfloor n/2 \rfloor, \lceil n/2 \rceil)$. Note that

$$[\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil)$$

is the empty set if n is even. Otherwise,

$$\begin{aligned} f^*(\bar{w}) &\leq m\big(\lceil x \rceil(n - \lceil x \rceil)(x - \lfloor x \rfloor) + \lfloor x \rfloor(n - \lfloor x \rfloor)(1 - x + \lfloor x \rfloor)\big) \\ &= m\big(\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor (x - \lfloor x \rfloor) + \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil (1 - x + \lfloor x \rfloor)\big) \\ &= m \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil \end{aligned}$$

which implies

$$n(n-1)(h-l) \leq m \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil$$

whence

$$m \geq \frac{n(n-1)}{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}(h-l). \tag{13}$$

This is precisely the bound of Theorem 6.1.

We summarize the above in the following theorem.

Theorem 6.5. *The following are necessary conditions for the existence of a* $(2, n, h, l, m)$ *-VCS:*

$$\begin{aligned} m &\geq nh, \quad \textit{if } l = 0 \\ n(n-1)(h-l) &\leq m\Big(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor \big(\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor\big) + \\ &\qquad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil \big(1 - \frac{n(m-h)}{m} \lfloor \frac{n(m-h)}{m} \rfloor\big)\Big), \\ &\qquad \textit{if } h > \tfrac{m}{2} + (\tfrac{n}{2} - \lfloor \tfrac{n}{2} \rfloor)(\tfrac{m}{n}) \\ m &\geq \frac{n(n-1)}{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}(h-l), \quad \textit{otherwise.} \end{aligned}$$

It is important to note that these bounds help determine the non-existence of particular $(2, n, h, l, m)$ schemes. Given n, h, l and m, we can determine which case we are in. If the inequality for this case is not satisfied, then a $(2, n, h, l, m)$ scheme does not exist. Letting m' be the smallest value of m for which the associated inequality is satisfied, we have a bound on m_{min}:

$$m_{min}(2, n, h, l) \geq m'.$$

Example 6.1. *Determining whether or not a* $(2, 4, 8, 4, 13)$*-VCS exists*

Since $h \geq m/2$, we are in Case 2. Theorem 6.4 states

$$\begin{aligned} m &\geq \frac{nh^2}{ln + h - l} \\ &= \frac{4 \times 8^2}{4 \times 4 + 8 - 4} \\ &= \frac{64}{5}. \end{aligned}$$

Since $\lceil 64/5 \rceil = 13$, Theorem 6.4 does not rule out the existence of a $(2,4,8,4,13)$-VCS. Now we examine Theorem 6.5. We have $n(n-1)(h-l) = 48$. If we calculate the right hand side of the Case 2 bound for Theorem 6.5, we find that the smallest value of m which satisfies the bound is $m = 14$. In particular, when $m = 13$, the right hand side is 46. Thus, Theorem 6.5 proves that a $(2,4,8,4,13)$-VCS does not exist. For reference, a $(2,4,8,4,14)$-VCS does exist.

6.3 Analysis of Equality

Under what conditions would the inequalities of Theorem 6.4 be met with equality? In Case 1, we have already answered this question. Namely, for any n and h, a $(2,n,h,0)$-VCS can be constructed such that $m = nh$, so there are no additional conditions. The inequality of Case 3 is met with equality only if we have an α_{NS}-optimal $(2,n,h,l)$-VCS, and this situation is examined in [7]. So we are only left with Case 2.

In particular, we search for schemes such that $h \geq m/2$ and

$$m = \frac{nh^2}{ln + h - l}.$$

Working backwards, we have

$$n(n-1)(h-l) = m\frac{n(m-h)}{m}\frac{nh}{m},$$

which implies that

$$\begin{aligned} n(n-1)(h-l) &= T(C) \\ &= \sum_{z=1} m w_z (n - w_z) \\ &= m\bar{w}(n-\bar{w}) \\ &= m\frac{n(m-h)}{m}\frac{nh}{m}. \end{aligned} \tag{14}$$

We can derive many implications from the above set of equalities. Firstly, we see that every column of $C \in \mathcal{C}_1$ must have weight $\bar{w}$, and further that $\bar{w} = n(m-h)/m$. We know that in any pair of rows of C, the unavoidable patterns $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$ must occur exactly $h-l$ times each [7]. This implies that the pattern $\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$ must occur exactly l times in each pair of rows of C (or the security condition would be violated), so every row of C must have a weight of exactly $m-h$. Finally, this implies that the pattern $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$ occurs exactly $m-2h+l$ times. Combining all this information, we find that C is the incidence matrix of an $(n, n(m-h)/m, m-2h+l)$ balanced incomplete block design (BIBD), as defined below.

Definition 6.1. *[8] A (v,k,λ)-BIBD is a pair $(\mathcal{V},\mathcal{B})$, where $\mathcal{V}$ is a set of v elements, or points, and $\mathcal{B}$ is a set of b subsets of $\mathcal{V}$, called blocks, such that each block contains exactly k points, and every pair of points is contained in exactly λ blocks.*

It follows from the Definition 6.1 that every point appears in exactly $r = \lambda(v-1)/(k-1)$ blocks, and also that $b = \lambda(v^2 - v)/(k^2 - k)$.

Definition 6.2. *Let $(\mathcal{V},\mathcal{B})$ be a design with $\mathcal{V} = \{V_1, \ldots, V_v\}$, $\mathcal{B} = \{B_1, \ldots, B_b\}$. Then the incidence matrix M of the design is a $v \times b$ matrix satisfying*

$$m_{ij} = \begin{cases} 1, & V_i \in B_j \\ 0, & \textit{otherwise.} \end{cases}$$

If every row of $C \in \mathcal{C}_1$ has weight $m-h$, then for $C \in \mathcal{C}_0$, we must have a permutation of the following:

$$\left[\begin{array}{cccccc} \multicolumn{3}{c}{\overbrace{\hphantom{1 \cdots 1}}^{\text{m-h}}} & \multicolumn{3}{c}{\overbrace{\hphantom{0 \cdots 0}}^{\text{h}}} \\ 1 & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right]$$

Thus, we arrive at the following theorem:

Theorem 6.6. *A $(2,n,h,l,m)$-VCS with $h \geq m/2$ and $m = (nh^2)/(ln+h-l)$ exists if and only if an $(n, n(m-h)/m, m-2h+l)$-BIBD exists.*

Example 6.2. *A $(2,13,9,6,13)$-VCS*
We have

$$\begin{aligned} \frac{nh^2}{ln+h-l} &= \frac{13 \times 9^2}{6 \times 13 + 9 - 6} \\ &= \frac{13 \times 9^2}{81} \\ &= 13, \end{aligned}$$

so a $(2,13,9,6,13)$-VCS exists if and only if a $(13,4,1)$-BIBD exists. Such a BIBD is described by the following incidence matrix:

$$\left[\begin{array}{c} 1111000000000 \\ 1000111000000 \\ 0100100110000 \\ 1000000101100 \\ 0010100001010 \\ 0010010100001 \\ 0001010011000 \\ 0010001010100 \\ 0100010000110 \\ 1000000010011 \\ 0001100000101 \\ 0001001100010 \\ 0100001001001 \end{array}\right].$$

This represents the basis matrix S_1 for our $(2,13,9,6,13)$-VCS. S_0 consists of 13 identical rows of weight 4.

Now we turn our attention to Theorem 6.5. Again, Case 1 and Case 3 follow from previous work, so we need only examine Case 2. In particular, we seek schemes such that

$$h \geq \frac{m}{2} + \left(\frac{n}{2} - \lfloor \frac{n}{2} \rfloor\right)\left(\frac{m}{n}\right)$$

and

$$\begin{aligned} n(n-1)(h-l) &= m\Big(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor \Big(\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor\Big) + \\ &\qquad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil \Big(1 - \frac{n(m-h)}{m} \lfloor \frac{n(m-h)}{m} \rfloor\Big)\Big). \end{aligned}$$

This condition implies a set of equations very similar to (14). Thus we find that every column of $C \in \mathcal{C}_1$ must have weight $\lfloor \bar{w} \rfloor$ or $\lceil \bar{w} \rceil$, where $\bar{w} = n(m-h)/m$. Also, every row of C has the same weight, namely $m-h$, and every pair of rows contains the pattern $\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$ exactly $m-2h+l$ times. So C is the incidence matrix of an $(n, \{\lfloor n(m-h)/m \rfloor, \lceil n(m-h)/m \rceil\}, m-2h+l)$ pairwise balanced design (PBD).

Definition 6.3. *[8] A (v, K, λ)-PBD is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a set of v points, K is a set of positive integers such that $2 \leq k < v$ for every $k \in K$, and $\mathcal{B}$ is a collection of blocks such that $|B| \in K$ for every $B \in \mathcal{B}$ and each pair of points is contained in exactly λ blocks.*

Once again, the above conditions also uniquely specify any $C \in \mathcal{C}_0$, and we have proven the following theorem:

Theorem 6.7. *A $(2, n, h, l, m)$-VCS with*

$$h \geq \frac{m}{2} + \left(\frac{n}{2} - \lfloor \frac{n}{2} \rfloor\right)\left(\frac{m}{n}\right)$$

and

$$\begin{aligned} n(n-1)(h-l) &= m\Big(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor \Big(\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor\Big) + \\ &\quad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil \Big(1 - \frac{n(m-h)}{m} \lfloor \frac{n(m-h)}{m} \rfloor\Big)\Big). \end{aligned}$$

exists if and only if an $(n, \lfloor n(m-h)/m \rfloor, \lceil n(m-h)/m \rceil\}, m-2h+l)$-PBD exists such that every point occurs in exactly $m-h$ blocks.

7 $(2, n, h, l, m)$ Schemes with Fixed S_0

7.1 Effects of the Restriction

In the previous section, we found that letting the pixel expansion be optimal forced every row of $C \in \mathcal{C}_0 \cup \mathcal{C}_1$ to have weight $m-h$. In this section, we start off by imposing this restriction on the rows of S_0 and S_1, and examine the effect on the pixel expansion. As we have seen, forcing rows to have weight $m-h$ has the benefit of completely specifying S_0 up to column permutation.

Another, less obvious effect of this new restriction is the following. The total number of 1's in S_1 is now fixed at $n(m-h)$. Thus $\bar{w}$, as defined in the previous section, is also fixed, as demonstrated by the following:

$$\begin{aligned} \bar{w} &= \frac{\sum_{z=1}^{m} w_z}{m} \\ &= \frac{n(m-h)}{m} \\ &= n - \frac{nh}{m}. \end{aligned}$$

Then, regardless of which case we are in, we have that

$$\begin{aligned} f^*(\bar{w}) &= m\Big(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor \Big(\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor\Big) + \\ &\quad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil \Big(1 - \frac{n(m-h)}{m} + \lfloor \frac{n(m-h)}{m} \rfloor\Big)\Big). \end{aligned}$$

Thus we have the following theorem.

Theorem 7.1. *In any $(2,n,h,l,m)$-VCS with all rows of the basis matrix S_0 having weight exactly $m-h$, we must have the following:*

$$\begin{aligned} n(n-1)(h-l) \quad &\leq \quad m\left(\lceil\frac{n(m-h)}{m}\rceil\lfloor\frac{nh}{m}\rfloor\left(\frac{n(m-h)}{m}-\lfloor\frac{n(m-h)}{m}\rfloor\right)+\right. \\ &\qquad \left.\lfloor\frac{n(m-h)}{m}\rfloor\lceil\frac{nh}{m}\rceil\left(1-\frac{n(m-h)}{m}+\lfloor\frac{n(m-h)}{m}\rfloor\right)\right). \end{aligned} \tag{15}$$

As before, we can interpret this bound by choosing various values for m, given n, h and l. Let m' be the smallest value of m for which (15) is satisfied, and let $m_{ei}(2,n,h,l)$ be the smallest m for which a $(2,n,h,l)$-VCS with every row having weight $m-h$ exists. Then we have

$$m_{ei}(2,n,h,l) \geq m'.$$

In Section 9, we will see a way to find the exact values of $m_{min}(2,n,h,l)$ and $m_{ei}(2,n,h,l)$. An analysis of the tightness of (15) and a comparison of m_{min} and m_{ei} thus appears after that section.

8 Another Design Theory Connection

We now consider an additional restriction on $(2,n,h,l)$ schemes. As well as enforcing that all rows of the basis matrices have weight $m-h$, suppose we also require the "or" of any two rows of the basis matrix S_1 to have weight exactly $m-l$. To simplify the notation, we will refer to such schemes as *forced*.

The restrictions allow us to more accurately pinpoint the structure of the basis matrix S_1. In particular, any two rows of a forced S_1 are a permutation of the following:

$$\left[\begin{array}{cccc} \overbrace{1 \cdots 1}^{m-2h+l} & \overbrace{1 \cdots 1}^{h-l} & \overbrace{0 \cdots 0}^{h-l} & \overbrace{0 \cdots 0}^{l} \\ 1 \cdots 1 & 0 \cdots 0 & 1 \cdots 1 & 0 \cdots 0 \end{array}\right]$$

We can interpret S_1 as the incidence matrix of an (r,λ)-design. Let us first define such a design.

Definition 8.1. *[8] An (r,λ)-design is a pair $(\mathcal{V},\mathcal{B})$ where $\mathcal{V}$ is a set of v elements and $\mathcal{B}$ is a collection of b subsets (blocks) of $\mathcal{V}$ such that every distinct pair of elements occurs in precisely λ blocks and every variety (element) occurs in precisely r blocks.*

S_1 in our forced VCS can be seen as the incidence matrix of such a design, where $r=m-h$, $\lambda=m-2h+l$, $v=n$, $b=m$. Moreover, it is clear that there is a one-to-one correspondence between forced $(2,n,h,l)$ schemes and $(m-h,m-2h+l)$-designs. We have proven the following theorem.

Theorem 8.1. *There exists a forced $(2,n,h,l,m)$-VCS if and only if there exists a $(m-h,m-2h+l)$-design.*

The benefit of this realization is that results on (r,λ) designs can be directly applied to results on forced $(2,n,h,l)$ schemes. In particular, we can restate Theorem 38.3 of [8] as a result in visual cryptography.

Theorem 8.2. *In any forced $(2,n,h,l)$-VCS,*

$$m \geq \frac{nh^2}{h+ln-l}.$$

Note that this bound is precisely equivalent to the case 2 bound in subsection 6.1. This is to be expected, since forced schemes have

$$\bar{w} = \frac{n(m-h)}{m}$$

and so

$$m\bar{w}(n-\bar{w}) \leq m(\frac{n(m-h)}{m})(\frac{nh}{m}),$$

as in case 2. Note also that if $l = 0$, Theorem 8.2 reduces to $m \geq nh$. This is also not surprising, as the scheme constructed to prove $m_{min}(2,n,h,0) \leq nh$ is a forced scheme.

9 A Linear Programming Approach

9.1 Defining the Linear Program

In this section, we derive an integer LP whose solution gives us the value of $m_{min}(2,n,h,l)$. Let $b_i, i = 0,\ldots,2^n-1$, be a column vector representation of the binary encoding of the integer i, where the first coordinate represents the most significant bit. We pad the encoding with 0's when necessary in order to ensure that each b_i has length n. Note that the basis matrix S_1 for any (k,n)-VCS can be thought of as the concatenation of a collection of columns $b_{i_1}, b_{i_2}, \ldots, b_{i_m}$. Conversely, we can uniquely specify a matrix M, up to column permutation, simply by providing a list of non-negative integers x_i, $i = 1,\ldots,2^n-1$, where x_i represents the multiplicity of column b_i in M.

We will construct the basis matrix S_1 by a list of this form. Of course, an arbitrary list of multiplicities will, in general, not satisfy the contrast conditions of a VCS. For $j = 1,\ldots,n$ and $k = j+1,\ldots,n$, let C_{jk} be the set of elements i for which b_i has a 0 in coordinates j and k, $i = 0,\ldots,2^n-1$. If the matrix S_1 we construct is to be a basis matrix, it will then have to satisfy the following inequality:

$$\textstyle\sum_{i \in C_{jk}} x_i \leq l, \quad j = 1,\ldots,n, \quad k = j+1,\ldots,n,$$

which is precisely the contrast condition for reconstructing black pixels.

The x_i's also implicitly determine the weights of the rows in S_1. We denote these weights by a_j, $j = 1,\ldots,n$. Recall that any row of S_0 must have the same weight as the corresponding row of S_1. We now show a necessary and sufficient condition on the a_j's to ensure that the corresponding basis matrix S_0 can be constructed.

Lemma 9.1. *Suppose we wish to construct an $n \times m$ $\{0,1\}$ matrix M, such that the weight of row j must have weight a_j, $j = 1,\ldots,n$. Further, suppose that M must satisfy the property that the "or" of any two of its rows has weight $\leq m-h$. Then M can be constructed if and only if $a_j \leq m-h$, $j = 1,\ldots,m$.*

Proof: First suppose that some $a_j, j = 1,\ldots,n$ has weight $> m-h$. Then the "or" of row j with any other row of M will have a 1 in each column that row j has a 1, giving it a weight no less than that of row j. Thus, no valid M exists.

Now suppose that $a_j \leq m-h, j = 1,\ldots,n$. Then consider the matrix M where row j consists of a_j 1's followed by $m-a_j$ 0's. The "or" of rows j_1 and j_2 of M, $j_1 \neq j_2$, has weight no greater than the larger of a_{j_1} and a_{j_2}, and so M satisfies the conditions of the lemma. ■

The condition on the a_j's translates into a condition on the x_i's as follows. For $j = 1,\ldots,n$, let B_j be the set of elements i for which b_i has a 0 in coordinate j, $i = 0,\ldots,2^n-1$. Then the condition which ensures the existence of the basis matrix S_0 is

$$\sum_{i \in B_j} x_i \geq h, \quad j = 1,\ldots,n.$$

We have proven the following lemma.

Lemma 9.2. *There exists a $(2,n,h,l,m)$-VCS if and only if there exist non-negative integers x_i satisfying the following conditions:*

1. $\sum_{i \in B_j} x_i \geq h$ *for all* $j = 1, \ldots, n$.

2. $\sum_{i \in C_{jk}} x_i \leq l$ *for all* $j = 1, \ldots, n,\ k = j+1, \ldots, n$.

Note that since every row has non-zero weight, there exists at least one copy of the all 1's vector in S_0. Thus, if there existed a copy of the all 1's vector in S_1, we could remove an all 1's column from S_0 and S_1 and get a $(2, n, h, l)$-VCS with a smaller m. Since we are searching for $m_{min}(2, n, h, l)$, we can assume without loss of generality that $x_{2^n - 1} = 0$.

Thus we arrive at the following integer linear program, denoted ILPMMIN, whose optimal solution is $m_{min}(2, n, h, l)$:

Minimize:

$$m = \sum_{i=0}^{2^n - 2} x_i$$

Subject to:

$$\begin{array}{ll} \sum_{i \in B_j} x_i \geq h & \text{for } j = 1, \ldots, n \\ \sum_{i \in C_{jk}} x_i \leq l & \text{for } j = 1, \ldots, n, k = j+1, \ldots, n \\ x_i \geq 0 & \text{for } i = 0, \ldots, 2^n - 2 \\ x_i \text{ integer} & \text{for } i = 0, \ldots, 2^n - 2 \end{array}$$

The tables in Appendix A were produced by solving ILPMMIN for various values of n, h and l. The solver used was CPLEX.

Example 9.1. *Finding* $m_{min}(2, 4, 5, 3)$

The integer linear program is:

Minimize:

$$m = \sum_{i=0}^{14} x_i$$

Subject to:

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \geq 5$$

$$x_0 + x_1 + x_2 + x_3 + x_8 + x_9 + x_{10} + x_{11} \geq 5$$

$$x_0 + x_1 + x_4 + x_5 + x_8 + x_9 + x_{12} + x_{13} \geq 5$$

$$x_0 + x_2 + x_4 + x_6 + x_8 + x_{10} + x_{12} + x_{14} \geq 5$$

$$x_0 + x_1 + x_2 + x_3 \leq 3$$

$$x_0 + x_1 + x_4 + x_5 \leq 3$$

$$x_0 + x_2 + x_4 + x_6 \leq 3$$

$$x_0 + x_1 + x_8 + x_9 \leq 3$$

$$x_0 + x_2 + x_8 + x_{10} \leq 3$$

$$x_0 + x_4 + x_8 + x_{12} \leq 3$$

$$x_i \geq 0 \qquad \text{for } i = 0, \ldots, 14$$

$$x_i \text{ integer} \qquad \text{for } i = 0, \ldots, 14$$

Plugging this into a linear program solver, we find $m_{min}(2, 4, 5, 3) = 8$. This corresponds to the solution

$$(x_0, \ldots, x_{14}) = (2, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0).$$

The basis matrices thus described are:

$$S_0 = \begin{bmatrix} 11100000 \\ 11100000 \\ 11100000 \\ 11100000 \end{bmatrix}, \qquad S_1 = \begin{bmatrix} 00000111 \\ 00011001 \\ 00101010 \\ 00110100 \end{bmatrix}.$$

9.2 An Explicit Solution to $m_{min}(2, 2, h, l)$

For $n = 2$, (ILPMMIN) reduces to:

Minimize:

$$m = x_0 + x_1 + x_2$$

Subject to:

$$x_0 + x_1 \geq h$$

$$x_0 + x_2 \geq h$$

$$x_0 \leq l$$

$$x_i \geq 0 \qquad \text{for } i = 0, \ldots, 2$$

$$x_i \text{ integer} \qquad \text{for } i = 0, \ldots, 2$$

It is obvious that the solution $x_0 = l$, $x_1 = h - l$, $x_2 = h - l$ is optimal. Thus:

$$m_{min}(2, 2, h, l) = 2h - l.$$

As per the solution, the basis matrices of a $(2, 2, h, l, 2h - l)$-VCS are a column permutation of:

$$S_0 = \left[\begin{array}{ccc} \overbrace{\begin{array}{ccc} 1 & \cdots & 1 \\ 1 & \cdots & 1 \end{array}}^{h-l} & \overbrace{\begin{array}{ccc} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{array}}^{h} \end{array} \right],$$

$$S_1 = \left[\begin{array}{ccc} \overbrace{\begin{array}{ccc} 1 & \cdots & 1 \\ 0 & \cdots & 0 \end{array}}^{h-l} & \overbrace{\begin{array}{ccc} 0 & \cdots & 0 \\ 1 & \cdots & 1 \end{array}}^{h-l} & \overbrace{\begin{array}{ccc} 0 & \cdots & 0 \\ 0 & \cdots & 0 \end{array}}^{l} \end{array} \right]$$

9.3 Another Optimal Class of $(2, n, h, l)$ Schemes

If we examine the tables in Appendix A, some patterns become evident. In particular, when h is large in comparison to l, the values of m_{min} seem to increase as a linear function of h, and decrease as a linear function of l. This motivates the following theorem:

Theorem 9.1. *If*

$$h \geq (n - 1)l, \tag{16}$$

then

$$m_{min}(2, n, h, l) = nh - \frac{n(n-1)}{2}l.$$

Proof: Given (16), we first describe a canonical $(2, n, h, l)$-VCS satisfying $m = nh - ln(n - 1)/2$. This will correspond to a solution to ILPMMIN with objective value $nh - ln(n - 1)/2$. The column multiplicities are as follows.

$$\mu_{0,0} = h, \qquad \mu_{n,0} = (n-1)h - \frac{n(n-1)}{2}l,$$

$$\mu_{n-2,1} = l, \qquad \mu_{n-1,1} = h - (n-1)l.$$

Note that $\mu_{n-1,1} \geq 0$ if and only if (16) holds.

We verify that the above μ's produce a VCS. Firstly,

$$\begin{aligned}
\sum_{j=0}^{n} \mu_{j,0} \binom{n}{j} &= h\binom{n}{0} + \left((n-1)h - \frac{n(n-1)}{2}l\right)\binom{n}{n} \\
&= nh - \frac{n(n-1)}{2}l, \\
\sum_{j=0}^{n} \mu_{j,1} \binom{n}{j} &= l\binom{n}{n-2} + \left(h - (n-1)l\right)\binom{n}{1} \\
&= \frac{n(n-1)}{2}l + nh - n(n-1)l \\
&= nh - \frac{n(n-1)}{2}l,
\end{aligned}$$

so

$$m = nh - \frac{n(n-1)}{2}l.$$

The weight of any row of S_0 is equal to $\mu_{n,0}$, or

$$(n-1)h - \frac{n(n-1)}{2}l.$$

The weight of any row of S_1 is

$$\begin{aligned}
\binom{n-1}{n-3}l + \binom{n-1}{n-2}\left(h - (n-1)l\right) &= \frac{(n-1)(n-2)}{2}l + (n-1)h - (n-1)^2 l \\
&= (n-1)h - \frac{n(n-1)}{2}l,
\end{aligned}$$

so the security condition is satisfied.

The "or" of any two rows of S_0 has weight equal to $\mu_{n,0}$, or

$$(n-1)h - \frac{n(n-1)}{2}l = m - h,$$

as well, so the first of the contrast conditions is satisfied. The "or" of any two rows of S_1 has weight equal to

$$\begin{aligned}
\left(\binom{n}{n-2} - 1\right)l + \binom{n}{n-1}\left(h - (n-1)l\right) &= nh - \left(\frac{n(n-1)}{2} - 1\right)l \\
&= m - l,
\end{aligned}$$

so the second contrast condition is satisfied, and we have the desired VCS.

We now examine the structure of ILPMMIN. We denote the constraints corresponding to

$$\sum_{i \in B_j} x_i \geq h \quad \text{for } j = 1, \ldots, n$$

as the *first set* of constraints, and the constraints corresponding to

$$\sum_{i \in C_{jk}} x_i \leq l \quad \text{for } j = 1, \ldots, n,\ k = j, \ldots, n$$

as the *second set* of constraints. Note that the first set contains n constraints, and the second set contains $n(n-1)/2$ constraints.

Let $X_j = \{x_i : w(b_i) = j\}$, $j = 0, \dots, n-1$. In other words, X_j is the set of variables corresponding to vectors of weight j. Every variable in X_j will occur in $n-j$ constraints from the first set, and $\binom{n-j}{2}$ constraints from the second set.

We drop the integrality constraints of ILPMMIN, put it in standard inequality form, and consider the dual linear program DILPMMIN. DILPMMIN will have $n + n(n-1)/2$ variables and $2^n - 2$ constraints. Denote the variables corresponding to the first set of primal constraints as the first set of dual variables, and label these $y_1, \dots, y_n$. Denote the variables corresponding to the second set of primal constraints as the second set of dual variables, and label these $y_{n+1}, \dots, y_{n+n(n-1)/2}$. Finally, we denote the set of dual constraints corresponding to primal variables in X_j by C_j.

Consider a solution $Y = (y_1, \dots, y_{n+n(n-1)/2}) = (1, \dots, 1)$. We must first prove this solution is feasible. Every dual constraint in C_{n-j} will contain j dual variables with coefficient 1 and $\binom{j}{2}$ dual variables with coefficient -1. If we plug Y into a dual constraint in C_{n-j}, we will obtain $j - \binom{j}{2}$. We must prove that this is ≤ 1, the right hand side of the constraint.

$$\begin{aligned} j - \binom{j}{2} &\leq 1 \Rightarrow \\ j - \frac{j(j-1)}{2} &\leq 1 \Rightarrow \\ (j-2)(j-1) \geq 0. \end{aligned}$$

Since j is integral, this inequality always holds. Finally, we note that Y is non-negative, and thus Y is feasible.

Evaluating the objective function at Y, we obtain

$$nh - \frac{n(n-1)}{2} l,$$

so we have found a feasible solution to DILPMMIN which has objective value equal to that of our solution to ILPMMIN. Thus, by strong duality, both solutions are optimal, and this completes the proof. ■

Example 9.2. *DILPMMIN for $n = 3$, $h = 7$, $l = 3$*

The dual is:

Maximize:

$$7y_1 + 7y_2 + 7y_3 - 3y_4 - 3y_5 - 3y_6$$

Subject to:

$$y_1 + y_2 + y_3 - y_4 - y_5 - y_6 \leq 1$$

$$y_1 + y_2 - y_4 \leq 1$$

$$y_1 + y_3 - y_5 \leq 1$$

$$y_1 \leq 1$$

$$y_2 + y_3 - y_6 \leq 1$$

$$y_2 \leq 1$$

$$y_3 \leq 1$$

$$y_i \geq 0 \qquad \text{for } i = 1, \ldots, 6$$

We see that $(1,1,1,1,1,1)$ is a feasible solution with objective value 12, precisely the value of $m_{min}(2,3,7,3)$.

10 A Comparison of m_{ei} and m_{min}

Theorem 6.5 contains a bound on $m_{min}(2,n,h,l)$ which is in three parts, whereas Theorem 7.1 is a single bound on $m_{ei}(2,n,h,l)$. We are ultimately concerned with m_{min}, but if m_{ei} provides a good approximation to m_{min}, than the reduction of three cases to one is very advantageous. Surprisingly, for $k=2$, m_{ei} is more than just an approximation.

Theorem 10.1. *$m_{min}(2,n,h,l) = m_{ei}(2,n,h,l)$.*

Proof: Firstly, since every $(2,n,h,l)$-VCS with rows of weight $m-h$ is still a $(2,n,h,l)$-VCS, we have $m_{min}(2,n,h,l) \leq m_{ei}(2,n,h,l)$.

Let S_0 and S_1 be basis matrices for a $(2,n,h,l)$-VCS with pixel expansion $m' = m_{min}(2,n,h,l)$. We will construct S_0' and S_1', which will be basis matrices for a $(2,n,h,l,m')$-VCS in which every row will have weight exactly $m'-h$. S_0' is defined as follows:

$$\begin{bmatrix} \overbrace{\begin{matrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{matrix}}^{m'-h} & \overbrace{\begin{matrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{matrix}}^{h} \end{bmatrix}$$

S_1' is derived from S_1 by replacing 0's with 1's in a random fashion until every row has weight exactly $m'-h$. Because we do not remove or alter the placement of any 1's in S_1, it follows immediately that the "or" of two rows of S_1' has weight no less than the "or" of the same two rows of S_1. In particular, the "or" of any two rows of S_1' has weight $\geq m'-l$. Thus, S_0' and S_1' are basis matrices for a $(2,n,h,l,m')$-VCS in which every row has weight $m'-h$. This shows that $m_{ei}(2,n,h,l) \leq m_{min}(2,n,h,l)$.

Combining the two inequalities, we have the desired result. ■

Theorem 10.1 shows that Theorem 7.1 is actually a bound on $m_{min}(2,n,h,l)$. Since the strongest bound is usually the most interesting, an obvious question to ask is which of Theorem 6.5 and Theorem 7.1 is stronger. We will examine the three cases of Theorem 6.5, and compare the two bounds in each case. First, recall (15), the bound contained in Theorem 7.1:

$$\begin{aligned} n(n-1)(h-l) \quad &\leq \quad m(\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor (\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor) + \\ &\qquad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil (1 - \frac{n(m-h)}{m} + \lfloor \frac{n(m-h)}{m} \rfloor)). \end{aligned}$$

The easiest case to analyze is Case 2, because in this case Theorem 6.5 and (15) are identical, and thus the two bounds are trivially equally strong.

If we rearrange the Case 3 bound, we obtain

$$n(n-1)(h-l) \leq m\lfloor n/2 \rfloor \lceil n/2 \rceil.$$

We note that

$$\begin{aligned} &\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor (\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor) + \\ &\quad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil (1 - \frac{n(m-h)}{m} + \lfloor \frac{n(m-h)}{m} \rfloor) \end{aligned}$$

can be considered as an average of two products, namely

$$\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor$$

and

$$\lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil.$$

Further, we note that each product is of the form $x(n-x)$. Then Lemma 6.3 applies to each product, and we see

$$\lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor \leq \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil$$

and

$$\lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil \leq \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil.$$

Thus we have

$$\begin{aligned} \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil \quad &\geq \quad \lceil \frac{n(m-h)}{m} \rceil \lfloor \frac{nh}{m} \rfloor (\frac{n(m-h)}{m} - \lfloor \frac{n(m-h)}{m} \rfloor) + \\ &\qquad \lfloor \frac{n(m-h)}{m} \rfloor \lceil \frac{nh}{m} \rceil (1 - \frac{n(m-h)}{m} + \lfloor \frac{n(m-h)}{m} \rfloor). \end{aligned}$$

This implies that the minimum value of m which satisfies (15) is no less than the minimum value of m which satisfies the Case 3 bound, and thus Theorem 7.1 is no weaker than Theorem 6.5.

Finally, we examine Case 1, where we know our bound is optimal. As proven in Appendix B, $f^*(x)$ can be written in the form

$$x(n-x) + \tau^2 - \tau,$$

where $\tau(x) = x - \lfloor x \rfloor$. Since $\tau^2 - \tau \leq 0$, this implies (15) is no weaker than Case 2 of Theorem 6.4, and when $l = 0$,

$$m \geq \frac{nh^2}{ln + h - l}$$

simply becomes $m \geq nh$. Thus, it must be that (15) implies that $m \geq nh$ if $l = 0$. We conclude that in all cases, Theorem 7.1 is at least as strong as Theorem 6.5, and we need only consider (15).

As a final comment, we can see that Theorem 7.1 actually predicts m_{min} quite well. The values of m_{min} for approximately 10000 choices of the parameters have been calculated. (A subset of these are displayed in Appendix A.) Theorem 7.1 correctly predicts these values in all but two instances, namely $(2, 7, 2, 1)$ and $(2, 8, 2, 1)$, where the bound allows m to be as small as 4. In reality, $m_{min}(2, 7, 2, 1) = m_{min}(2, 8, 2, 1) = 5$.

11 Conclusions and Open Problems

We have examined the Naor and Shamir and the Verheul and Van Tilborg definitions of contrast, and found them both inadequate. We have provided a new measurement for contrast. However, the correctness of α_T has by no means been established. An appropriate measurement for contrast remains a central open problem.

A new question has been introduced, namely that of finding the smallest value of m for which a (k, n, h, l, m)-VCS exists. We have proven basic existence theorems for (k, n, h, l) schemes. Progress has been made in the case $k = 2$. In particular, two classes of $(2, n, h, l)$ schemes have been described in which $m = m_{min}(2, n, h, l)$. A new bound on $m_{min}(2, n, h, l)$ has been given, which works very well for tested parameter values. Several connections between $(2, n, h, l)$ schemes and designs have been demonstrated. We have also described an integer linear program whose solution gives both $m_{min}(2, n, h, l)$ and a $(2, n, h, l)$ scheme meeting this bound. Slight variations of the ILP find the corresponding values of $m_{ei}(2, n, h, l)$ and $m_{ee}(2, n, h, l)$.

We have also introduced many open questions. The central problem is an explicit expression for $m_{min}(k, n, h, l)$. Other questions include how well m_{ei} approximates m_{min}, how well the bound performs for large values of n, and whether a linear program exists to find $m_{min}(k, n, h, l)$ for values of $k > 2$.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson. Extended capabilities for visual cryptography. To appear in *Theoretical Computer Science.*

[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129:86–106, 1996.

[3] C. Blundo and A. De Bonis. New constructions for visual cryptography. In *Theoretical Computer Science (Prato, 1998)*, pages 290–303. World Sci. Publishing, 1998.

[4] C. Blundo, A. De Bonis, and A. De Santis. Improved schemes for visual cryptography. Preprint.

[5] C. Blundo, P. D'Arco, A. De Santis, and D.R. Stinson. Contrast optimal threshold visual cryptography schemes. To appear in *SIAM Journal on Discrete Mathematics.*

[6] C. Blundo and A. De Santis. Visual cryptography schemes with perfect reconstruction of black pixels. *Computers and Graphics*, 22:449–455, 1998.

[7] C. Blundo, A. De Santis, and D.R. Stinson. On the contrast in visual cryptography schemes. *Journal of Cryptology*, 12:261–289, 1999.

[8] C.J. Colbourn and J.H. Dinitz, editors. *The CRC Handbook of Combinatorial Designs.* CRC Press, 1996.

[9] S. Droste. New results on visual cryptography. In *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 401–415. Springer-Verlag, 1996.

[10] T. Hofmeister, M. Krause, and H.U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. In *Computing and Combinatorics (Shanghai, 1997)*, volume 1276 of *Lecture Notes in Computer Science*, pages 176–185. Springer-Verlag, 1997.

[11] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 1995.

[12] E.R. Verheul and H.C.A. van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes, and Cryptography*, 11:179–196, 1997.

A Solutions to ILPMMIN and ILPMEE

The following tables represent the values of $m_{min}(2, n, h, l)$ for $n = 2, \ldots, 8$, $h = 1, \ldots, 24$, $l = 0, \ldots, h-1$. The values were obtained by solving ILPMMIN using CPLEX.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	2																							
2	4	3																						
3	6	5	4																					
4	8	7	6	5																				
5	10	9	8	7	6																			
6	12	11	10	9	8	7																		
7	14	13	12	11	10	9	8																	
8	16	15	14	13	12	11	10	9																
9	18	17	16	15	14	13	12	11	10															
10	20	19	18	17	16	15	14	13	12	11														
11	22	21	20	19	18	17	16	15	14	13	12													
12	24	23	22	21	20	19	18	17	16	15	14	13												
13	26	25	24	23	22	21	20	19	18	17	16	15	14											
14	28	27	26	25	24	23	22	21	20	19	18	17	16	15										
15	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16									
16	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17								
17	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18							
18	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19						
19	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20					
20	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21				
21	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22			
22	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23		
23	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	
24	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25

Table 1: Values of $m_{min}(2, 2, h, l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	3																							
2	6	3																						
3	9	6	4																					
4	12	9	6	5																				
5	15	12	9	7	6																			
6	18	15	12	9	8	7																		
7	21	18	15	12	10	9	8																	
8	24	21	18	15	12	11	10	9																
9	27	24	21	18	15	13	12	11	10															
10	30	27	24	21	18	15	14	13	12	11														
11	33	30	27	24	21	18	16	15	14	13	12													
12	36	33	30	27	24	21	18	17	16	15	14	13												
13	39	36	33	30	27	24	21	19	18	17	16	15	14											
14	42	39	36	33	30	27	24	21	20	19	18	17	16	15										
15	45	42	39	36	33	30	27	24	22	21	20	19	18	17	16									
16	48	45	42	39	36	33	30	27	24	23	22	21	20	19	18	17								
17	51	48	45	42	39	36	33	30	27	25	24	23	22	21	20	19	18							
18	54	51	48	45	42	39	36	33	30	27	26	25	24	23	22	21	20	19						
19	57	54	51	48	45	42	39	36	33	30	28	27	26	25	24	23	22	21	20					
20	60	57	54	51	48	45	42	39	36	33	30	29	28	27	26	25	24	23	22	21				
21	63	60	57	54	51	48	45	42	39	36	33	31	30	29	28	27	26	25	24	23	22			
22	66	63	60	57	54	51	48	45	42	39	36	33	32	31	30	29	28	27	26	25	24	23		
23	69	66	63	60	57	54	51	48	45	42	39	36	34	33	32	31	30	29	28	27	26	25	24	
24	72	69	66	63	60	57	54	51	48	45	42	39	36	35	34	33	32	31	30	29	28	27	26	25

Table 2: Values of $m_{min}(2,3,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	4																							
2	8	4																						
3	12	6	4																					
4	16	10	7	5																				
5	20	14	10	8	6																			
6	24	18	12	10	8	7																		
7	28	22	16	13	11	9	8																	
8	32	26	20	16	14	12	10	9																
9	36	30	24	18	16	14	12	11	10															
10	40	34	28	22	19	17	15	13	12	11														
11	44	38	32	26	22	20	18	16	14	13	12													
12	48	42	36	30	24	22	20	18	16	15	14	13												
13	52	46	40	34	28	25	23	21	19	17	16	15	14											
14	56	50	44	38	32	28	26	24	22	20	18	17	16	15										
15	60	54	48	42	36	30	28	26	24	22	20	19	18	17	16									
16	64	58	52	46	40	34	31	29	27	25	23	21	20	19	18	17								
17	68	62	56	50	44	38	34	32	30	28	26	24	22	21	20	19	18							
18	72	66	60	54	48	42	36	34	32	30	28	26	24	23	22	21	20	19						
19	76	70	64	58	52	46	40	37	35	33	31	29	27	25	24	23	22	21	20					
20	80	74	68	62	56	50	44	40	38	36	34	32	30	28	26	25	24	23	22	21				
21	84	78	72	66	60	54	48	42	40	38	36	34	32	30	28	27	26	25	24	23	22			
22	88	82	76	70	64	58	52	46	43	41	39	37	35	33	31	29	28	27	26	25	24	23		
23	92	86	80	74	68	62	56	50	46	44	42	40	38	36	34	32	30	29	28	27	26	25	24	
24	96	90	84	78	72	66	60	54	48	46	44	42	40	38	36	34	32	31	30	29	28	27	26	25

Table 3: Values of $m_{min}(2,4,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	5																							
2	10	4																						
3	15	7	5																					
4	20	10	7	5																				
5	25	15	10	8	6																			
6	30	20	14	10	9	7																		
7	35	25	17	14	11	10	8																	
8	40	30	20	17	14	12	10	9																
9	45	35	25	20	17	15	13	11	10															
10	50	40	30	24	20	17	15	14	12	11														
11	55	45	35	27	24	20	18	16	15	13	12													
12	60	50	40	30	27	24	20	19	17	15	14	13												
13	65	55	45	35	30	27	24	21	20	18	16	15	14											
14	70	60	50	40	34	30	27	24	22	20	19	17	16	15										
15	75	65	55	45	37	34	30	27	25	23	21	20	18	17	16									
16	80	70	60	50	40	37	34	30	27	25	24	22	20	19	18	17								
17	85	75	65	55	45	40	37	34	30	28	26	25	23	21	20	19	18							
18	90	80	70	60	50	44	40	37	34	30	29	27	25	24	22	21	20	19						
19	95	85	75	65	55	47	44	40	37	34	31	30	28	26	25	23	22	21	20					
20	100	90	80	70	60	50	47	44	40	37	34	32	30	29	27	25	24	23	22	21				
21	105	95	85	75	65	55	50	47	44	40	37	35	33	31	30	28	26	25	24	23	22			
22	110	100	90	80	70	60	54	50	47	44	40	37	35	34	32	30	29	27	26	25	24	23		
23	115	105	95	85	75	65	57	54	50	47	44	40	38	36	35	33	31	30	28	27	26	25	24	
24	120	110	100	90	80	70	60	57	54	50	47	44	40	39	37	35	34	32	30	29	28	27	26	25

Table 4: Values of $m_{min}(2,5,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	6																							
2	12	4																						
3	18	7	5																					
4	24	11	7	6																				
5	30	15	10	8	6																			
6	36	21	14	11	9	7																		
7	42	27	18	14	11	10	8																	
8	48	33	22	17	14	12	11	9																
9	54	39	26	21	17	15	13	12	10															
10	60	45	30	25	20	18	15	14	12	11														
11	66	51	36	29	24	21	18	16	15	13	12													
12	72	57	42	33	28	24	21	19	17	16	14	13												
13	78	63	48	37	32	27	24	22	20	18	17	15	14											
14	84	69	54	41	36	31	27	25	22	21	19	18	16	15										
15	90	75	60	45	40	35	30	28	25	23	21	20	18	17	16									
16	96	81	66	51	44	39	34	31	28	26	24	22	21	19	18	17								
17	102	87	72	57	48	43	38	34	31	29	26	25	23	22	20	19	18							
18	108	93	78	63	52	47	42	37	34	32	29	27	26	24	23	21	20	19						
19	114	99	84	69	56	51	46	41	37	35	32	30	28	27	25	24	22	21	20					
20	120	105	90	75	60	55	50	45	40	38	35	33	30	29	27	26	24	23	22	21				
21	126	111	96	81	66	59	54	49	44	41	38	36	33	31	30	28	27	25	24	23	22			
22	132	117	102	87	72	63	58	53	48	44	41	39	36	34	32	31	29	28	26	25	24	23		
23	138	123	108	93	78	67	62	57	52	47	44	42	39	37	35	33	32	30	29	27	26	25	24	
24	144	129	114	99	84	71	66	61	56	51	47	45	42	40	37	36	34	33	31	30	28	27	26	25

Table 5: Values of $m_{min}(2,6,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	7																							
2	14	5																						
3	21	7	5																					
4	28	12	7	6																				
5	35	17	11	8	7																			
6	42	21	14	11	9	7																		
7	49	28	19	14	12	10	8																	
8	56	35	24	18	14	12	11	9																
9	63	42	28	21	18	15	13	12	10															
10	70	49	33	26	21	18	16	14	13	11														
11	77	56	38	31	25	21	19	17	15	14	12													
12	84	63	42	35	28	25	21	19	17	16	14	13												
13	91	70	49	40	33	28	25	22	20	18	17	15	14											
14	98	77	56	45	38	32	28	25	23	21	19	18	16	15										
15	105	84	63	49	42	35	32	28	26	24	21	20	19	17	16									
16	112	91	70	54	47	40	35	32	28	26	24	22	21	20	18	17								
17	119	98	77	59	52	45	39	35	32	29	27	25	23	22	21	19	18							
18	126	105	84	63	56	49	42	39	35	32	30	28	26	24	23	21	20	19						
19	133	112	91	70	61	54	47	42	39	35	33	31	28	27	25	24	22	21	20					
20	140	119	98	77	66	59	52	46	42	39	35	33	31	29	28	26	25	23	22	21				
21	147	126	105	84	70	63	56	49	46	42	39	36	34	32	30	28	27	26	24	23	22			
22	154	133	112	91	75	68	61	54	49	46	42	39	37	35	33	31	29	28	27	25	24	23		
23	161	140	119	98	80	73	66	59	53	49	46	42	40	38	35	33	32	30	29	28	26	25	24	
24	168	147	126	105	84	77	70	63	56	53	49	46	42	40	38	36	34	33	31	30	28	27	26	25

Table 6: Values of $m_{min}(2, 7, h, l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	8																							
2	16	5																						
3	24	8	5																					
4	32	12	8	6																				
5	40	18	11	8	7																			
6	48	23	15	11	9	8																		
7	56	28	19	14	12	10	8																	
8	64	36	24	18	15	12	11	9																
9	72	44	30	22	18	15	13	12	10															
10	80	52	35	26	22	18	16	14	13	11														
11	88	60	40	31	26	22	19	17	15	14	12													
12	96	68	46	36	30	25	22	19	18	16	15	13												
13	104	76	51	42	34	29	25	22	20	18	17	16	14											
14	112	84	56	47	38	33	28	26	23	21	19	18	16	15										
15	120	92	64	52	43	37	32	29	26	24	22	20	19	17	16									
16	128	100	72	58	48	41	36	32	29	26	24	23	21	20	18	17								
17	136	108	80	63	54	45	40	36	32	30	27	25	23	22	21	19	18							
18	144	116	88	68	59	50	44	40	36	33	30	28	26	24	23	22	20	19						
19	152	124	96	74	64	55	48	44	39	36	33	31	29	27	25	24	23	21	20					
20	160	132	104	79	70	60	52	48	43	39	36	34	31	30	28	26	25	24	22	21				
21	168	140	112	84	75	66	56	52	47	42	40	37	34	32	30	28	27	26	24	23	22			
22	176	148	120	92	80	71	62	56	51	46	43	40	37	35	33	31	29	28	27	25	24	23		
23	184	156	128	100	86	76	67	60	55	50	46	43	40	38	36	34	32	30	29	28	26	25	24	
24	192	164	136	108	91	82	72	64	59	54	50	46	44	41	38	36	35	33	31	30	29	27	26	25

Table 7: Values of $m_{min}(2, 8, h, l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	2																							
2	4	3																						
3	6	5	4																					
4	8	7	6	5																				
5	10	9	8	7	6																			
6	12	11	10	9	8	7																		
7	14	13	12	11	10	9	8																	
8	16	15	14	13	12	11	10	9																
9	18	17	16	15	14	13	12	11	10															
10	20	19	18	17	16	15	14	13	12	11														
11	22	21	20	19	18	17	16	15	14	13	12													
12	24	23	22	21	20	19	18	17	16	15	14	13												
13	26	25	24	23	22	21	20	19	18	17	16	15	14											
14	28	27	26	25	24	23	22	21	20	19	18	17	16	15										
15	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16									
16	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17								
17	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18							
18	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19						
19	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20					
20	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21				
21	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22			
22	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23		
23	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	
24	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25

Table 8: Values of $m_{ee}(2, 2, h, l)$.

Tables 8 through 14 represent the values of $m_{ee}(2, n, h, l)$ for $n = 2, \ldots, 8$, $h = 1, \ldots, 24$, $l = 0, \ldots, h-1$. The values were calculated by solving ILPMEE.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	3																							
2	6	3																						
3	9	6	4																					
4	12	9	6	5																				
5	15	12	9	7	6																			
6	18	15	12	9	8	7																		
7	21	18	15	12	10	9	8																	
8	24	21	18	15	12	11	10	9																
9	27	24	21	18	15	13	12	11	10															
10	30	27	24	21	18	15	14	13	12	11														
11	33	30	27	24	21	18	16	15	14	13	12													
12	36	33	30	27	24	21	18	17	16	15	14	13												
13	39	36	33	30	27	24	21	19	18	17	16	15	14											
14	42	39	36	33	30	27	24	21	20	19	18	17	16	15										
15	45	42	39	36	33	30	27	24	22	21	20	19	18	17	16									
16	48	45	42	39	36	33	30	27	24	23	22	21	20	19	18	17								
17	51	48	45	42	39	36	33	30	27	25	24	23	22	21	20	19	18							
18	54	51	48	45	42	39	36	33	30	27	26	25	24	23	22	21	20	19						
19	57	54	51	48	45	42	39	36	33	30	28	27	26	25	24	23	22	21	20					
20	60	57	54	51	48	45	42	39	36	33	30	29	28	27	26	25	24	23	22	21				
21	63	60	57	54	51	48	45	42	39	36	33	31	30	29	28	27	26	25	24	23	22			
22	66	63	60	57	54	51	48	45	42	39	36	33	32	31	30	29	28	27	26	25	24	23		
23	69	66	63	60	57	54	51	48	45	42	39	36	34	33	32	31	30	29	28	27	26	25	24	
24	72	69	66	63	60	57	54	51	48	45	42	39	36	35	34	33	32	31	30	29	28	27	26	25

Table 9: Values of $m_{ee}(2,3,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	4																							
2	8	5																						
3	12	6	4																					
4	16	10	7	5																				
5	20	14	10	8	6																			
6	24	18	12	10	8	7																		
7	28	22	16	13	11	9	8																	
8	32	26	20	16	14	12	10	9																
9	36	30	24	18	16	14	12	11	10															
10	40	34	28	22	19	17	15	13	12	11														
11	44	38	32	26	22	20	18	16	14	13	12													
12	48	42	36	30	24	22	20	18	16	15	14	13												
13	52	46	40	34	28	25	23	21	19	17	16	15	14											
14	56	50	44	38	32	28	26	24	22	20	18	17	16	15										
15	60	54	48	42	36	30	28	26	24	22	20	19	18	17	16									
16	64	58	52	46	40	34	31	29	27	25	23	21	20	19	18	17								
17	68	62	56	50	44	38	34	32	30	28	26	24	22	21	20	19	18							
18	72	66	60	54	48	42	36	34	32	30	28	26	24	23	22	21	20	19						
19	76	70	64	58	52	46	40	37	35	33	31	29	27	25	24	23	22	21	20					
20	80	74	68	62	56	50	44	40	38	36	34	32	30	28	26	25	24	23	22	21				
21	84	78	72	66	60	54	48	42	40	38	36	34	32	30	28	27	26	25	24	23	22			
22	88	82	76	70	64	58	52	46	43	41	39	37	35	33	31	29	28	27	26	25	24	23		
23	92	86	80	74	68	62	56	50	46	44	42	40	38	36	34	32	30	29	28	27	26	25	24	
24	96	90	84	78	72	66	60	54	48	46	44	42	40	38	36	34	32	31	30	29	28	27	26	25

Table 10: Values of $m_{ee}(2,4,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	5																							
2	10	6																						
3	15	7	7																					
4	20	10	7	5																				
5	25	15	10	8	6																			
6	30	20	14	10	9	7																		
7	35	25	17	14	11	10	8																	
8	40	30	20	17	14	12	10	9																
9	45	35	25	20	17	15	13	11	10															
10	50	40	30	24	20	17	15	14	12	11														
11	55	45	35	27	24	20	18	16	15	13	12													
12	60	50	40	30	27	24	20	19	17	15	14	13												
13	65	55	45	35	30	27	24	21	20	18	16	15	14											
14	70	60	50	40	34	30	27	24	22	20	19	17	16	15										
15	75	65	55	45	37	34	30	27	25	23	21	20	18	17	16									
16	80	70	60	50	40	37	34	30	27	25	24	22	20	19	18	17								
17	85	75	65	55	45	40	37	34	30	28	26	25	23	21	20	19	18							
18	90	80	70	60	50	44	40	37	34	30	29	27	25	24	22	21	20	19						
19	95	85	75	65	55	47	44	40	37	34	31	30	28	26	25	23	22	21	20					
20	100	90	80	70	60	50	47	44	40	37	34	32	30	29	27	25	24	23	22	21				
21	105	95	85	75	65	55	50	47	44	40	37	35	33	31	30	28	26	25	24	23	22			
22	110	100	90	80	70	60	54	50	47	44	40	37	35	34	32	30	29	27	26	25	24	23		
23	115	105	95	85	75	65	57	54	50	47	44	40	38	36	35	33	31	30	28	27	26	25	24	
24	120	110	100	90	80	70	60	57	54	50	47	44	40	39	37	35	34	32	30	29	28	27	26	25

Table 11: Values of $m_{ee}(2, 5, h, l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	6																							
2	12	7																						
3	18	7	8																					
4	24	11	7	9																				
5	30	15	10	8	6																			
6	36	21	14	11	9	7																		
7	42	27	18	14	11	10	8																	
8	48	33	22	17	14	12	11	9																
9	54	39	26	21	17	15	13	12	10															
10	60	45	30	25	20	18	15	14	12	11														
11	66	51	36	29	24	21	18	16	15	13	12													
12	72	57	42	33	28	24	21	19	17	16	14	13												
13	78	63	48	37	32	27	24	22	20	18	17	15	14											
14	84	69	54	41	36	31	27	25	22	21	19	18	16	15										
15	90	75	60	45	40	35	30	28	25	23	21	20	18	17	16									
16	96	81	66	51	44	39	34	31	28	26	24	22	21	19	18	17								
17	102	87	72	57	48	43	38	34	31	29	26	25	23	22	20	19	18							
18	108	93	78	63	52	47	42	37	34	32	29	27	26	24	23	21	20	19						
19	114	99	84	69	56	51	46	41	37	35	32	30	28	27	25	24	22	21	20					
20	120	105	90	75	60	55	50	45	40	38	35	33	30	29	27	26	24	23	22	21				
21	126	111	96	81	66	59	54	49	44	41	38	36	33	31	30	28	27	25	24	23	22			
22	132	117	102	87	72	63	58	53	48	44	41	39	36	34	32	31	29	28	26	25	24	23		
23	138	123	108	93	78	67	62	57	52	47	44	42	39	37	35	33	32	30	29	27	26	25	24	
24	144	129	114	99	84	71	66	61	56	51	47	45	42	40	37	36	34	33	31	30	28	27	26	25

Table 12: Values of $m_{ee}(2, 6, h, l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	7																							
2	14	8																						
3	21	7	9																					
4	28	12	7	10																				
5	35	17	11	8	11																			
6	42	21	14	11	9	7																		
7	49	28	19	14	12	10	8																	
8	56	35	24	18	14	12	11	9																
9	63	42	28	21	18	15	13	12	10															
10	70	49	33	26	21	18	16	14	13	11														
11	77	56	38	31	25	21	19	17	15	14	12													
12	84	63	42	35	28	25	21	19	17	16	14	13												
13	91	70	49	40	33	28	25	22	20	18	17	15	14											
14	98	77	56	45	38	32	28	25	23	21	19	18	16	15										
15	105	84	63	49	42	35	32	28	26	24	21	20	19	17	16									
16	112	91	70	54	47	40	35	32	28	26	24	22	21	20	18	17								
17	119	98	77	59	52	45	39	35	32	29	27	25	23	22	21	19	18							
18	126	105	84	63	56	49	42	39	35	32	30	28	26	24	23	21	20	19						
19	133	112	91	70	61	54	47	42	39	35	33	31	28	27	25	24	22	21	20					
20	140	119	98	77	66	59	52	46	42	39	35	33	31	29	28	26	25	23	22	21				
21	147	126	105	84	70	63	56	49	46	42	39	36	34	32	30	28	27	26	24	23	22			
22	154	133	112	91	75	68	61	54	49	46	42	39	37	35	33	31	29	28	27	25	24	23		
23	161	140	119	98	80	73	66	59	53	49	46	42	40	38	35	33	32	30	29	28	26	25	24	
24	168	147	126	105	84	77	70	63	56	53	49	46	42	40	38	36	34	33	31	30	28	27	26	25

Table 13: Values of $m_{ee}(2,7,h,l)$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	8																							
2	16	9																						
3	24	17	10																					
4	32	12	18	11																				
5	40	18	11	19	12																			
6	48	23	15	11	20	13																		
7	56	28	19	14	12	21	8																	
8	64	36	24	18	15	12	16	9																
9	72	44	30	22	18	15	13	17	10															
10	80	52	35	26	22	18	16	14	18	11														
11	88	60	40	31	26	22	19	17	15	19	12													
12	96	68	46	36	30	25	22	19	18	16	20	13												
13	104	76	51	42	34	29	25	22	20	18	17	21	14											
14	112	84	56	47	38	33	28	26	23	21	19	18	16	15										
15	120	92	64	52	43	37	32	29	26	24	22	20	19	17	16									
16	128	100	72	58	48	41	36	32	29	26	24	23	21	20	18	17								
17	136	108	80	63	54	45	40	36	32	30	27	25	23	22	21	19	18							
18	144	116	88	68	59	50	44	40	36	33	30	28	26	24	23	22	20	19						
19	152	124	96	74	64	55	48	44	39	36	33	31	29	27	25	24	23	21	20					
20	160	132	104	79	70	60	52	48	43	39	36	34	31	30	28	26	25	24	22	21				
21	168	140	112	84	75	66	56	52	47	42	40	37	34	32	30	28	27	26	24	23	22			
22	176	148	120	92	80	71	62	56	51	46	43	40	37	35	33	31	29	28	27	25	24	23		
23	184	156	128	100	86	76	67	60	55	50	46	43	40	38	36	34	32	30	29	28	26	25	24	
24	192	164	136	108	91	82	72	64	59	54	50	46	44	41	38	36	35	33	31	30	29	27	26	25

Table 14: Values of $m_{ee}(2,8,h,l)$.

B An Analysis of $f^*(x)$

B.1 Continuity and Differentiability

Recall that we defined the function $f^*(x)$ as follows:

$$f^*(x) = m\big(\lceil x\rceil(n-\lceil x\rceil)(x-\lfloor x\rfloor) + \lfloor x\rfloor(n-\lfloor x\rfloor)(1-x+\lfloor x\rfloor)\big).$$

Since m is just a constant term, it will not affect our analysis, and we can assume $m = 1$. We note that with this simplification, $f^*(x)$ is equivalent to the following:

$$f^*(x) = x(n-x) + \tau^2 - \tau,$$

where $\tau(x) = x - \lfloor x\rfloor$. Let $g(\tau(x)) = \tau(x)^2 - \tau(x)$, and consider g over the interval $x \in [c, c+1]$, $c \in \mathbb{Z}$. First, $g(\tau(c)) = g(0) = 0$. For $x \in (c, c+1)$, $g(\tau(x))$ is certainly continuous. Finally,

$$\begin{aligned} \lim_{x\to c+1} g(\tau(x)) &= 0 \\ &= g(\tau(c+1)) \end{aligned}$$

so g is continuous at $x = c+1$. Since g is periodic in x with period 1, g is continuous.

Now we examine the question of differentiability. Let $x \in (c, c+1)$, $c \in \mathbb{Z}$. Then $\tau(x) = x - c$, and

$$\begin{aligned} f^*(x) &= x(n-x) + (x-c)^2 - (x-c) \\ &= xn - x^2 + x^2 - 2cx + c^2 - x + c \\ &= x(n-2c-1) + c^2 + c \Rightarrow \\ f^{*'}(x) &= n - 2c - 1. \end{aligned}$$

Thus,

$$f^{*'}(x) \begin{cases} > 0, & c < \frac{n-1}{2} \\ = 0, & c = \frac{n-1}{2} \\ < 0, & c > \frac{n-1}{2}. \end{cases}$$

If n is odd, then

$$\begin{aligned} c &< \frac{n-1}{2} \Rightarrow \\ \lfloor x\rfloor &< \frac{n-1}{2} \Rightarrow \\ x &< \frac{n-1}{2} \Rightarrow \\ x &< \lfloor \frac{n}{2} \rfloor. \end{aligned}$$

If n is even, then

$$\begin{aligned} c &< \frac{n-1}{2} \Rightarrow \\ \lfloor x\rfloor &< \frac{n-1}{2} \Rightarrow \\ x &< \frac{n}{2} \Rightarrow \\ x &< \lfloor \frac{n}{2} \rfloor. \end{aligned}$$

By a similar analysis, we can show that

$$c = \frac{n-1}{2} \Rightarrow x \in [\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil).$$

Note that if n is even, this represents the empty set. Also,

$$c > \frac{n-1}{2} \Rightarrow x \geq \lceil \frac{n}{2} \rceil.$$

So we have

$$f^{*'}(x) \begin{cases} > 0, & x < \lfloor \frac{n}{2} \rfloor \\ = 0, & x \in [\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil) \\ < 0, & x \geq \lceil \frac{n}{2} \rceil. \end{cases}$$

The continuity of $f^*(x)$, which follows directly from the continuity of $g(\tau(x))$, shows that the behaviour of $f^*(x)$ at integral points must be the same as at non-integral points. In other words, $f^*(x)$ is increasing for $x \in [0, \lfloor n/2 \rfloor)$, constant for $x \in [\lfloor n/2 \rfloor, \lceil n/2 \rceil)$ and decreasing for $x \in [\lceil n/2 \rceil, n]$.

B.2 Plots of $f^*(x)$

The following plots were generated using MAPLE. They show $f^*(x)$ for various values of m and n. Note the correspondence with the above analysis.

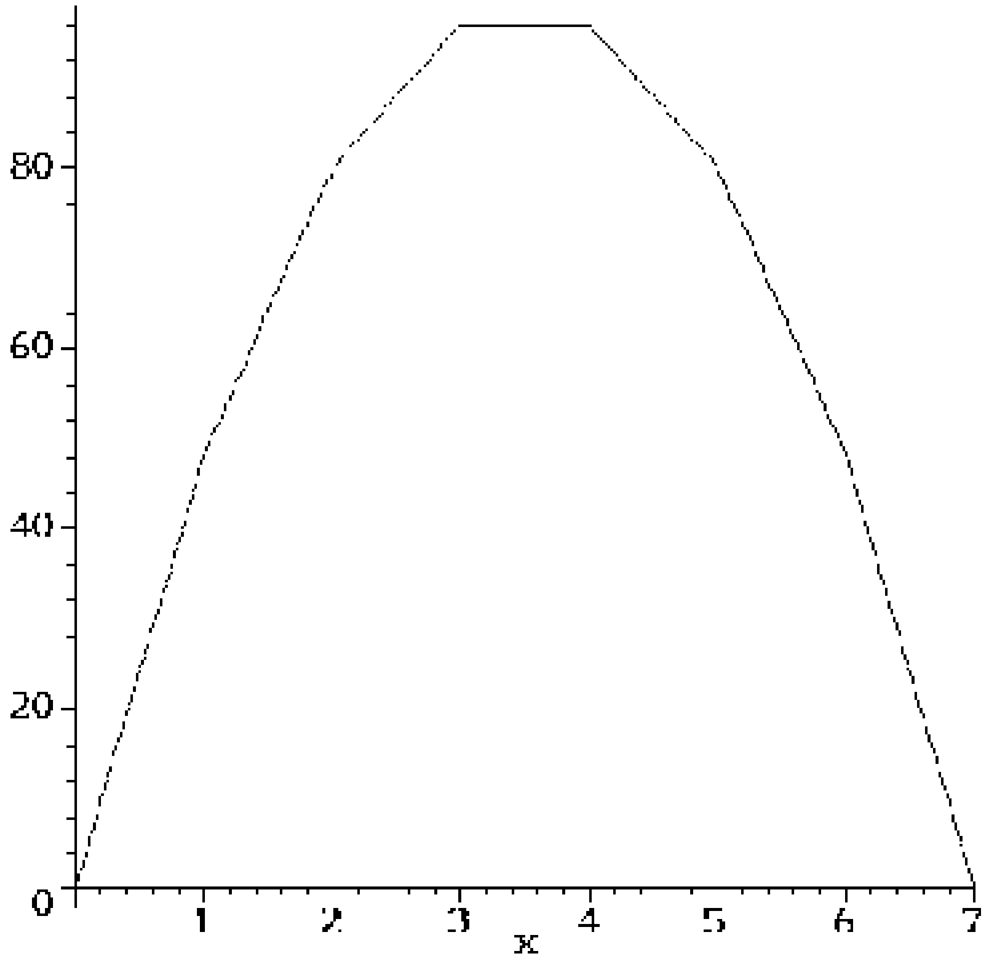

Figure 5: $f^*(x)$ for $m = 8$, $n = 7$.

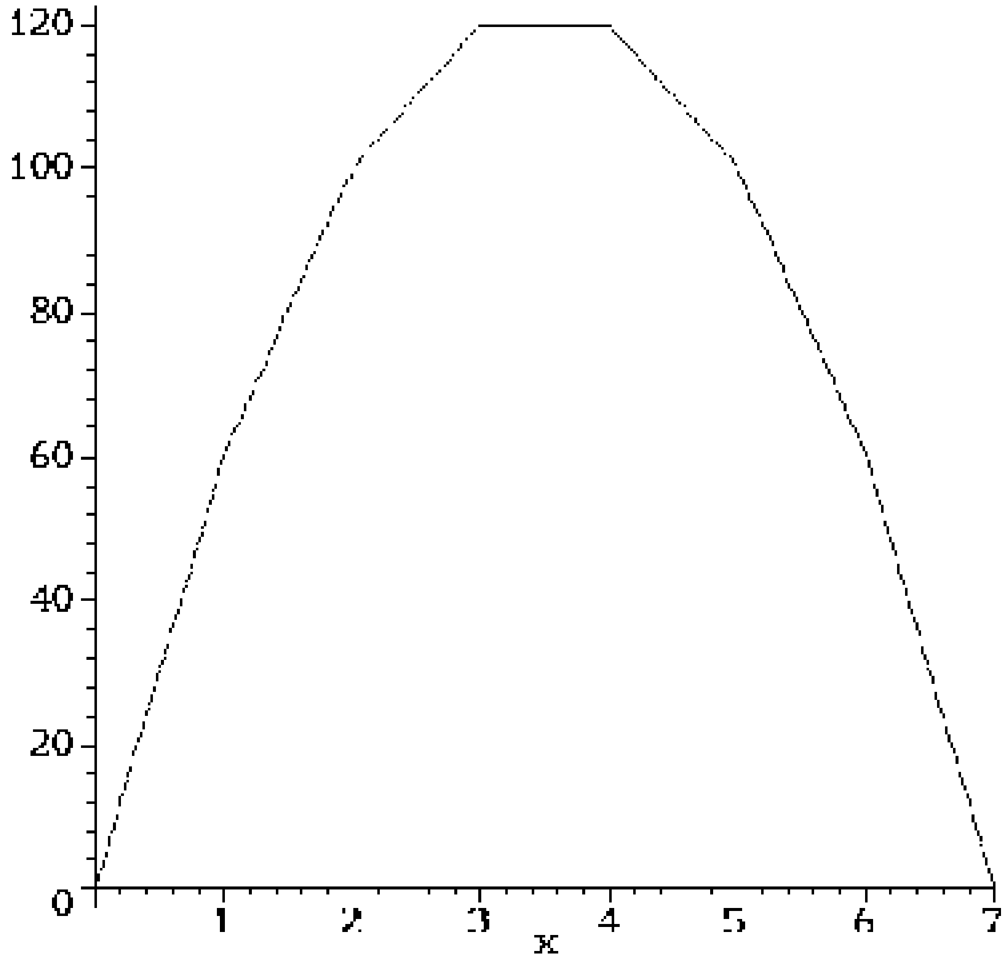

Figure 6: $f^*(x)$ for $m = 10$, $n = 7$.

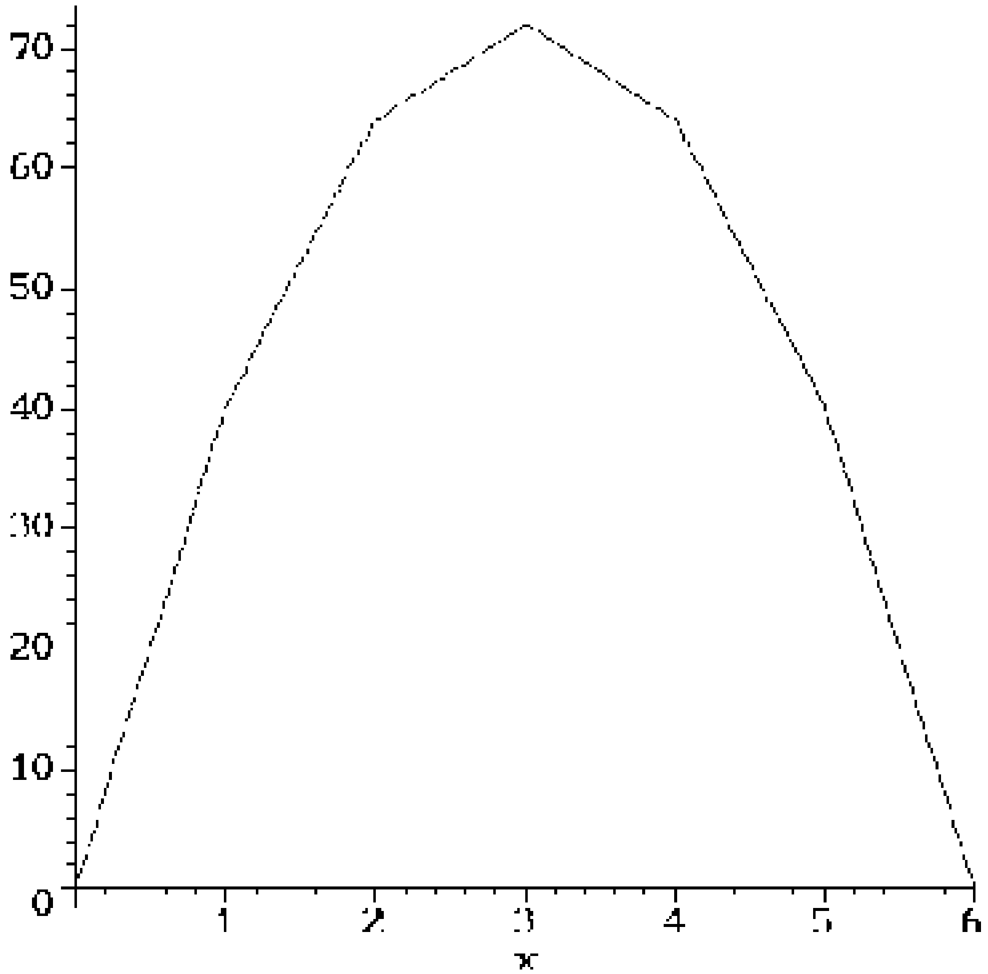

Figure 7: $f^*(x)$ for $m = 8$, $n = 6$.