AUTOSTEREOGRAMS—ANALYSIS AND ALGORITHMS

By

LAU Shek Kwan Mark

A Thesis

Submitted in Partial Fulfillment of the Requirements

of the Degree of Master of Philosophy in

Mechanical and Automation Engineering

June 2001

Acknowledgment

I would like to express my thanks to my supervisor Professor C. P. Kwong for his kindness and patient guidance. I am grateful for his great passion in research and education, which deeply impress me.

I am thankful for the joyful experiences with my colleagues in this department: Wai-keung Fung, Winston Sun, Samuel Au, Alan Lam, Cedric Law, Hok-chun Lo, Eric Wong and He Yong. Thanks are due to their friendships and caring.

I would like to dedicate this thesis to my parents, brothers and Ying for their unreserved support and love.

Abstract

Three-dimensional depth information of surfaces can be encoded in two-dimensional images called autostereograms. They appear to be some scrambled patterns, which are meaningless to the viewers. But, if they are viewed with a special technique, the three-dimensional effects of the surfaces can be perceived.

Visual distortions of the original surfaces result from the viewing positions and eye separations of viewers, which vary in real situations. If the distortions are too serious, the viewers may feel uncomfortable to recognize the original surfaces. We show that such distortions can be controlled if the parameters are appropriately chosen. In this thesis, the relations between parameter selections and the visual distortions, namely vertical and lateral distortion are studied.

One of the shortcomings of the existing algorithms is the inability of exact reconstructions of the original surfaces from autostereograms. This is due to echoes, which are surface segments produced by falsely matched positions on autostereograms. Echoes are visually unpleasant fragments distracting the viewers. We categorize echoes into Type 1 and Type 2, and the respective conditions for echo avoidance are derived. Then, a new autostereogram generation algorithm incorporating these conditions is proposed.

We have observed that applications of autostereograms are limited to entertainments and commercial advertising. Echoes and other problems related to the

inability of exact reconstructions seem to be the bottlenecks of their prospects. By imposing restrictions on the generations, we show that any original surface can be exactly reconstructed. This opens up applications in which exact reconstructions are needed. Then, we demonstrate how autostereograms can be applied in cryptography. Indeed, under some conditions, we show that autostereogram is a variation of a classical cryptosystem—Substitution Cipher.

摘 要

單一隨機立體圖（以下簡稱立體圖）是一種二維圖像，它們包含了三維表面圖的深度訊息。對觀者來說，它們是混雜而毫無意義的圖樣，不過，假如利用某種特別的技巧來觀看它們的話，觀者便會感到立體效果。

在實際情況下，每一個觀者的眼距和位置都未必相同，這就造成原來表面圖視覺上的失真。我們把視覺失真分類爲直向失真和橫向失真。假如失真的情況過於嚴重，觀者在辨認原來表面圖時便會感到困難。我們研究那些視覺失真和各參數之間的關係，並示範以合適的參數來控制失真的程度。

現有的立體圖算法的其中一個弊病就是未能把原來表面圖從立體圖完整地還原，這是由於「迴音」而導致的，而迴音則是位置的錯誤配對所形成的還原表面圖分節。另外，它對觀者造成視覺上的騷擾和誤導。我們將迴音分爲甲型和乙型，並推論出避免它們出現的條件。之後，我們建議一個加入了這些條件的新的立體圖算法。

我們留意到立體圖現時的應用只限於娛樂及商業推廣上。迴音及有關未能完整地還原的問題似乎成爲立體圖發展的主要障礙。我們證明在某些條件下，任何原來表面圖都可以完整地還原。這個結果可以替立體圖開拓一些需要完整地還原資料的應用。最後，我們示範立體圖如何應用在加密技術上。而事實上，在某些條件下，立體圖是經典的加密技術「替代密碼」（Substitution Cipher）的變種。

Contents

Chapter 1

Introduction

Known as the "magic eyes", the strange and self-repeating patterns are guaranteed to attract the crowds. These patterns seem to be meaningless at the first sight. But if they are viewed correctly using the special technique, impressive stereo effects jump out of the planes of the papers. Excitements can be rewarding when the stereo effects can be perceived.

The images containing these patterns are known as *autostereograms*. Not surprisingly, autostereogram is a fantastic media for commercial advertising. Indeed, it became a cult art which has swept all over Japan, Europe and America, where an enormous amount of books and posters printed with autostereograms have been published.

Nevertheless, the existing computer algorithms to generate autostereograms are rather ad hoc, in a sense that the selections of parameters are try-and-error-based. The relations between the parameters and the visual effects have not been systematically studied. In addition, the causes of the problem of *echo* have not been revealed. Echoes may result in visual artifacts on the perceived surfaces, which are distracting and misleading. So that the original surfaces can be hardly recognized from the perceived surfaces, especially when they are not familiar to the viewers. Further-

more, in the presences of echo, the original surfaces can be uniquely reconstructed by neither the human visual systems nor computer algorithms, which definitively limits the prospects of autostereogram for other applications.

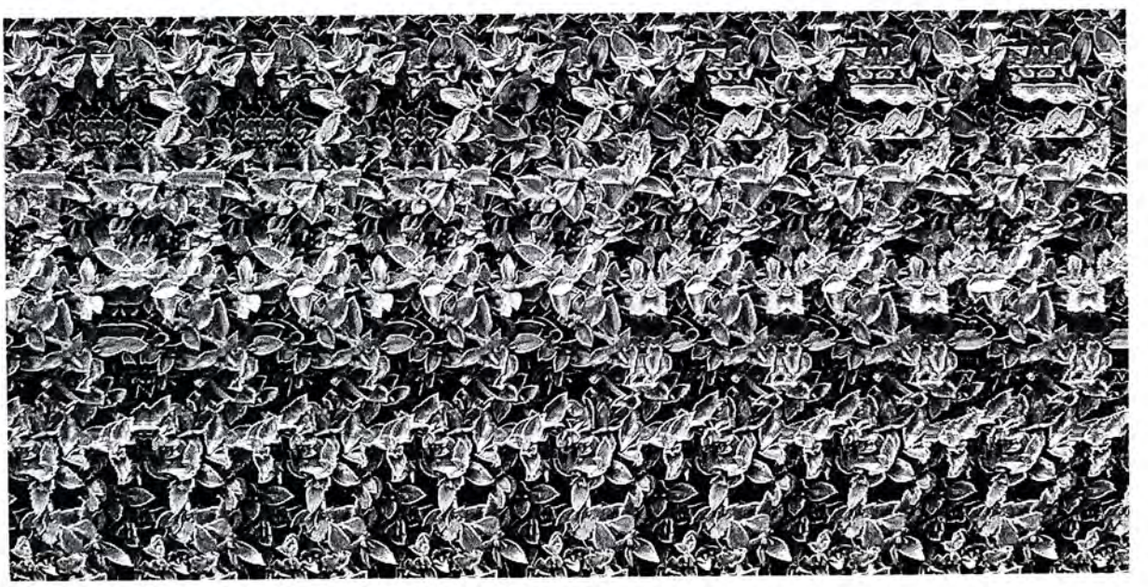
We observed that the parameter adjustments for visually pleasant autostereograms result in complications of autostereogram constructions. Autostereograms have been using only for entertainments so far. We believe that their prospects will be widened, if the problem of echo can be solved. These are the incentives for the study of autostereograms.

1.1 Historical Background

Random-dot-stereogram (stereogram pair) was first introduced by Julesz [2] to study human visual perceptions of depth in the early 60's. Stereogram pairs are pairs of computer-generated images which are capable to encode depth information of surfaces. They appear completely random when viewed monocularly. But if they are viewed binocularly such that the corresponding picture elements (pixels) on the left and the right images of the stereogram pairs are matched, the surfaces will be reconstructed in human brains by the visual systems, which give the viewers three-dimensional effects. These surfaces are usually taken from some simple and familiar real-world-objects which can be easily recognized by the viewers. For instance, the surfaces of pyramids were used by Julesz [2]; and the corresponding stereogram pair is shown in Fig. 1.1(a).

In fact, all knowledge except binocular parallax of the surfaces are devoid in stereogram pairs. Hence, control experiments on human stereopsis can be conducted using stereogram pairs. For this reason, they have been used extensively in studying the computational theory of human stereopsis processes. Numerous of stereo

(a)



(b)

Figure 1.1: (a) The stereogram pair used by Julesz; (b) an example of autostereogram (encoding two rabbits) for entertainments.

matching algorithms incorporating the computational structure of human stereopsis have been proposed, [5] for instances, which may hopefully yield insights into the brain mechanism of depth perceptions. The stereo matching capabilities of these algorithms are often exhibited on stereogram pairs.

A new type of random-dot-stereogram was invented by Tyler and Clark [3] in the early 90's. They combined stereogram pairs into single images called *single-image random-dot-stereograms* or, more widely known as *autostereograms*. By modulating the horizontally repeated patterns with the variations of height[1] of surfaces, they showed that it is possible to demonstrate the same stereo effects of stereogram pairs on single computer-generated images. To perceive surfaces from autostereograms, one may need a "special technique" to relax his or her eyes to create a suitable focal point, such that the corresponding pixels are matched to give the stereo effects. One of the distinguish features of autostereograms is that they appear as nothing more than repeated random patterns printed on single sheets of paper. Furthermore, they require no special viewing apparatus, such as the mirror stereoscopes, the lens stereoscopes and various prismatic stereoscopes. Nonetheless, the viewers may take few minutes to practice before perceiving the surfaces.

Nevertheless, the excitements are rewarding when the stereo effects "jump" out. Therefore, autostereograms have been a cult art, and an enormous amount of autostereograms have been published mainly for entertainments and commercial uses. An example of autostereograms for entertainments is shown in Fig. 1.1(b). Since early 90's, the autostereogram boom had started. Numerous books containing autostereograms were published, and several companies were founded to produce autostereogram relating products.

In 1994, another computer algorithm to generate autostereograms was proposed by Thimbleby *et al.* [10]. Being incorporated into their algorithm, a technique called *Hidden Surface Removal* was proposed to reduce echoes. Echoes are reconstructed surface segments from autostereograms, which do not belong to the original sur-

[1] "Height" refers to the measurement of vertical distance. We use "depth" for the physical characteristics of being deep.

faces. They appear as narrow fragments "floating" in the space, which can be very distracting and misleading to the viewers. Compared with the algorithm developed by Tyles and Clark, Thimbleby's algorithm produces autostereograms having better quality in terms of the reconstructed surfaces. This is due to the considerable reductions of echoes. The algorithm has been well adopted to produce autostereograms. We will introduce Thimbleby's algorithm and HSR in next section.

1.2 Introduction to Autostereograms

1.2.1 Geometrical Model

We consider the ray diagram shown in Fig. 1.2. It shows the top view when a surface denoted by $S(x, y)$ is being viewed through an image plane (y-axis is hidden). The image plane, being parallel to the plane containing eyes L and R, is a transparent plane with zero thickness. We will see that the image plane indeed is an autostereogram. According to the ray diagram, light rays CAL and CBR are emitted from light source C. Then, they intercept with the image plane at A and B, and enter the eyes L and R, respectively.

Suppose the colors of A and B are set to be the same, and the surface is now removed so that it is invisible to the viewer. If the viewer converges his or her eyes to create a focal point at the position where C was located, the perception of the depth of C can nevertheless be obtained. In other words, if the colors of the light sources on the image plane are appropriately allocated according to the heights of the surface, the viewer's brain can be "faked" to produce an illusion of the surface. Then, it is not difficult to see that the image plane indeed is an autostereogram.

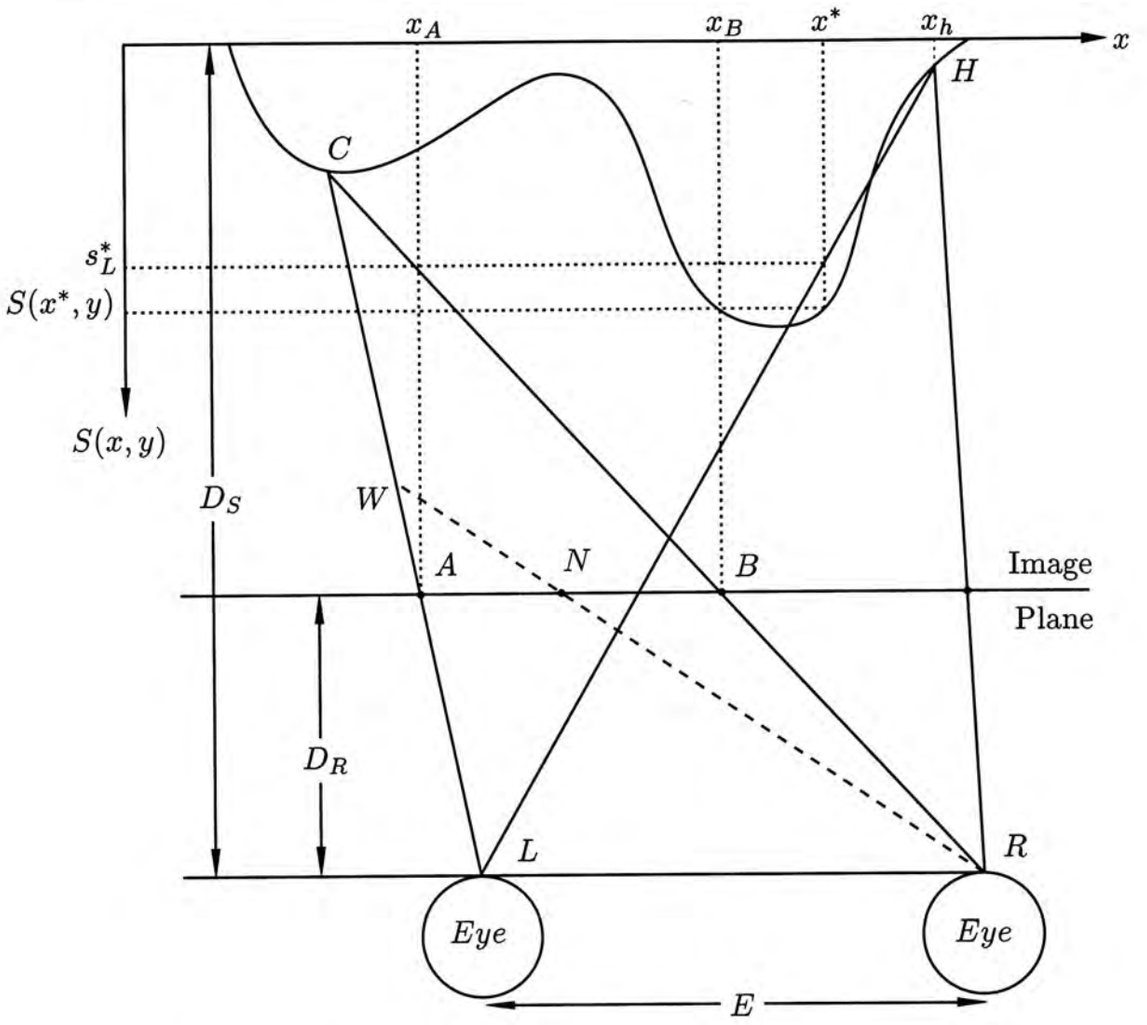


Figure 1.2: The geometrical model of autostereograms.

1.2.2 IS-separation

It has been noted that the crucial element to encode the depth of C is the distance between A and B. This quantity is called *image stereo separation* (IS-separation) [10] owing to its dependence on stereo disparity. Let $s = S(x, y)$ be the heights attained at points (x, y) of the surface, then IS-separation is obviously a function of s. We denote this function by $\sigma_I(s)$. In fact, IS-separation $\sigma_I(s)$ can be expressed explicitly by using the geometry of the ray diagram. As shown in Fig. 1.2, E is the distance of eye separation, and D_S and D_R are the perpendicular distances from the eyes to the bottom ($s = 0$) of the surface and the image plane, respectively. Without

loss of generality, by similar triangles $\triangle LCR$ and $\triangle ACB$, IS-separation can be expressed [10] as

$$\sigma_I(s) = E - \frac{ED_R}{D_S - s}. \tag{1.1}$$

for all attainable heights s of surface $S(x, y)$.

In general, autostereograms are generated by mapping each point, say (x_0, y), on the original surface into two points (x_1, y) and $(x_1 - \sigma_I(S(x_0, y)), y)$ on the same row of the autostereogram. The mapping is applied recursively for all positions (x, y). Indeed, the mapping rules vary depending upon the generation schemes. But the autostereograms generated by such schemes are in common in a sense that the depth information of surfaces is encoded in the "horizontal correlations", instead of the values of some particular points on the autostereograms. Therefore, autostereograms take the appearances of repeated patterns which, in some senses, are independent of the original surfaces. Thus, these patterns can be arbitrary that the creators of autostereograms can use any pattern for their purposes. For instance, autostereograms with patterns of dinosaurs are often used for commercial advertising. We called these patterns *pre-defined patterns* which play an important role in autostereogram analysis. This will be evident in the following chapters.

1.2.3 The Hidden Surfaces

Sometimes, due to the transitions of surfaces (say, from a point of greater height to a point of smaller height), surface segments in the foregrounds may obscure one eye's views of more distant points. For such situation, we say that the obscured points are "hidden" to the viewers. For instance, as shown in Fig. 1.2, point H is hidden to the viewer since the view of eye L is obscured. By the geometry of the ray diagram, H is hidden if there exists a point (x^*, y) such that $S(x^*, y) \geq s_L^*$, where s_L^* is the height attained by the light ray which is emitted from H and enters eye L.

According to [10], s_L^* is obtained from

$$s_L^* = \frac{2\,(x_h - x^*)\,(D_S - S(x_h, y))}{E} + S(x_h, y) \tag{1.2}$$

for $x_h > x^*$. But if $x_h < x^*$, we have

$$s_L^* = \frac{2\,(x^* - x_h)\,(D_S - S(x_h, y))}{E} + S(x_h, y). \tag{1.3}$$

Hence, it can be concluded that any point (x, y) on a surface $S(x, y)$ is hidden to the viewers if and only if there exists a point (x^*, y) such that

$$S(x^*, y) \geq \frac{2\,|x^* - x|\,(D_S - S(x, y))}{E} + S(x, y). \tag{1.4}$$

We will see that Eq. 1.4 is a crucial condition for Hidden Surface Removal.

1.2.4 False Target and Echo

As mentioned, to perceive surfaces from autostereograms, one needs a "special technique" to relax the eyes to create a suitable focal point. Then, the features on the left eye and the right eye images are matched in human brain to create the stereo effect. This is called correspondence matching, which is a classical problem in stereopsis. In terms of computer algorithm, this problem is however very difficult. The difficulties are due to the fact that there can be more than two pixels satisfying the matching criterion such as pixel color. In this case, since no further information about the surface is available with autostereograms such as geometrical information, we have no way to figure out the falsely matched pixels surely. Hence, the original surfaces cannot be reconstructed exactly. This problem is called *false target.*

False target is depicted in Fig. 1.2. Suppose A, B and N are somehow set to have the same color. If N and A are falsely matched, then not only the depth of C, but the depth of W which does not belong to the original surface is also perceptible

to the viewers. However, we cannot tell whether C or W is at the original surface if no additional information is available.

The problem of false target worsens when the pre-defined patterns "repeat too frequently" in the horizontal direction. In the extreme case, the pre-defined patterns consist of only black and white pixels. It was Marr and Poggio [4] who partially overcame the problem using a cooperative algorithm with constraints derived from the properties of physical surfaces taken from the real world. In fact, false targets can nevertheless be avoided if the pre-defined patterns are chosen in such a way that they do not repeat in the horizontal direction, or "horizontally uncorrelated". With the knowledge of the ranges of IS-separations, the surface reconstruction processes can be greatly simplified.

However, in some cases, we still cannot guarantee the uniqueness of the reconstructed surfaces even though the pre-defined patterns have been appropriately chosen. This is due to both insufficient lengths of the periods of the repeating pixels on autostereograms and the depth transitions on the original surfaces. Under such circumstances, the autostereogram generation algorithm generate ambiguities which interfere the matching processes. As the result, the reconstructed surfaces will have multiple values at some positions. The surface segments resulted from these ambiguities are called *echoes*. To the viewers, echoes appear as distracting, repeating and narrow fragments "floating" in the space. They may interfere the eye convergences such that the viewers feel difficult to make suitable focal points. Similar to the case of false target, the original surfaces cannot reconstructed exactly due to the non-uniqueness of the reconstructed surfaces, which indeed limits their applications.

Echoes are briefly described in [10] together with an echo reduction method called

Hidden Surface Removal (HSR), which will be introduced in the next section. The authors reported that the autostereogram generation algorithm incorporating HSR produces clearer autostereograms, from which echoes are unlikely to be noticeable.

1.3 The Autostereogram Generation Algorithm

The autostereogram generation algorithm developed by Thimbleby *et. al.* [10] is well known for the ease of implementation and the incorporation of HSR. For the sake of completeness for the literature review, the algorithm as well as HSR will be introduced in this section.

In the authors' original paper, the algorithm was presented using a program listing. To get the algorithm clearer, we reproduce the algorithm using flowcharts as shown in Fig. 1.3 and Fig. 1.4. In addition, the syntax of Matlab is adopted in these flowcharts, which hopefully would be more friendly for algorithmic descriptions. In these flow charts, the rectangles having double-lined sides are used for subroutines which are presented in Fig. 1.4. The subroutine names, arguments and return variables are indicated in the terminators of the subroutines, which take the shape of elongated circles. In the following verbal descriptions of the algorithm, the names of program functions, variables and arrays are in typewriter fonts.

Before introducing the algorithm, we first describe the purposes of array `same`. In the authors' terminology, "pixel constraints" are specified by `same`. In fact, each entry of `same` is the x-coordinate at which the pixel is constrained to have the same color as the current pixel. This idea can be illustrated using an example. As shown in Fig. 1.2, A and B are constrained to have the same color to encode the depth of C. Suppose x_A and x_B ($x_A < x_B$) are, respectively, specified by the variables `xA` and `xB`, then we will have `same(xA,y)=xB` such that the color of x_A is

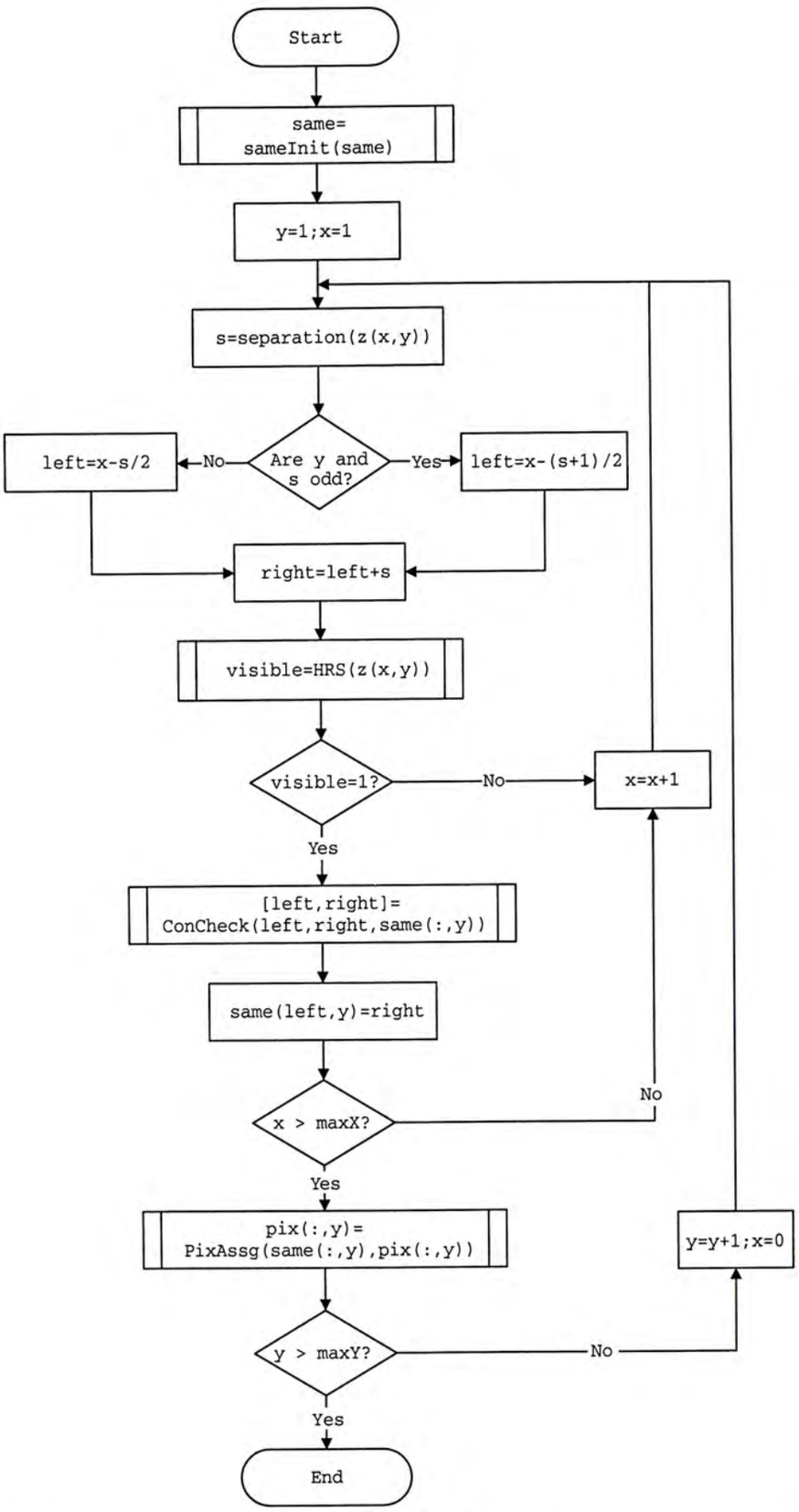


Figure 1.3: The main routine of Thimbleby's algorithm.

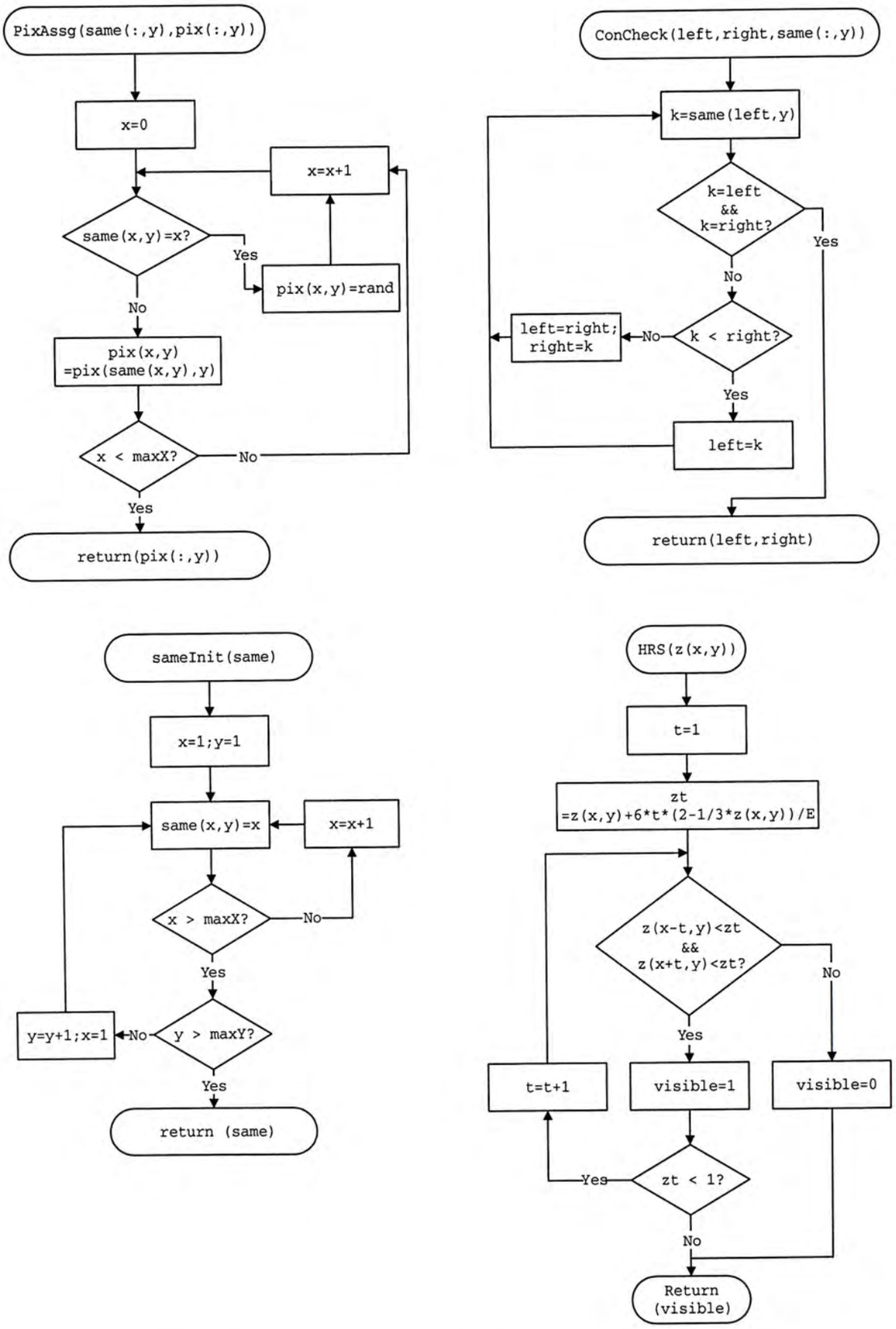


Figure 1.4: The subroutines of Thimbleby's algorithm.

constrained to be the same as that of x_B. Note that this array assignment is true only if subroutine `PixAssg` processes *from right to left*, which means that the color of x_B is assigned before the assignment of x_A. If the direction is reversed, we should have `same(xB,y)=xA`.

We now start introducing the algorithm. We refer to the main routine in Fig. 1.3. The program begins with `y=1` and `x=1`. It executes each row independently and terminates when `y>maxY` and `x>maxX`. But before the program actually starts, variables and arrays are initialized (which are not shown in the flowchart). Note that array `same` is initialized separately using subroutine `sameInit`. Taking `same` as the argument, `sameInit` set `same(x,y)=x` for each `x` and `y`, which means that the pixel constraint is the x-coordinate of itself.

After the initializations, the IS-separation $\sigma_I(S(x,y))$ (specified by array `s`) at (x,y) is computed by `separation` where

```
separation(z(x,y))=E*(1-z(x,y)/3)/(2-z(x,y)/3).
```

In fact, `separation` is implanted from Eq. 1.1 with $S(x,y) = \dfrac{z(x,y)D_R}{3}$ and $D_S = 2D_R$, where $z \in [0,1]$ specified by array `z` is used originally in their paper representing the height of surfaces. To encode height $S(x,y)$ in the autostereogram, two corresponding pixels separated by $\sigma_I(S(x,y))$ are set to have the same color. The x-coordinates of these pixels are recorded in variables `left` and `right`, where `left=x-s/2` and `right=x+left`. In case `s` is odd, one is added to `s` before dividing by two to avoid the truncations.

Afterwards, the subroutine `HSR` for Hidden Surface Removal is executed. Under this technique, no constraint should be imposed on the pixels which are hidden to the viewers. Eliminations of such redundant constraints reduce false matches of pixels, which result in reductions of echoes. To figure out the hidden pixels, every pixel

(x, y) is checked against the condition stated in Eq. 1.4. If there exists (x^*, y) such that Eq. 1.4 is satisfied, then (x, y) is hidden to the viewers. Thus, the execution on (x, y) will be bypassed so that no constraint will be imposed, and `same` remains unchanged. To search for pixel (x^*, y), the pixel on the left and the right of (x, y) have to be checked against Eq. 1.4. In the program, this task is accomplished by checking

```
z(x-t,y)<zt && z(x+t,y)<zt,
```

where `zt` is computed by

```
zt=z(x,y)+6*t*(2-1/3*z(x,y))/E
```

which is implanted from Eq. 1.4 with $t = |x^* - x|$, $D_S = 2D_R$ and $S(x, y) = \frac{z(x, y)D_R}{3}$. If `z(x-t,y)<zt && z(x+t,y)<zt` is true, we set `visible=1` for the fact that (x, y) is not hidden (or visible), otherwise set `visible=0`.

If pixel (x, y) is visible, i.e. `visible=1`, the fact that pixel at `left` is constrained to be the same as the pixel at `right` is recorded. This is accomplished by setting `same(left,y)=right`. Nevertheless, the pixel at `left` may have been already constrained to other pixels, i.e. `same(left,y)` neither equals `left` nor `right`. To ensure that the action do not overwrite any constraint in `same(left,y)`, subroutine `ConCheck` is executed before the statement `same(left)=right` to follow the constraints (using a dummy variable `k`) rightwards to find a pixel that is not otherwise constrained. If the constraints are settled, then they are recorded by `same(left)=right`.

Finally, the values of the pixels on the autostereograms are assigned by the subroutine `PixAssg`. The subroutine processes from right to left since the constraints of the pixels refer to the corresponding pixels on the right. If it is found that no constraint was imposed on the pixel at (x, y), i.e., `same(x,y)=x`, then a random

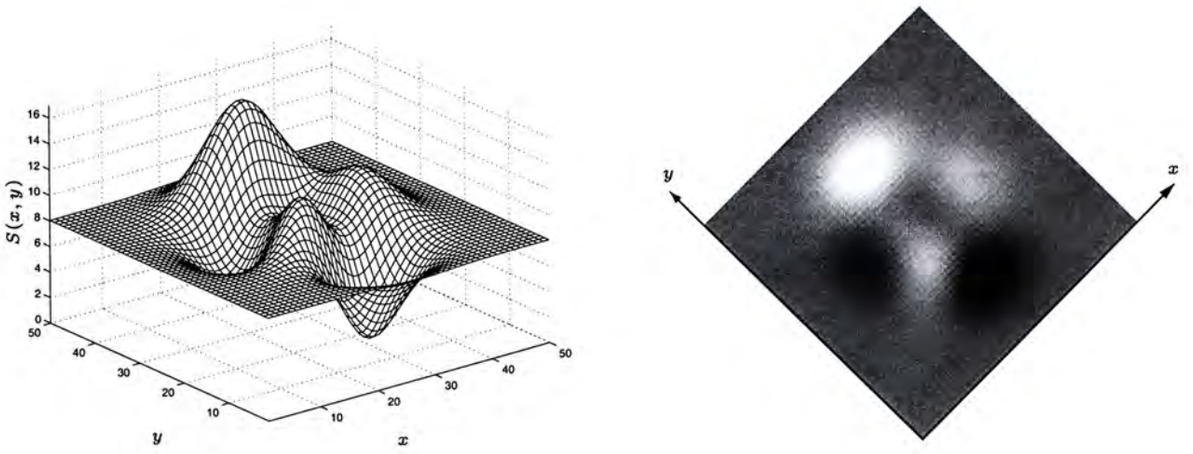
number is picked for `pix(x,y)` by the random number generator `rand`. Otherwise, the value of `pix(x,y)` is assigned by `pix(x,y)=pix(same(x,y),y)`.

1.4 Further Applications of Autostereograms

We have observed that applications of autostereograms are limited to entertainments. Besides the excitements behind the stereo effects, the distinguish mechanism for surface encoding in autostereograms inspired us to conjecture that they can be useful in other applications, including image coding and cryptography.

It is not difficult to see that the collection of points of a surface can be considered as a gray image, in which the gray intensity is somehow directly related to the height of the corresponding surface. One of the typical examples is geographical map, in which the areas of different altitudes are painted in different colors. Usually, light colors are used for high mountains while dark colors are used for low lands. In terms of gray images such as shown in Fig. 1.5, it is natural to assume that the maximum height attained by a surface corresponds to the maximum gray intensity (white) while zero height corresponds to the minimum gray intensity (black), then the values in between are linearly interpolated.

In fact, from the mathematical point of view, surfaces and images are nothing more that two-dimensional functions. Therefore, autostereograms can be applied as a novel image encoding method. Moreover, data are encoded in autostereogram by using the correlations of pixels, so that the appearances of autostereograms are arbitrary and independent of the data contents in some senses. Thus, the proposed image encoding method will be differentiated from other existing methods, such as orthogonal transforms or fractal transforms. When "random dots" are used as the pre-defined patterns, the resulting autostereogram seems to be a piece of completely



(a) (b)

Figure 1.5: Representing (a) a surface $S(x, y)$ as (b) an image.

scrambled data. Thus, it appear to be meaningless to the observers.

The above observations and the content independent feature lead to a conjecture that autostereograms can be applied to *cryptography*. To draw a conclusion for this conjecture, two questions are posted:

1. Does autostereogram fits the mathematical structure of cryptosystems?

2. If the answer for the first question is "yes", is it feasible to use autostereogram as a cryptosystem?

The most crucial requirement to fit the mathematical structure of cryptosystems is that the encoding function (known as encryption function) is a one-to-one map such that its inverse exists. If we consider autostereogram generation as the encoding function of surfaces, the inverse exists if and only if the original surfaces can be reconstructed exactly from autostereograms. But exact reconstruction would be nevertheless a challenging problem because of echoes and the shortcomings of the existing autostereogram generation algorithms.

Furthermore, it is undesirable if the cryptosystem is not secure enough to protect the secrete messages from breaking by the enemies. In practical, the secure system has to be efficient in terms of encryption/decryption computations and key managements. A cryptosystem would be feasible if it is secure and efficient in that sense. Otherwise, it would has limited uses, especially in commercial applications. The limitations of the cryptosystems using autostereograms will be discussed in Chapter 4.

1.5 Organization of Thesis

The organization of the thesis is as follows. In Chapter 2, we study various aspects of autostereograms. The chapter begins with a formal definition of original surface. Then, expression of IS-separation is derived. To gain insights into IS-separation, we propose a new method to generate autostereograms, which is more general than the conventional method. After the general expression is obtained, we consider two particular cases, which are deduced to Thimbleby's expression and our proposed expression. We argue that his expression has shortcoming in computer generations due to the truncation problem, which lead to inability of exact reconstructions. On the other hand, we show that the problem can be successfully avoided using our proposed expression. We introduce autostereograms by giving explicit formulae for their generations and surface reconstructions. Afterwards, we study the visual distortions of the original surfaces by the perceived surfaces. We classify them as vertical distortions and lateral distortions. If fact, they behave differently with respect to Thimbleby's and our proposed expression. We derive explicit equations for such distortions. Finally, discrete autostereograms are considered. We extend the generation and reconstruction formulae to discrete cases and prove that usage

of Thimbleby's expression results in inability for exact reconstructions. We therefore conclude that it is may not be desirable for computer generations. Finally, the Chapter ends with a new autostereogram generation algorithm, in which our proposed expression for IS-separations is incorporated.

In Chapter 3, we resolve the problem of echo. The chapter begins with a derivation of the necessary and sufficient condition for the existence of echo. Based on this condition, we observed that echoes result from two situations, namely insufficient lengths of the periods of repeating patterns and overlapping of copying steps. Echoes resulted from these situations are referred as Type 1 and Type 2 echoes, respectively. Then, we study them individually, and propose echo avoidance methods, which are illustrated with examples. We show that these techniques avoid echo successfully. However, there are drawbacks from such avoidance. We find that avoidance of Type 2 echoes leads to losses of depth information of the original surfaces. The lost information is recoverable only for some surfaces which have some special "shapes". Therefore exact reconstructions are still not guaranteed for any surface. In the last section, we derive some conditions to further restrict the generations of autostereograms such that *any* encoded surfaces can be exactly reconstructed. This opens up new applications to autostereograms such as image coding.

In Chapter 4, we show how autostereograms are applied to cryptography. The chapter starts with a brief introduction to cryptography including the general structure, mathematical structure and a classical cryptosystem know as Substitution Cipher. Then, we consider autostereogram generation as an encoding function of surfaces. We show that this function indeed is one-to-one with unique inverse, which satisfy the crucial requirement of cryptosystems. Furthermore, we show that autostereogram is a variation of Substitution Cipher. Nevertheless, we propose sev-

eral drawbacks for applying autostereograms in cryptography. Finally, we conclude our works in Chapter 5.

Chapter 2

Analysis of Autostereograms

In this chapter, we study various aspects of autostereograms, including IS-separations, autostereogram generations, surface reconstructions, visual distortions and the discrete counterpart of autostereograms.

First of all, we give a formal definition of original surface. Afterwards, a more general expression for IS-separation is derived. In the derivation, we use a new configuration to generate autostereograms, which gives insights into the problem. We compare our proposed expression to the well-known expression developed by Thimbleby *et. al.* [10], we argue that the proposed expression may not desirable when autostereograms are generated using computers due to truncation. We will show that various problems result from such truncations, including the inability of exact reconstructions. On the other hand, our proposed expression can successfully avoid the truncations, which leads to the simplicity of autostereogram generations as well as echo avoidance.

Nevertheless, we discover that whichever expression has been used, in most of the cases, the perceived surfaces distort the original surfaces in both vertical (height) and lateral directions. These distortions are in fact due to the viewing positions and eye separations of the viewers. If the distortions are serious, they may create

visual artifacts, so that the viewers may feel uncomfortable to recognize the original surfaces. We show that such distortions can be controlled to an acceptable level if the parameters are appropriately chosen. The relations between parameter selections and the corresponding visual distortions are studied.

Finally, explicit formulations for both autostereogram generations and surface reconstructions are given. Then, these formulae are extended to their discrete counterparts for computer generations. Then, we propose a new generation algorithm in which our proposed expression for IS-separation is incorporated.

2.1 IS-separation

Let $\mathbf{C} = \mathbf{X} \times \mathbf{Y}$ be a subset of the Euclidean plane $\mathbf{R}^2$, where $\mathbf{X} = \{x \in \mathbf{R} \mid 1 \leq x \leq x_s\}$ and $\mathbf{Y} = \{y \in \mathbf{R} \mid 1 \leq y \leq y_s\}$ for some finite numbers x_s and y_s. Hence, the *distance* between any two points on $\mathbf{C}$ is the Euclidean metric. We define a *original surface* $S(x, y)$ to be a non-negative real-valued function[1] defined on $\mathbf{C}$. The range of original surface $S(x, y)$ is the set $\mathcal{S} = \{s \in \mathbf{R} \mid 0 \leq s \leq \bar{s}\}$ where $\bar{s}$ denotes the upper bound of function $S(x, y)$. Most often, bound $\bar{s}$ is the height at the image plane for the fact that the original surface do not intercept with the image plane. Then the bound is

$$\bar{s} = D_S - D_R, \tag{2.1}$$

where D_S and D_R are, respectively, the perpendicular distances from the plane containing the eyes to the bottom of the surface and the image plane. Unless specified, we adopt this bound throughout this thesis.

It has been shown in Section 1.2 that the expression for IS-separations can be

[1]For the functions, say f, appearing throughout this thesis, the notation $f(x, y)$ refer either to the function f or to the value of the function f at a specific (x, y). The distinction between these two will be evident from the context.

easily deduced from the geometry of the ray diagram such as shown in Fig. 1.2. IS-separation is indeed the crucial element in many aspects, such as autostereogram analysis and echo avoidance. To get insights into the problem, we introduce a new configuration to generate autostereograms, which is more general compared with the configuration in Fig. 1.2.

As shown in Fig. 2.1, a configuration is set to generate autostereograms, which is similar to that in Fig 1.2, except that optical device G is placed between original surface $S(x, y)$ and the image plane. We assume that some kinds of optical processes are carried out by G to bend the paths of the light rays passing through. For instance, the light rays emitted from D are bent by G, in such a way that the bent light rays give D an apparent image at C which is right below D with height $g(s)$. The distance between A and B is the IS-separation of C for the height $g(s)$.

In general, let $g : \mathcal{S} \to (-\infty, \bar{s}\,]$ be a strictly monotonic increasing (s.m.i.) mapping which maps the height s to the apparent height $g(s)$. Using such configuration, the apparent surfaces produced by G are encoded in the autostereograms, instead of original surfaces $S(x, y)$. Since we allow $g(s)$ to have negative values so that the apparent surfaces may extend from $\bar{s}$ to minus infinity[2].

We denote the IS-separations for the apparent heights $g(s)$ by σ_g, where the subscript g indicates the transformation g. By using the property of similar triangles $\triangle ABC$ and $\triangle LRC$, without loss of generality, $\sigma_g(s)$ can be expressed as

$$\sigma_g(s) = E - \frac{ED_R}{D_S - g(s)} \tag{2.2}$$

for all height $s \in \mathcal{S}$. We define $\Sigma(g)$ be a set of composite functions σ_g for all s.m.i. g. The elements in $\Sigma(g)$ are called IS-separations.

[2]In fact, the viewers do not notify the difference between negative height and positive height. Negative heights are for mathematical interpretations.

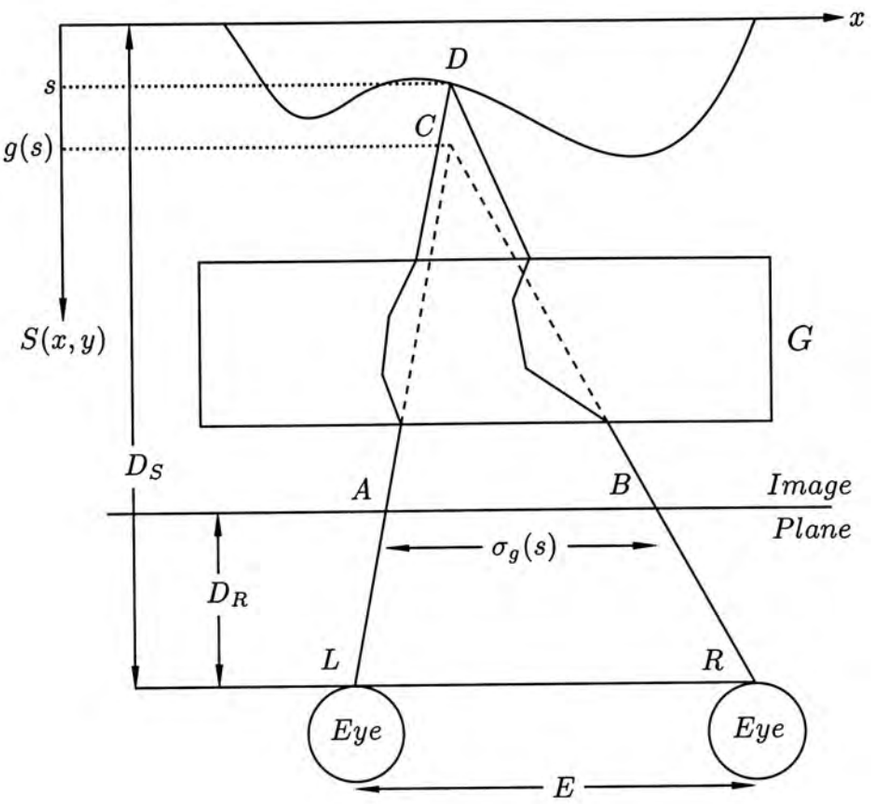


Figure 2.1: Generating autostereograms with optical device G.

In particular, suppose device G does not bend the light rays passing through, or device G does not exist. Therefore, g is an identity mapping, i.e. $g(s) = s$. Let $\sigma_I \in \Sigma(g)$ be the IS-separation for such g, it can be expressed as

$$\sigma_I(s) = E - \frac{ED_R}{D_S - s} \tag{2.3}$$

for all $s \in \mathcal{S}$. In this case, the same expression as Eq. 1.1 is arrived. The subscript I indicates that g is an identity mapping.

In fact, IS-separation σ_I is well adopted to generate autostereograms. One of the possible reasons is that the original surfaces are encoded "directly", without being transformed by G, in the autostereograms. But, we will show that the perceived surfaces from such autostereograms also suffer from visual distortions. Furthermore, IS-separation σ_I has shortcomings for computer generations owing to the truncation problem. Since autostereograms generated in computers are two-dimensional

discrete sequences defined on all integer values of the horizontal and vertical coordinates, the distance between any two defined points on the surface is an integer. Obviously, the fraction in $\sigma_I(s)$ may introduce decimals. So that, when autostereograms are generated by computers, IS-separations $\sigma_I(s)$ have to be truncated to integers for some s. However, such truncations induce various problems, including the inability for exact reconstructions and difficulties in echo analysis.

Prior to the generations of autostereograms in computers, the amplitudes of the original surfaces are quantized to integers. Thus, truncations can nevertheless be avoided if IS-separation σ_g are integers for all integer heights s. This can be accomplished by choosing a proper transformation g. We propose that one of the possible transformations is

$$g(s) = D_S - \frac{D_R \bar{s}}{s}. \tag{2.4}$$

Let $\sigma \in \Sigma(g)$ be the IS-separation for such g. By Eq. 2.2, it can be expressed as

$$\sigma(s) = E - \frac{sE}{\bar{s}} \tag{2.5}$$

for all $s \in \mathcal{S}$. Clearly, IS-separations $\sigma(s)$ are integers for all s if the values of E and $\bar{s}$ are chosen such that E is a multiple of $\bar{s}$. Note that the subscript is omitted in this case.

In some cases, the perceived surfaces distort the original surfaces in vertical and lateral directions. In fact, the usages of IS-separation σ contribute partially to the problem, since the encoded is not the original surfaces, but merely its "approximations". In addition, the distortions are caused by the positions and eye separations of the viewers, which may be different from the respective values of D_R and E assumed in the formulations of IS-separations. Unfortunately, the influences of IS-separation σ and viewers' positions are coupled so that they cannot be studied individually.

It has been mentioned that IS-separation σ is advantageous over σ_I in terms of

exact reconstructions. But the visual distortions of the original surfaces contributed by IS-separation σ are also worth investigating. This issue will be discussed in Section 2.4.

2.2 Autostereogram Generations

The vital operation in autostereogram generations is *copying step* by which value of one position on the autostereogram is *copied* to another position. We define the verb "copy" as follows: given two functions, say f and f^*, defined on the same domain; if the value of $f(x_1, y_1)$ is copied to $f^*(x_2, y_2)$, then the value of f^* at (x_2, y_2) is set to be the same as that of f at (x_1, y_1), i.e. $f^*(x_2, y_2) = f(x_1, y_1)$. The action of copying at one position is called a *copying step*, and a series of copying steps is called *copying procedure*.

Another recipe of autostereogram generations is *pre-defined pattern* which is a function $\Pi(x, y)$ defined on $\mathbf{C}$. Informally speaking, the pre-defined patterns give the appearances of autostereograms, which appear repeatedly along the horizontal direction. The periods of the repetitions are modulated by the variations of height of the original surfaces. In fact, the depth information of the original surfaces are encoded in such horizontal correlations rather than the values of some particular points on the autostereograms. Therefore, function $\Pi(x, y)$ is indeed arbitrary. The "appearances" of the pre-defined patterns can be chosen depending upon the applications and the creators' will[3]. Nevertheless, we will see that a restriction have to be imposed on the pre-defined patterns in order to avoid problems related to exact reconstructions.

Here we are ready to define autostereogram. An autostereogram $R(x, y)$ is a

[3]We have observed that the pre-defined patterns affect the visual quality of the perceived surfaces. Some types of patterns seem to result in better quality than others for the same surface and parameters D_S, D_R and E.

function defined on **C**, which is determined by the following formula

$$R(x,y) = \begin{cases} \Pi(x,y), & 1 \le x \le \sigma_0 \\ R(x - \sigma_g(S(x,y)), y), & \sigma_0 < x \le x_s \end{cases} \tag{2.6}$$

where $\sigma_0 = \sigma_g(0)$ for all IS-separations $\sigma_g \in \Sigma(g)$ and positions $(x,y) \in \mathbf{C}$. As seen from Eq. 2.6, autostereograms $R(x,y)$ are in fact pre-defined patterns $\Pi(x,y)$ when $1 \le x \le \sigma_0$. According to IS-separation σ_g, the values of $R(x,y)$ on the other positions $(\sigma_0 < x \le x_s)$ are copied from their preceding positions $(x - \sigma_g(S(x,y)), y)$. Consequently, the values of pre-defined patterns $\Pi(x,y)$ are copied recursively to the succeeding positions on the right. These recursive copying steps proceed along the horizontal direction until $x = x_s$. Therefore, the pre-defined patterns appear repeatedly along the horizontal direction.

Notice that autostereograms $R(x,y)$ in Eq. 2.6 are generated row-wise, which are independent of the y-axis. The depth information is encoded by the horizontal correlations, so that stereo effects are achievable only when the autostereograms are upright, or upside down. Another type of autostereograms called *orthogonal autostereograms* are described in [3]. Orthogonal autostereograms are autostereograms in which surfaces are encoded using both horizontal and vertical correlations. Therefore, additional stereo effects can be perceived with a 90 degree or 270 degree rotation. They either presenting the same surface or two separate surfaces in all viewing directions. However, as shown by the authors, paradigms for orthogonal autostereograms are rather restricted.

2.3 Surface Reconstructions

The human visual systems provide us with an excellent correspondence matching algorithm for stereopsis. Computer algorithms incorporating the computational

structures of human stereopsis have been proposed [5], which may hopefully yield insights into the brain mechanism underlying depth perceptions. But the problem of false target seems to be the bottle-necks for stereopsis using machines. In this study, we do not attempt to resolve false targets. Instead, we are rather focusing on the problem of echo, which can be analyzed using a simple surface reconstruction procedure.

Since we do not attempt to resolve false target, the pre-defined patterns are assumed to be *horizontally uncorrelated*, namely

$$\Pi(x_1, y_1) \neq \Pi(x_2, y_1) \tag{2.7}$$

for all $1 \leq x_1, x_2 \leq \sigma_0$ and $x_1 \neq x_2$. Under this assumption, false targets are devoid so that any false match solely results in echo. The matching criteria is simple without considering false targets. We claim that (x_1, y_1) and $(x_1 - d, y_1)$ are the corresponding positions if and only if they are identical, i.e.

$$R(x_1, y_1) = R(x_1 - d, y_1) \tag{2.8}$$

for some $1 \leq d \leq \sigma_0$. Since transformation g is s.m.i., then by Eq. 2.2, σ_g is strictly monotonic decreasing (s.m.d.) that its inverse σ_g^{-1} exists. In this case, the *reconstructed surfaces* $\tilde{S}(x, y)$ are determined using

$$\tilde{S}(x,y) = \begin{cases} 0, & 1 \leq x \leq \sigma_0 \\ \sigma_g^{-1}(d), & \sigma_0 < x \leq x_s,\ R(x,y) = R(x-d,y) \\ \text{undefined}, & \text{otherwise} \end{cases} \tag{2.9}$$

for all IS-separations $\sigma_g \in \Sigma(g)$, positions $(x, y) \in \mathbf{C}$ and $1 \leq d \leq \sigma_0$. This expression is given under the assumption that pre-defined pattern $\Pi(x, y)$ is horizontally uncorrelated. However, this rarely happens in real world situations. Therefore,

Eq. 2.9 accounts for neither the actual stereo matching algorithm in the human visual system, nor stereopsis.

Reconstructed surfaces $\tilde{S}(x, y)$ are obtained by searching for the corresponding positions. This can be accomplished by comparing $R(x, y)$ and $R(x - d, y)$. If correspondence is established between $R(x, y)$ and $R(x - d, y)$ such that $R(x, y) = R(x - d, y)$ for some values of $1 \leq d \leq \sigma_0$, reconstructed height $\tilde{S}(x, y)$ is determined by $\sigma_g^{-1}(d)$. If no correspondence is found, $\tilde{S}(x, y)$ is undefined.

Recall that pre-defined patterns $\Pi(x, y)$ are assigned to $R(x, y)$ for $1 \leq x \leq \sigma_0$. Since they are horizontally uncorrelated, no corresponding positions can be found in this region. Consequently, reconstructed surfaces $\tilde{S}(x, y)$ are undefined for $1 \leq x \leq \sigma_0$, so that the depth information of original surfaces $S(x, y)$ in this region is lost in the reconstruction processes. To avoid such losses of depth information, original surfaces $S(x, y)$ should not carry any depth information for $1 \leq x \leq \sigma_0$. Instead, they are set to zeroes (or any arbitrary convenient value), i.e. $S(x, y) = 0$. The surfaces actually start when $x > \sigma_0$. Accordingly, the reconstructed surface are $\tilde{S}(x, y) = 0$ for $1 \leq x \leq \sigma_0$.

The reconstructed surface $\tilde{S}(x, y)$ from Eq. 2.9 may have multiple values at some positions in the presence of echoes. This is because there may be more than one values of d satisfying the criterion $R(x, y) = R(x - d, y)$. Without additional information, we have no way to figure out the original surfaces from the reconstructed surfaces.

2.4 Visual Distortions

It does not make any sense to restrict the viewers of autostereograms to some specific positions. Either, we would not assume that the eye separations of the viewers are

all identical. In fact, these factors vary in the real situations. Thus, the assumptions on the values of the parameters D_S, D_R and E do not reflect the real situations, since the viewing positions and eye separations of the viewers vary. So that the perceived surfaces differ from the original surfaces in many ways. For instance, it was reported in [10] that the heights of perceived surfaces are not linearly portrayed as that in the original surfaces.

In that cases, we say that the original surfaces are *distorted* by the perceived surfaces. We observed that the distortions can be categorized into two types, namely vertical distortion and lateral distortion. In fact, the extent of the distortions depends on height s and position (x, y) of original surfaces $S(x, y)$. More precisely, denoted by $S_{p,g}(u, v)$, *perceived surface* is defined as

$$S_{p,g}(u, v) = v_g(S(\eta_g(x), y)) \tag{2.10}$$

for all g and positions $(x, y) \in \mathbf{C}$, where functions v_g and η_g account for the vertical distortions and lateral distortions, respectively. Note that perceived surfaces $S_{p,g}(u, v)$ do not distort the original surfaces in y direction since autostereograms are independent of that. Therefore, we have $v = y$.

In this section, we first give a general expression of v_g for all s.m.i. g. We noted that the perceived surface vertically distorts the original surfaces in two ways, namely *change of depth field* and *non-linear distortion*. We study them individually with respect to IS-separations σ and σ_I. Finally, η_g for the vertical distortions is derived. In fact, the formulation of η_g varies depending upon the generation scheme. Nevertheless, the derivation is demonstrated using our proposed scheme.

We have to mention that we do not have a subjective measurement on the visual effects resulted from such distortions since it involves the psychological aspects which are to board to be included in this thesis. Therefore, the distortions are studied on

a functional level.

2.4.1 Problem Model For Vertical Distortions

We model the situation with references to Fig. 2.2. Let the perpendicular distance from the viewer to the autostereogram be $D_{R,v}$, where $D_{R,v} = aD_R$ for some fixed real factors $a \geq 0$. Accordingly, the perpendicular distance from the viewer to the bottom of original surface $S(x, y)$ is $D_{S,v} = \bar{s} + D_R$.

Suppose the viewer has eye separation[4] E_v. We reasonably assume that E_v is fairly larger that E. For any pair of corresponding positions, if E_v is smaller than the distance between them, as shown in Fig. 2.3, the viewer is unable to make a suitable focal point behind ("wall-eyed" or "boss-eyed") the autostereogram. Nevertheless, the viewer is still able to focus on the points in front ("cross-eyed") of the autostereogram, but such kind of convergence creates surface with the heights inverted. For instance, the lowest point on the original surface is perceived as the highest point. We therefore exclude this case since it is undesirable. Furthermore, we believe that the smaller E is, to a certain extent, the easier the eye muscles can be controlled to converge for a fixed E_v. It is because the separations of the corresponding positions are directly proportional to E. For that reasons, we assume that E_v is greater that E such that $E_v = eE > E$ for some positive real factors $e > 1$. For instance, $e = 2$ was suggested in [9].

Suppose (x, y) and $(x - \sigma(S(x)), y)$ are the corresponding positions to give *perceived height* $v_g(s)$. By geometry of the ray diagram, it can be expressed as

$$v_g(s) = D_{S,v} - \frac{E_v D_{R,v}}{E_v - \sigma_g(s)} \tag{2.11}$$

for all IS-separations $\sigma_g \in \Sigma(g)$ and heights $s \in \mathcal{S}$. By substituting the parameters

[4]The pupils of an adult human's eye are about 7 centimeters apart[7].

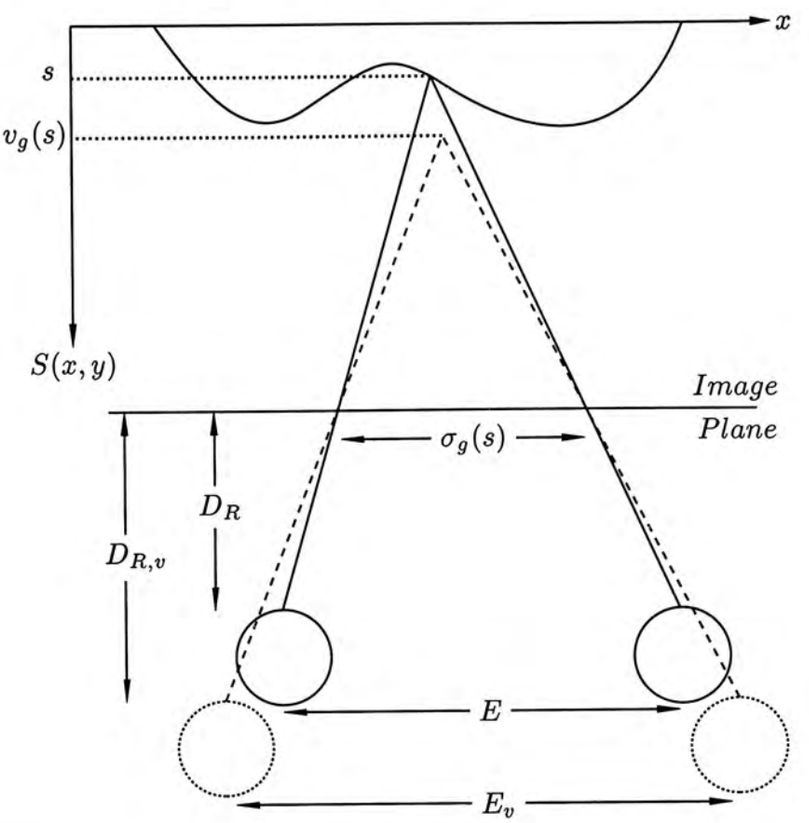


Figure 2.2: Viewing an autostereogram with eye separation E_v and distance $D_{R,v}$.

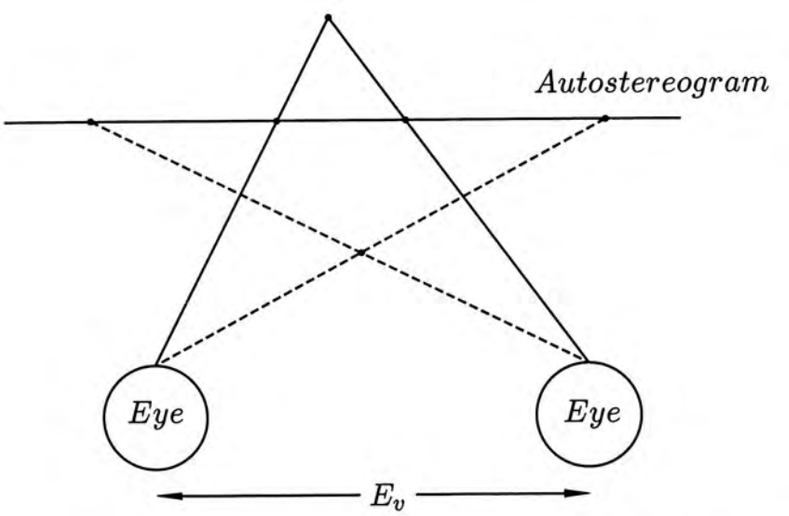


Figure 2.3: Viewing an autostereogram with wall-eyed (solid lines) and cross-eyed (dashed lines).

$E_v = eE$, $D_{R,v} = aD_R$ and $D_{S,v} = \bar{s} + D_{R,v}$, we conclude that

$$v_g(s) = \bar{s} + aD_R - \frac{eaED_R}{eE - \sigma_g(s)} \tag{2.12}$$

for all $\sigma_g \in \Sigma(g)$ and $s \in \mathcal{S}$.

Let us consider two particular cases. Firstly, let $v(s)$ be the perceived heights when IS-separation σ is used to generate autostereograms. By Eq. 2.12 and Eq. 2.5, perceived heights $v(s)$ are

$$v(s) = \bar{s} + aD_R - \frac{eaED_R}{eE - \sigma(s)} \tag{2.13}$$

$$= \bar{s} + aD_R - \frac{eaD_R}{e - 1 + s\bar{s}^{-1}} \tag{2.14}$$

for all heights $s \in \mathcal{S}$. On the other hand, let v_I be the perceived height when IS-separation σ_I is used. By Eq. 2.12 and Eq. 2.3, perceived heights $v_I(s)$ are

$$v_I(s) = \bar{s} + aD_R - \frac{eaED_R}{eE - \sigma_I(s)} \tag{2.15}$$

$$= \bar{s} + aD_R - \frac{eaD_R}{e - 1 + D_R(D_S - s)^{-1}} \tag{2.16}$$

for all heights $s \in \mathcal{S}$.

Before moving to the analysis of those equations, we first show an example in Fig. 2.4 to get some ideas on the distortions. In this example, we let the parameters $E = 1.5\text{cm}$, $D_R = 2.5\text{cm}$, $D_S = 3.75\text{cm}$. It is assumed that the viewer is $D_{R,v} = 60\text{cm}$ away from the autostereogram, and the eye separation is $E_v = 6.75\text{cm}$. Hence, the factors are $a = 24$ and $e = 4.5$. In the figure, perceived heights $v(s)$ and $v_I(s)$ are plotted against s. The hidden straight lines are the contrasts to the non-linearly distorted curves $v(s)$ and $v_g(s)$. We see that the perceived height $v(s)$ and $v_I(s)$ are portrayed non-linearly. Moreover, their interceptions $v(0)$ and $v_I(0)$ of the vertical axis are non-zero such that the depth fields of the perceived surfaces, in both cases, are "deeper" than that of the original surfaces. The former distortion is referred as *non-linear distortion*, while the later is referred as *change of depth field.*

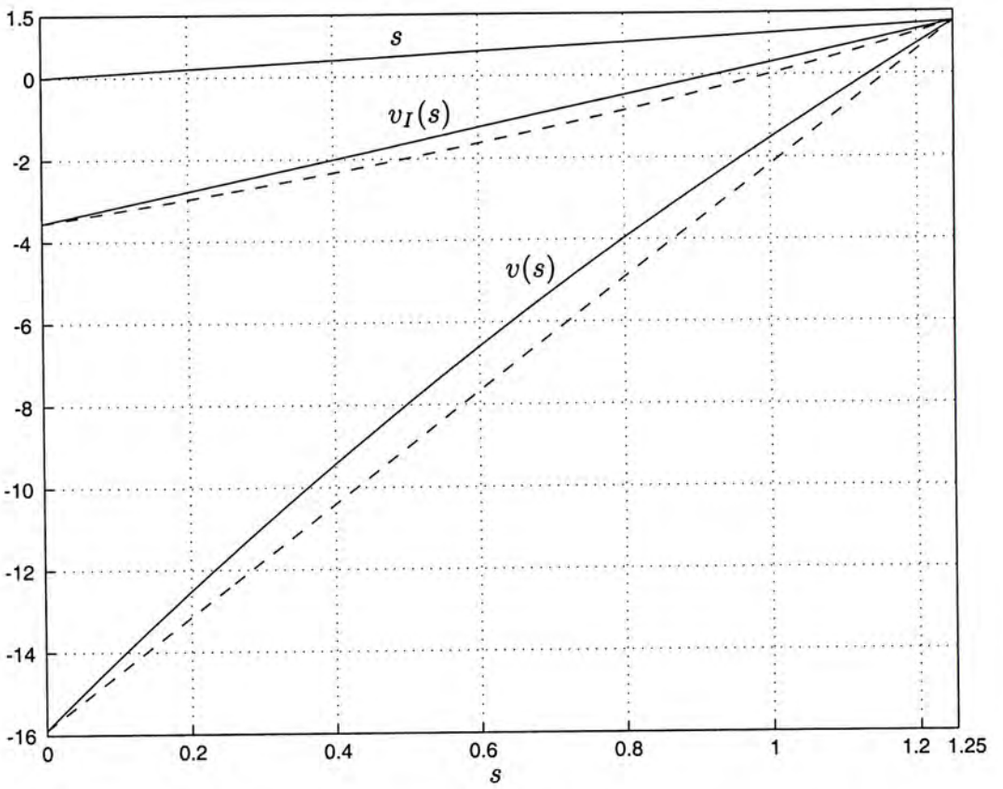


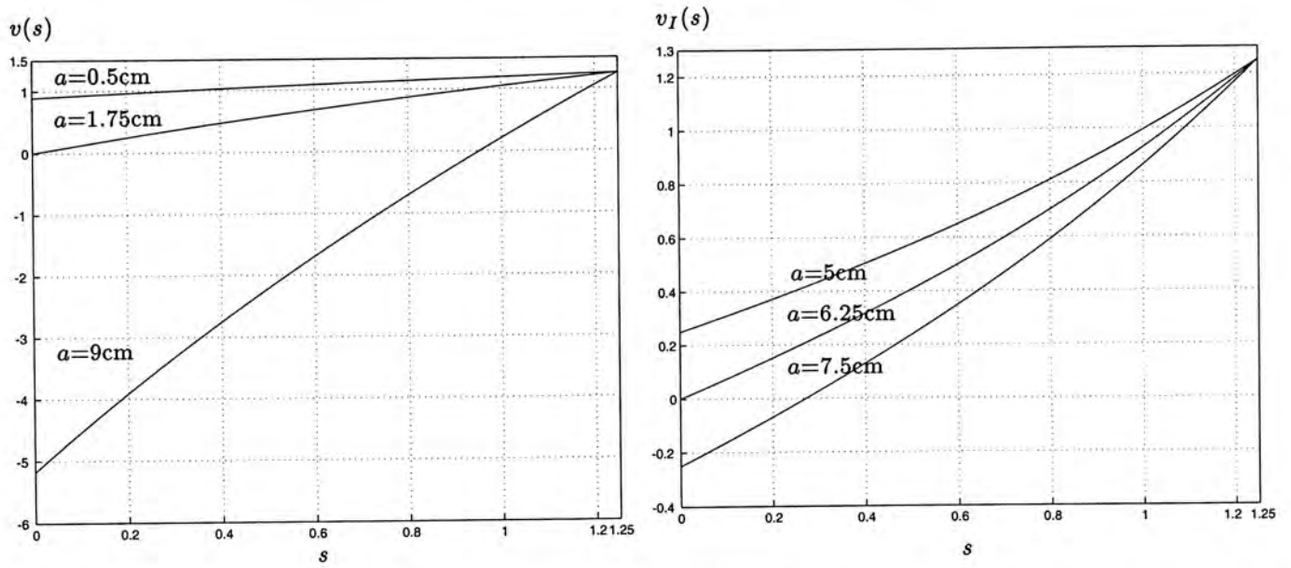
Figure 2.4: An example illustrating the vertical distortion: change of depth field and non-linear distortion.

2.4.2 Change of Depth Field

This type of distortion concerns about compressions and elongations of the original surfaces. In general, as seen from Eq. 2.12, perceived heights $v_g(\bar{s})$ are

$$v_g(\bar{s}) = \bar{s} \tag{2.17}$$

for all IS-separations $\sigma_g \in \Sigma(g)$. Owing to this fact, if perceived height $v_g(0)$ is below zero, perceived surface $S_{p,g}(u, v)$ elongates the original surface, which extends negatively beyond the bottom of the original surface. On the other hand, if $v_g(0)$ is positive, the original surface is compressed such that the bottom of perceived surface $S_{p,g}(u, v)$ is pushed upwards above the bottom of the original surface. Otherwise, the depth field of perceived surface $S_{p,g}(u, v)$ is the same as that of original surface $S(x, y)$.



(a) (b)

Figure 2.5: (a) The plots of (a) $v(s)$ and (b) $v_I(s)$ against s.

IS-separations	Compressed	Elongated	The depth field unchanged
$\sigma_I(s)$	$\frac{D_S}{D_R} > \frac{a-1}{e-1}$	$\frac{D_S}{D_R} < \frac{a-1}{e-1}$	$\frac{D_S}{D_R} = \frac{a-1}{e-1}$
$\sigma(s)$	$\frac{D_S}{D_R} > 1 + \frac{a}{e-1}$	$\frac{D_S}{D_R} < 1 + \frac{a}{e-1}$	$\frac{D_S}{D_R} = 1 + \frac{a}{e-1}$

Table 2.1: The relations between the changes of depth field and the parameters when IS-separations σ_I and σ are employed to generate the autostereogram.

In particular, from Eq. 2.14 and Eq. 2.16, the vertical interceptions of curve $v(s)$ and $v_I(s)$ are, respectively,

$$v(0) = \bar{s} - \frac{aD_R}{e-1}, \tag{2.18}$$

and

$$v_I(0) = \bar{s}\left(1 - \frac{aD_R}{eD_S - \bar{s}}\right). \tag{2.19}$$

Using the above observations, the relations between the changes of depth field and the parameters with respect to IS-separations σ and σ_I are presented in Table 2.1. These relations are also visualized in Fig. 2.5 using several examples. In

Fig. 2.5(a), we let the parameters be $D_S = 3.75$cm, $D_R = 2.5$cm and $e = 4.5$, but let the value of a varies. When $a = 0.5$cm and $a = 9$cm, the original surface are compressed ($v(0) > 0$) and elongated ($v(0) < 0$), respectively. Otherwise, the depth field is not changed ($v(0) = 0$) when $a = 1.75$cm. In Fig. 2.5(b), the parameters D_S, D_R and e are set to be the same as that in Fig. 2.5(a). In this case, when $a = 5$cm and $a = 7.5$cm, the original surface is compressed ($v_I(0) > 0$) and elongated ($v_I(0) < 0$), respectively. Otherwise, depth field of the perceived surface is same as that of the original surface ($v_I(0) = 0$) when $a = 6.25$cm.

From our intuitive feelings, this type of distortion usually do not cause significant problem to the viewers in recognizing the encoded surfaces, since the features of the surfaces may still remain.

Using the same parameters D_R, D_S, E, a and e, the depth field for IS-separation σ is always greater that for IS-separation σ_I for the fact that

$$v(0) < v_I(0). \tag{2.20}$$

2.4.3 Non-linear Distortion

When the original surfaces are distorted non-linearly, the perceived surfaces may be out of scale, or lopsided. This can be seen from the instance in Fig. 2.4 that the points of medium heights are much distorted than the others. In the extreme cases, the heights at some points may be too exaggerated, and the other points may be seriously compressed. Therefore, under serious distortions of such kind, the viewers may feel uncomfortable to recognize the original surfaces.

We measure the extent of non-linear distortion using the second derivative $v_g''(s)$ (or curvature) of the perceived height with respect to s. In fact, the greater the absolute values of the curvatures are, the greater extent the original surfaces are non-linearly distorted . Further, curvatures $v_g''(s)$ change as s, e and a vary. The

relations between the changes of the parameters and the respective distortions can be studied using the partial derivatives with respect to these parameters. In the following, we will study the non-linear distortions with respect to IS-separations σ and σ_I.

Firstly, we consider the distortions when IS-separation σ is used. The curvature of perceived heights $v(s)$ with respect to s is

$$v''(s) = \frac{d^2 v_g(s)}{ds^2} \tag{2.21}$$

$$= -\frac{2aeD_R}{\bar{s}^2(e-1+s\bar{s}^{-1})^3} < 0 \tag{2.22}$$

for all $s \in \mathcal{S}$. To account for the influences of e and s on curvature $v''(s)$, we study the partial derivative

$$\frac{\partial^2 v''}{\partial s \partial e} = \frac{\partial}{\partial s}\left\{\frac{2aD_R(2e+1-s\bar{s}^{-1})}{\bar{s}^2(e-1+s\bar{s}^{-1})^4}\right\} \tag{2.23}$$

$$\tag{2.24}$$

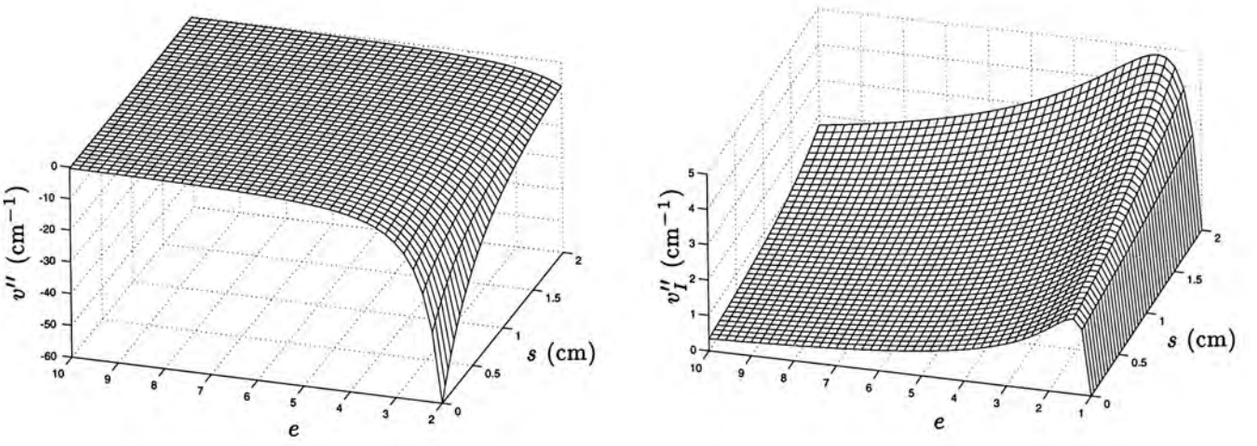
$$= -\frac{6aD_R}{\bar{s}^3} \times \frac{3e-1-s\bar{s}^{-1}}{(e-1+s\bar{s}^{-1})^5} < 0. \tag{2.25}$$

In the above partial derivative, a is not involved since the influences of changing a are obvious from Eq. 2.22.

For the cases that IS-separation σ_I is used, the curvature of perceived height $v_I(s)$ is

$$v_I''(s) = \frac{d^2 v(s)}{ds^2} \tag{2.26}$$

$$= \frac{2aeD_R{}^2}{(e-1+D_R(D_S-s)^{-1})^2(D_S-s)^3} \times \left[1 - \frac{D_R}{(e-1)(D_S-s)+D_R}\right] \geq 0 \tag{2.27}$$



(a) (b)

Figure 2.6: The three-dimensional plots of (a) v'', and (b) v_I'' against e and s with $a = 24$, $D_R = 2.5$cm and $D_S = 4.5$cm.

for all $s \in \mathcal{S}$. Then, the partial derivative of v_I'' with respect to e and s is

$$\frac{\partial^2 v_I''}{\partial s \partial e} = \frac{\partial}{\partial s}\left\{\frac{2aD_R{}^2\left(e^2(s-D_S)+2eD_R+\bar{s}-s)\right)}{\left(D_S-s\right)^4\left(e-1+D_R(D_S-s)^{-1}\right)^4}\right\} \tag{2.28}$$

$$\tag{2.29}$$

$$= 6aD_R^2 \times \frac{e^2\left(s-D_S+3D_Re^{-1}+(\bar{s}-s)e^{-1}\right)}{(e-1)^4\left[(D_S-s)+D_R(e-1)^{-1}\right]^5}. \tag{2.30}$$

It is noted that curvatures $v''(s)$ and $v_I''(s)$ behave very differently. Firstly, $v''(s) < 0$, but in contrast $v_I''(s) \geq 0$ for all s. Secondly, the changes of curvatures v'' and v_I'' with respect to e and s is also remarkably different. The observations are summarized in Table 2.2. Using the parameters $a = 24, D_R = 2.5$cm and $D_S = 4.5$cm, the curvatures v'' and v_I'' are plotted in Fig. 2.6 to visualize the contributions of e and s to the non-linear distortions. The shapes of these plots are resembled using different parameters. In the following, these observations are elaborated in terms of the curvatures and partial derivatives.

As seen from Eq. 2.25, when both e and s tend to be large, the denominator $(e-1+s\bar{s}^{-1})^5$ tends to be very large such that $\dfrac{\partial^2 v''}{\partial s \partial e}$ tends to zero, which implies

	e: $1 \rightarrow +\infty$, for a particular s	$s \uparrow$, for a particular e
v''	Very neg. $\xrightarrow{\text{Rapidly}}$ Less neg. $\xrightarrow{\text{Gradually}} 0$	$\uparrow$ rapidly, then gradually
v''_I	$0 \xrightarrow{\text{Rapidly}}$ Max. pt.* $\xrightarrow{\text{Exponentially}} 0$	$\uparrow$ almost constant rate

* The maximum point attains at the solution of Eq 2.31.

Table 2.2: The changes of the curvatures v'' and v''_I with respect to e and s.

that the curvature v'' does not change very much for large e and s. On the other hand, when both e and s are small such that denominator $(e - 1 + s\bar{s}^{-1})$ is smaller than unity, $\frac{\partial^2 v''}{\partial s \partial e}$ becomes very negative, which results in the dramatical drop of curvature v'' towards negative infinity. Also, the extent of non-linear distortions depends on a as well. It is obvious that curvature v'' increases with a, which implies that the father away the viewers from the autostereograms, the greater extent the perceived surfaces will be distorted non-linearly.

In contrast, $\frac{\partial^2 v''_I}{\partial s \partial e}$ is not all the way negative. In fact, curvature v''_I is not monotonic with respect to e. For a fixed s, v''_I increases gradually as e decreases. Afterward, it attains the maximum point when the partial derivative of v''_I with respect to e (embraced in the big brackets of Eq. 2.28) equals to zero. This is equivalent to that e is the solution of

$$e^2(s - D_S) + 2eD_R + \bar{s} - s = 0 \tag{2.31}$$

for a fixed s. Afterwards, v''_I drops significantly to reach 0 at $e = 1$ $(E_v = E)$, at which the perceived surfaces are not distorted non-linearly, disregarding the distances from the viewers to the autostereograms.

2.4.4 Lateral Distortions

In the following, we will derive η_g for the lateral distortions with references to Fig. 2.7. In this figure, point A and B are the corresponding points to encode

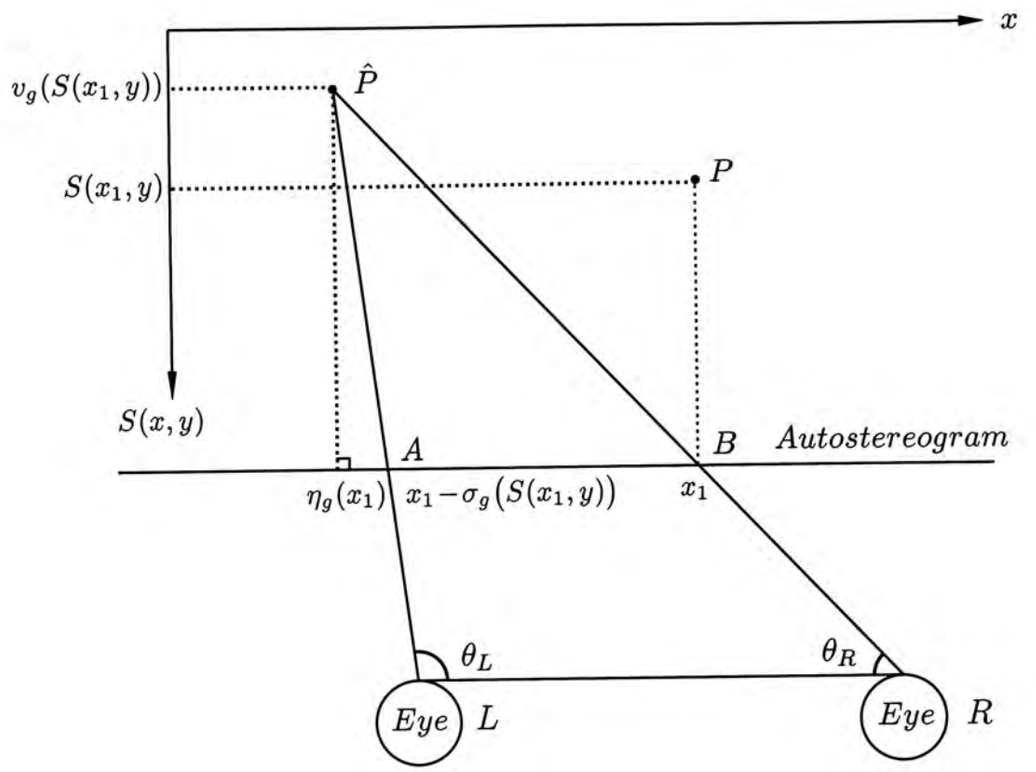


Figure 2.7: Lateral distortions.

the height of P which belongs to original surface $S(x, y)$. Under our proposed autostereogram generation method, it is assumed that the horizontal position of P is the same as that of B. Suppose P appears at $\hat{P}$ when the autostereogram is being viewed due to both vertical and horizontal distortions. Let the x-coordinates of $\hat{P}$ be $\eta_g(x)$. Then, the heights attained by $\hat{P}$ and P are, respectively, $v_g(S(x_1, y))$ and $S(x_1, y)$, where the function v_g is owing to the vertical distortions. Also, let θ_L be the angle between AL and LR, and θ_R be the angle between RB and LR. By simple

geometry, the derivation for η_g is straight forward. In general, $\eta_g(x)$ is expressed as

$$\eta_g(x) = \begin{cases} x - \sigma_g(S(x), y) - \dfrac{\bar{s} - v_g(S(x,y))}{\tan(180^\circ - \theta_L)}, & \theta_L > \theta_R; \\ x + \dfrac{\bar{s} - v_g(S(x), y)}{\tan(180^\circ - \theta_R)}, & \theta_R > \theta_L; \\ x + \sigma_g(S(x,y))/2, & \theta_L = \theta_R. \end{cases} \tag{2.32}$$

for all IS-separations $\sigma_g \in \Sigma(g)$ and $\sigma_0 \leq x \in \mathbf{X}$.

2.5 Discrete Autostereograms

Practically, autostereograms are generated by computers in most applications. However, it is not feasible to represent functions in computers with absolute fidelity using infinite points. "Continuous" functions, say $f(x, y)$, are often sampled uniformly in space and quantized in amplitude before performing manipulations in computers, namely

$$f_d(i, j) = Q[f(iT, jT)] \tag{2.33}$$

where $Q[\cdot]$ is the quantization process, and T is the sampling interval. Then, $f_d(i, j)$ are discrete-space sequences consisting a finite number of samples denoted by (i, j).

Accordingly, to generate autostereograms in computers, original surfaces $S(x, y)$ are sampled to produce their discrete counterparts $S_d(i, j)$. In common practices, the samples are taken with sampling interval $T = 1$ and quantized to integers. More precisely,

$$S_d(i, j) = Q_I[S(i, j)] \tag{2.34}$$

for $i = 1, \ldots, L_1$ and $j = 1, \ldots, L_2$ where $L_1 \leq x_s$ and $L_2 \leq y_s$. The process $Q_I[\cdot]$ is the quantization process in which real numbers are rounded to integers using any rounding rule.

Autostereograms encoding surfaces $S_d(i,j)$ are discrete autostereograms $R_d(i,j)$, which can be obtained by the extension of Eq. 2.6

$$R_d(i,j) = \begin{cases} \Pi(i,j), & 1 \le i \le \sigma_0 \\ R_d\big(i - Q_I[\sigma_g(S(i,j))], j\big), & \sigma_0 < i \le L_1, \end{cases} \tag{2.35}$$

for all IS-separations $\sigma_g \in \Sigma(g)$ and (i,j). Not surprisingly, discrete autostereograms $R_d(i,j)$ are two-dimensional discrete-space sequences with $L_1 \times L_2$ samples defined on the positions (i,j).

It is not guaranteed that IS-separations $\sigma_g(S_d(i,j))$ are integers. But, autostereograms $R_d(i,j)$ are defined for the integer values of i and j. Thus, IS-separations $\sigma_g(S_d(i,j))$ have to be truncated to integers by the quantization process $Q_I[\cdot]$ in Eq. 2.35. For instance, as suggested in [10], such values are rounded to the nearest integers followed by adding 1s randomly to avoid systematic bias.

Since $\sigma(g)$ is an one-to-one mapping (s.m.d.) such that inverse σ_g^{-1} exists. Then, the reconstructed surface $\tilde{S}_d(i,j)$ can be determined by extending Eq. 2.9 such that

$$\tilde{S}_d(i,j) = \begin{cases} 0, & 1 \le i \le \sigma_0 \\ \sigma_g^{-1}(d), & \sigma_0 < i \le L_1,\ R(i,j) = R(i-d,j) \\ \text{undefined}, & \text{otherwise} \end{cases} \tag{2.36}$$

for all IS-separations $\sigma_g \in \Sigma(g)$, positions (i,j) and $d = 1, \ldots, \sigma_0$.

2.5.1 Truncation Problem

We now assume that false targets and echoes are devoid such that every pair of the corresponding positions on the autostereogram are correctly matched. Thus, the distance between any pair of the matched positions is $d = Q_I[\sigma_g(S_d(i,j))]$ as stated in Eq. 2.35. In this case, by Eq. 2.36, original surfaces $S_d(i,j)$ are exactly

reconstructed if

$$S_d(i,j) = \tilde{S}_d(i,j) \tag{2.37}$$

$$= \sigma_g^{-1}(d) \tag{2.38}$$

for all $\sigma_0 < i \leq L_1$. Substituting $d = Q_I\big[\sigma_g(S(i,j))\big]$, we find that the condition in Eq. 2.38 becomes

$$S_d(i,j) = \sigma_g^{-1}\big(Q_I\big[\sigma_g(S_d(i,j))\big]\big) \tag{2.39}$$

for all $\sigma_0 < i \leq L_1$. Obviously, the above equality holds if and only if the argument of $Q_I[\cdot]$ is integer.

Assume we have the IS-separation $\sigma(s) = E - \frac{sE}{\bar{s}}$. The argument of $Q[\cdot]$ in Eq. 2.39 becomes

$$\sigma(S_d(i,j)) = E - \frac{S_d(i,j)E}{\bar{s}}. \tag{2.40}$$

Suppose bound $\bar{s}$ is an integer. If E is a multiple of $\bar{s}$, IS-separation $\sigma(S_d(i,j))$ are integers for all $\sigma_0 < i \leq L_1$. In this case, the condition of Eq. 2.38 holds, and hence exact reconstructions are feasible, provided that echo and false target are devoid.

On the other hand, if the IS-separation is σ_I, the argument of $Q[\cdot]$ in Eq. 2.39 becomes

$$\sigma_I(S_d(i,j)) = E - \frac{ED_R}{D_S - S_d(i,j)}. \tag{2.41}$$

However, the fraction introduces decimal, which contradicts the condition in Eq. 2.38 for some (i,j). Hence, original surfaces $S_d(i,j)$ can not be reconstructed exactly.

2.5.2 Computer Algorithms for Autostereograms

We develop a new autostereogram generation algorithm, in which IS-separation σ is adopted. We have seen that if the IS-separation σ is adopted, discrete surfaces $S_d(i,j)$ can be exactly reconstructed from discrete autostereograms provided that

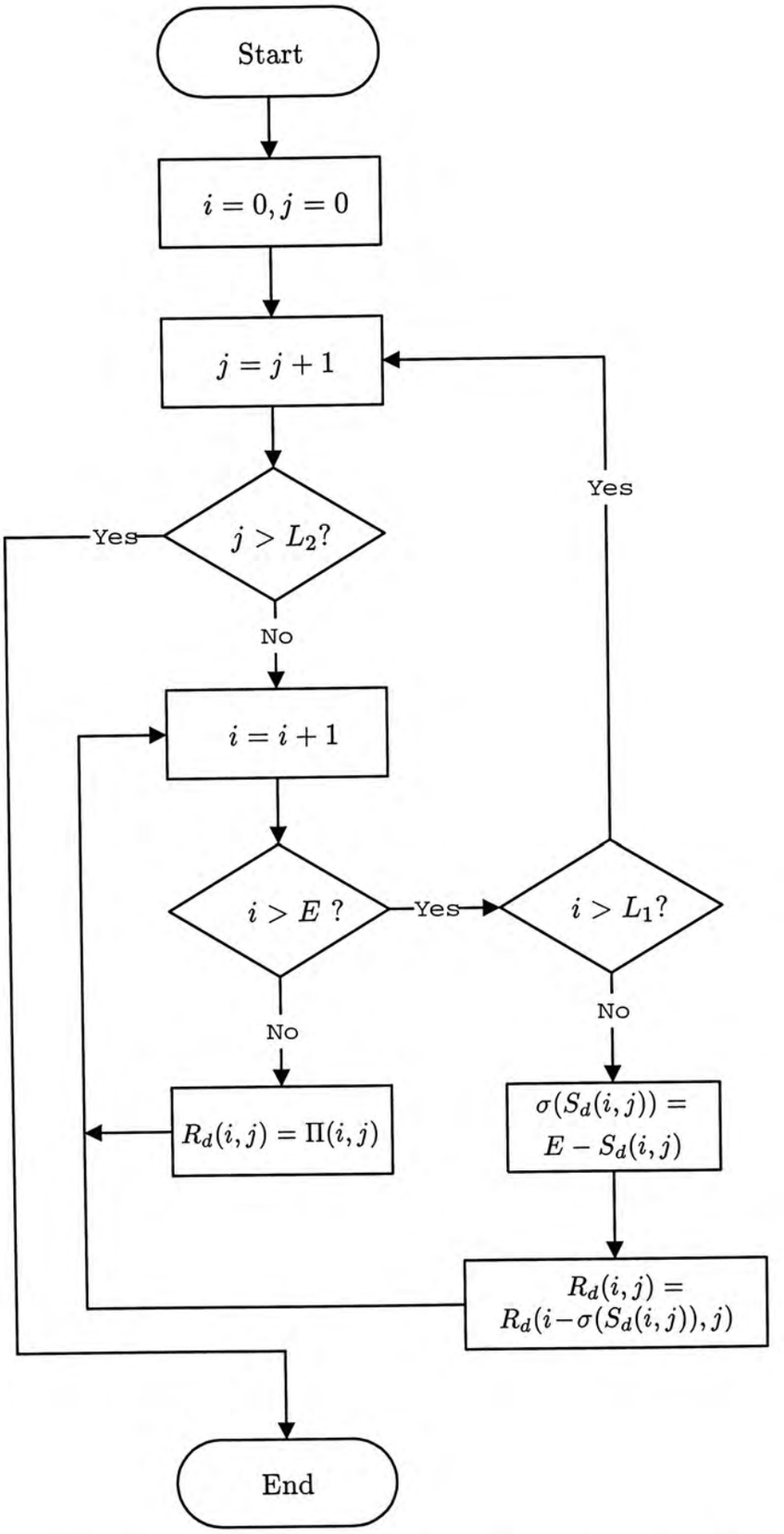


Figure 2.8: The proposed autostereogram generation algorithm.

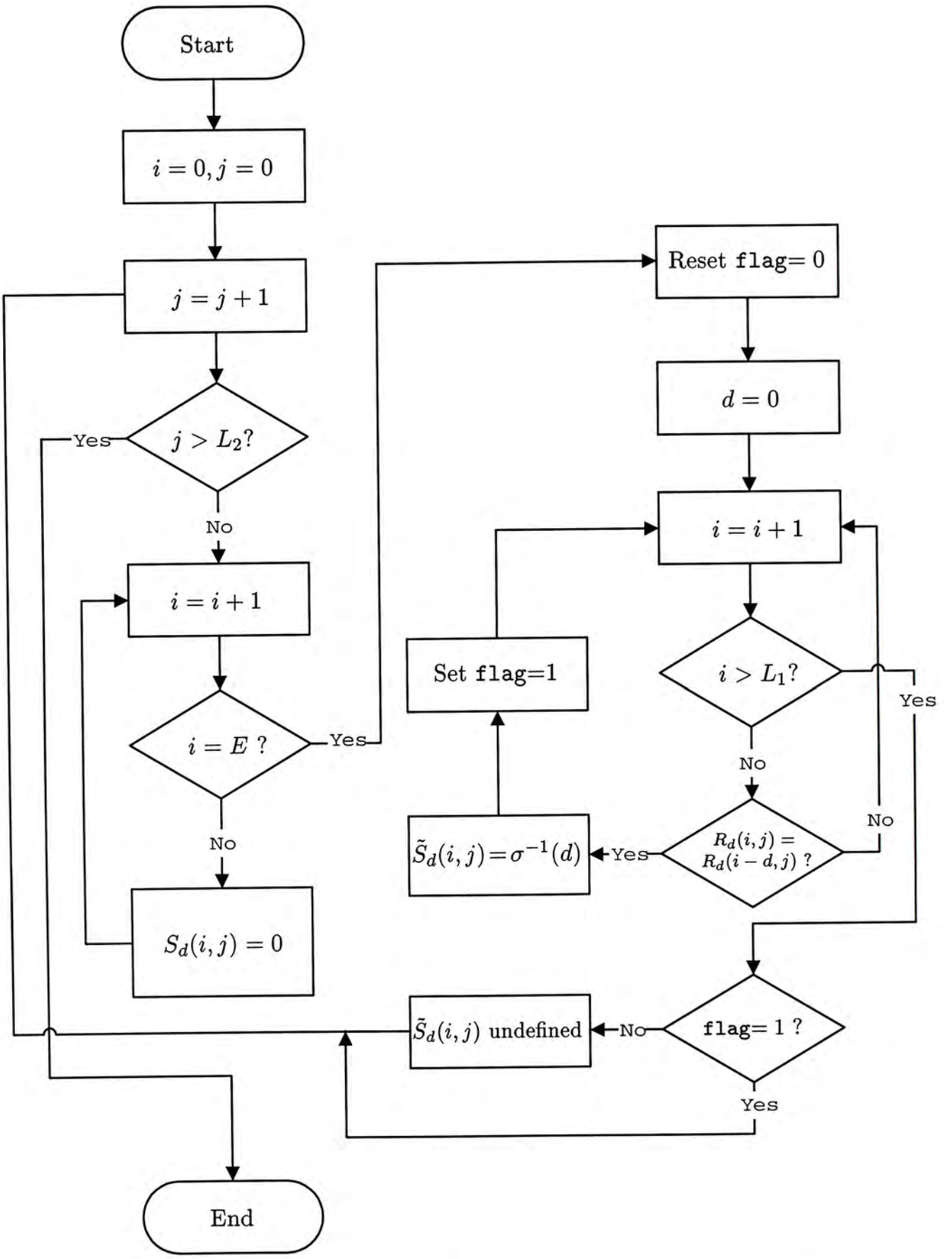


Figure 2.9: The proposed surface reconstruction algorithm.

echoes and false targets are devoid. The false target and echo avoidance techniques will be developed in the coming sections. We will see that by imposing some conditions, any original surface $S_d(i,j)$ can be exactly reconstructed from the autostereogram $R_d(i,j)$ using this algorithm.

The generation and surface reconstruction algorithms are implanted from Eq. 2.36 and Eq. 2.35, and developed in the flowcharts in Fig. 2.8 and Fig. 2.9, respectively. We have to mention that bound $\bar{s}$ is assumed to be equal to E, i.e. $\bar{s} = E$. In fact, other values such as $\bar{s} = E/2$, $\bar{s} = E/3$,... are possible to avoid the truncation problem, as long as E is a multiple of bound $\bar{s}$. But, the greatest bound $\bar{s}$ should be chosen to allow the greatest flexibility of the original surfaces for a fixed E. Thus, with the above assumption, the IS-separation is expressed as

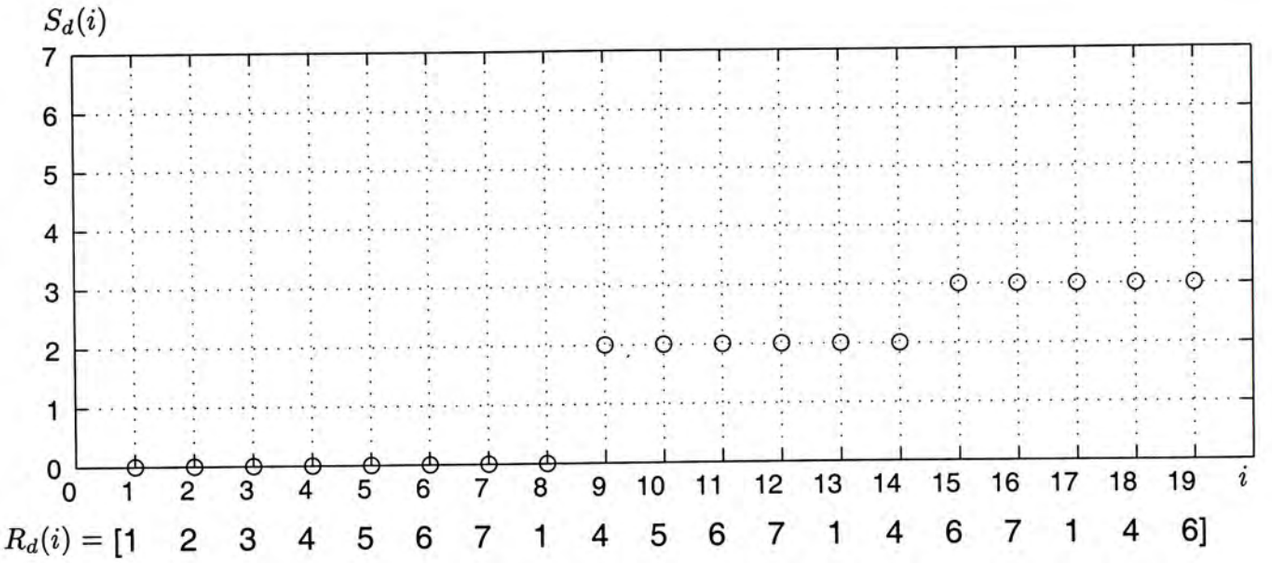
$$\sigma\big(S_d(i,j)\big) = E - S_d(i,j) \tag{2.42}$$

for all (i,j). Then, the IS-separation of zero height is $\sigma_0 = \sigma(0) = E$. We will see that by imposing some conditions to avoid echoes, any original surface $S_d(i,j)$ can be exactly reconstructed from the autostereogram using these algorithms. For the rest of the examples, Eq. 2.42 will be used to compute IS-separations.

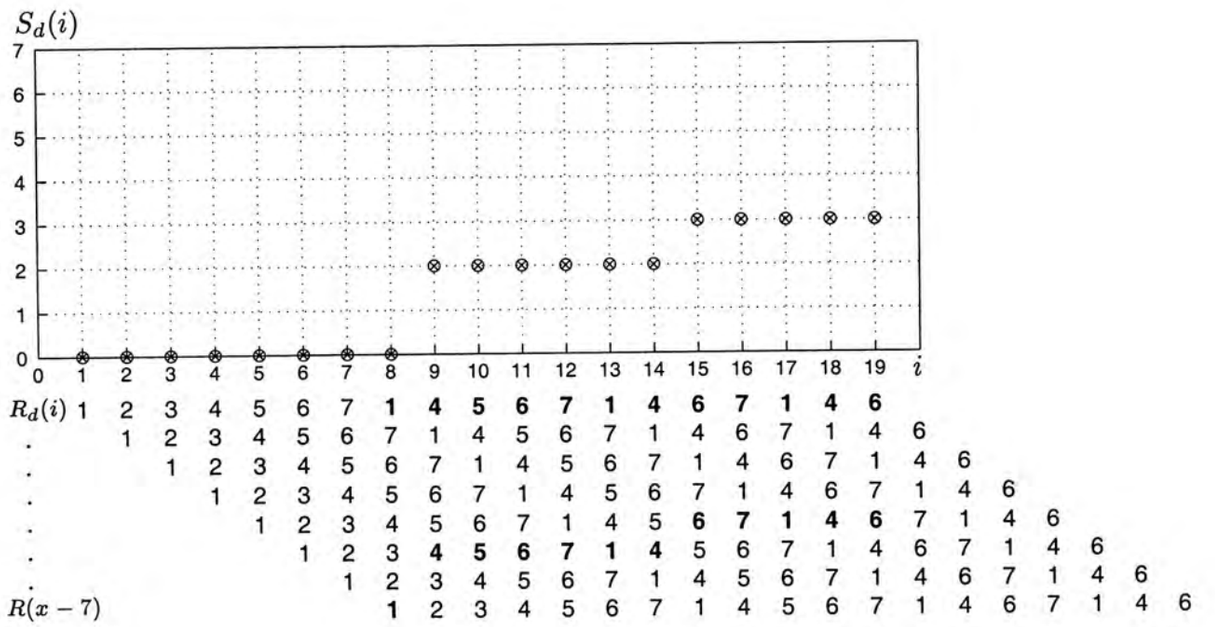
Example 2.1. We aim at demonstrating discrete autostereogram generations and surface reconstructions using the proposed algorithms. The one-dimensional discrete surface $S_d(i)$ is represented in "circles" in Fig. 2.10(a). By letting $\bar{s} = 7$, the IS-separations are computed using $\sigma(S_d(i)) = 7 - S_d(i)$. To avoid the loss of depth information, the values of $S_d(i)$ are set to zeroes for $1 \leq i \leq \sigma_0$, and the actual surface starts at $i = 8$. Moreover, we use a horizontally uncorrelated sequence $\Pi = [\ 1\ \ 2\ \ \cdots\ \ 7\ ]$ as the pre-defined pattern to prevent false targets. In the first seven iterations ($i = 1, 2, \ldots, 7$), the autostereogram are assigned with the pre-defined patterns, i.e. $R_d(i) = \Pi(i)$. In the rest of the iterations, $R_d(i,j)$ are assigned

by copying from $R_d(i - \sigma_{S,d}(i))$, i.e. $R_d(i) = R_d(i - \sigma_{S,d}(i))$. For instance, since IS-separation $\sigma(S_d(14)) = 7 - 2 = 5$, we have $R_d(14) = R_d(9) = 4$. The copying steps operate recursively until $i > L_1 = 19$.

The corresponding surface reconstruction process is shown in Fig 2.10(b). Since the leftmost positions ($i = 1, 2, \cdots, 7$) do not contain any depth information, the reconstructed heights at these positions are simply zeroes, i.e. $\tilde{S}_d(i) = 0$. For the rest of the positions ($1 \leq i \leq L_1 = 19$), reconstructed surface $\tilde{S}_d(i)$ is obtained by first shifting $R_d(i)$ to get $R_d(i - d)$ for $d = 1, 2, \ldots, 7$. Then, they are compared with each other to look for the correspondences (in bold face). For instance, $R_d(16)$ and $R_d(12)$ are the corresponding positions with the separation $d = 4$, therefore, reconstructed height $\tilde{S}_d(16)$ is 3. The reconstructed surface $\tilde{S}_d(i)$ is shown in the figure using "crosses".



(a)



(b)

Figure 2.10: Demonstrating autostereogram generations and reconstructions: (a) one-dimensional surface $S_d(i)$ (in "circles") and the corresponding autostereogram $R_d(i)$; (b) surface reconstruction process and reconstructed surface $\tilde{S}_d(i)$ (in "crosses").

Chapter 3

Analysis of Echoes

Echoes limit autostereograms in many aspects. To the viewers, echoes are visually unpleasant and distracting fragments seem to be "floating" in the space to interfere eye convergences. An illustration depicting the visual problem due to echoes is shown in Fig. 3.1. Suppression of echoes becomes a major concern for generating good quality autostereograms. But in fact, their causes have not been fully understood so that the method proposed to avoid echoes are intuitive and ad hoc.

In the presence of echo, some positions of the reconstructed surfaces $\tilde{S}(x, y)$ have multiple values. Thus, the reconstructed surfaces are not uniquely obtained, so that the original surfaces are not guaranteed to be exactly reconstructed. The inability of exact reconstructions narrows the prospects of autostereograms towards new applications, especially for which exact reconstruction is the key requirement.

In this chapter, the problem of echo is revealed. We first obtain the necessary and sufficient condition for the presences of echo. Based on this condition, we observed that echoes appear in two situations, namely *insufficient lengths of the periods of the repeating patterns* and *overlapping of copying steps*. Conditions are derived to avoid such situations. The drawbacks of such avoidance are also discussed. We discover that although the reconstructed surface is uniquely obtained from an

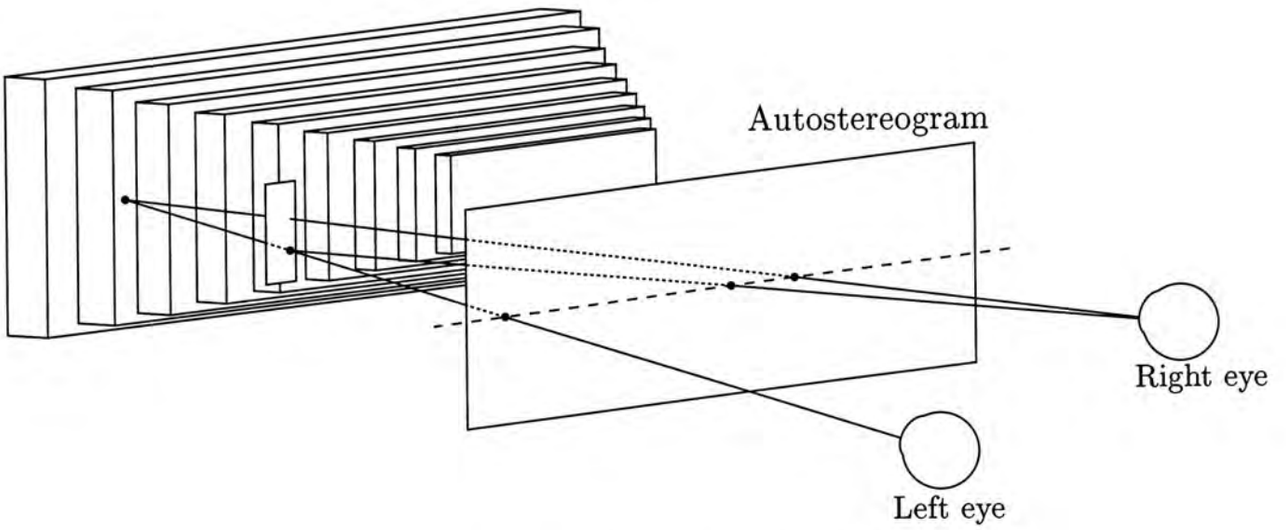


Figure 3.1: An illustration of echoes.

echo-free autostereogram, exact reconstruction of the original surface is still not guaranteed. Therefore, we develop further conditions to restrict the generations of autostereograms such that the original surfaces can always be exactly reconstructed from the resulting autostereograms.

Autostereograms are generated row-wise. The depth information is encoded by the correlations in the x-direction only. Therefore, autostereograms $R(x, y)$ are independent of the y-axis. To simplify the discussions and notations, one-dimensional autostereograms $R(x)$ and surface profiles $S(x)$ are used interchangeably in the followings.

3.1 Causes of Echoes

Surface reconstruction processes are, in fact, matching processes in which $R(x, y)$ and $R(x - d, y)$ are compared, where $R(x - d, y)$ are obtained by shifting $R(x, y)$ to the right for $1 \leq d \leq \sigma_0$. Let $\sigma_0 < x_0 \leq x_s$, if $R(x_0, y_0)$ and $R(x_0 - d, y_0)$ are identical, then by Eq. 2.9 $\tilde{S}(x_0, y_0)$ are determined by

$$\tilde{S}(x_0, y_0) = \sigma_g^{-1}(d) \tag{3.1}$$

for all IS-separation $\sigma_g \in \Sigma(g)$. If there are more than one, say m, values of d such that $R(x_0, y_0) = R(x_0 - d, y_0)$ holds, then $\tilde{S}(x_0, y_0)$ will have m values. Consequently, the reconstructed surfaces $\tilde{S}(x, y)$ are not unique.

Conversely, suppose reconstructed surfaces $\tilde{S}(x, y)$ are not unique at (x_0, y_0) such that $\tilde{S}(x_0, y_0)$ have m values. Thus, on the same row y_0 of autostereograms $R(x, y)$, there exist m positions at which correspondences are established. By Eq. 2.8, these m positions have the same value, which are separated horizontally by a distance $1 \leq d \leq \sigma_0$. Thus, the following conclusion is deduced:

> Echo appears if and only if there exist more than two positions (x, y) on the same row of the autostereogram $R(x, y)$ satisfying the matching criterion, and the greatest distance of separation between these positions is not greater than σ_0 for all positions $(x, y) \in \mathbf{C}$ and IS-separation $\sigma_g \in \Sigma(g)$. (3.2)

When the reconstructed surfaces are not unique, the surface segments which do not belong to the original surfaces are indistinguishable since no additional information about the original surfaces is available with the autostereograms. Therefore, exact reconstructions of the original surfaces are not guaranteed. The reconstructed surface segments which do not belong to the original surfaces are called echoes.

Based on condition 3.2, we found that echoes result from two situations. In the first situation, the patterns on autostereograms repeat too frequently to cause false matches; in the second situation, the copying steps of positions at different heights interfere each others. We refer the situations as *insufficient lengths of the periods of repeating patterns* and *overlappings of copying steps*, respectively. The respective echoes associated with these situations are referred as *Type 1* and *Type 2*. In the following, we will explain how these situations cause echoes, which are followed by the conditions for echo avoidance in next section.

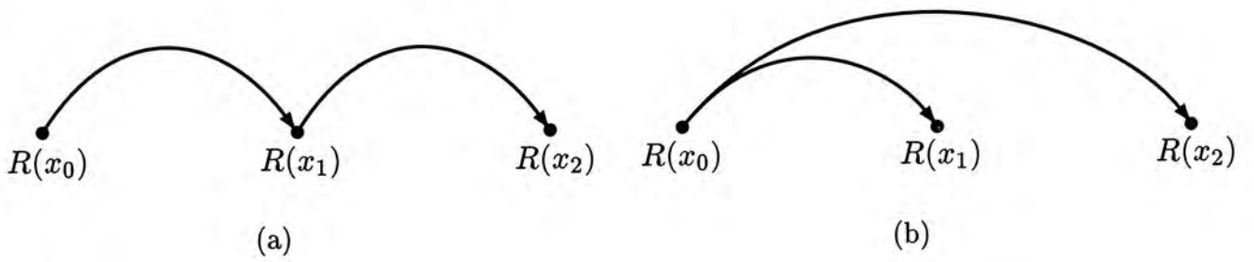


Figure 3.2: Illustration of the causes of echoes: (a) insufficient lengths of the periods of repeating patterns; (b) overlapping of copying steps.

3.1.1 Insufficient Lengths of The Periods of Repeating Patterns

Let $x_0, x_1, x_2 \in \mathbf{X}$ be the x-coordinates of autostereogram $R(x)$ such that $x_0 < x_1 < x_2$ as shown in Fig. 3.2(a). This figure illustrates a series of copying steps in which $R(x_2)$ is copied from $R(x_1)$ which in turn is copied from $R(x_0)$. Hence, $R(x_0)$, $R(x_1)$ and $R(x_2)$ are identical. Clearly, the maximum separation of these positions is the sum of the IS-separations of $S(x_1)$ and $S(x_2)$, i.e. $\sigma_g(S(x_1))+\sigma_g(S(x_2))$. If the periods of these repeating values are too small such that this sum is not greater than σ_0, then there are *at least* three positions having the same value on $R(x)$, and their maximum separation is less than or equal to σ_0. Then, by condition 3.2 echo(es) appear on the autostereogram.

3.1.2 Overlapping of Copying Steps

Another cause of echoes is overlapping of copying steps, which results from the depth transitions of the surface. We use the word "overlapping" due to the fact that a single position is involved in two copying steps. When copying steps overlap, they are copying the same position.

Again, we let $x_0, x_1, x_2 \in \mathbf{X}$ be the x-coordinates of $R(x)$ such that $x_0 < x_1 < x_2$ as shown in Fig. 3.2(b). In this figure, both values of $R(x_1)$ and $R(x_2)$ are copied from

$R(x_0)$. Thus, $R(x_0)$, $R(x_1)$ and $R(x_2)$ are identical, and their maximum distance of separation is IS-separation $\sigma_g(S(x_2))$, which is not greater than σ_0 for all IS-separation $\sigma_g \in \Sigma(g)$. Consequently, there are *at least* three positions on the same row having the same value, and the maximum separation among them is less than or equals to σ_0. Then by Eq. 3.2, we conclude that reconstructed surfaces $\tilde{S}(x)$ are not unique, and hence echo appears if copying steps overlap.

3.2 Avoidance of Type 1 Echoes

Some authors may use intuitive methods to avoid echoes. They observed that echoes are somehow related to the periods of the repeating patterns on autostereograms. Therefore, they tend to make the IS-separations intuitively large so that the patterns repeat less frequently, [9] for instance. In this section, we obtain a condition on the greatest height attained by the original surfaces $S(x, y)$, which guarantees that the periods of the repeating patterns are large enough to avoid Type 1 echoes.

We have seen in Fig. 3.2(a) that $R(x_0)$, $R(x_1)$ and $R(x_2)$ are identical. The maximum separation between them is the sum of the IS-separations of $S(x_1)$ and $S(x_2)$. In the surface reconstruction processes, these positions will *not* be falsely matched to give Type 1 echoes if and only if this sum is greater than σ_0, i.e.

$$\sigma_g(S(x_2)) + \sigma_g(S(x_1)) > \sigma_0. \tag{3.3}$$

for all $\sigma_g \in \Sigma(g)$. Nevertheless, condition of Eq. 3.3 is not algorithmic convenient in the sense that every pair of the corresponding positions have to be checked against it prior to autostereogram generations. We will make the condition more general in the following.

Since σ_g are s.m.d., the values of IS-separations σ_g are bounded such that

$$\sigma_g(\bar{s}_e) \leq \sigma_g(s) \leq \sigma_0 \tag{3.4}$$

for all IS-separations $\sigma_g \in \Sigma(g)$. Suppose we have the minimum IS-separation $\sigma_g(\bar{s}_e)$ such that

$$2\sigma_g(\bar{s}_e) > \sigma_0. \tag{3.5}$$

Thus, condition (3.3) holds if Eq. (3.5) is satisfied since $\sigma_g(\bar{s}_e)$ is the minimum IS-separation. We now aim at finding $\bar{s}_e$ which satisfies Eq. 3.5. By Eq. 2.2, the above equation becomes

$$2\left(E - \frac{ED_R}{D_S - g(\bar{s}_e)}\right) > E - \frac{ED_R}{D_S - g(0)}, \tag{3.6}$$

which can be further developed to

$$g(\bar{s}_e) < D_S - \frac{2D_R(D_S - g_0)}{D_S + D_R - g_0}, \tag{3.7}$$

where $g_0 = g(0)$ for all g. Furthermore, since g is s.m.i., the inverse g^{-1} exists. Finally, the condition of Eq. 3.5 becomes

$$\bar{s}_e < g^{-1}\left(D_S - \frac{2D_R}{1 + D_R(D_S - g_0)^{-1}}\right) \tag{3.8}$$

for all g.

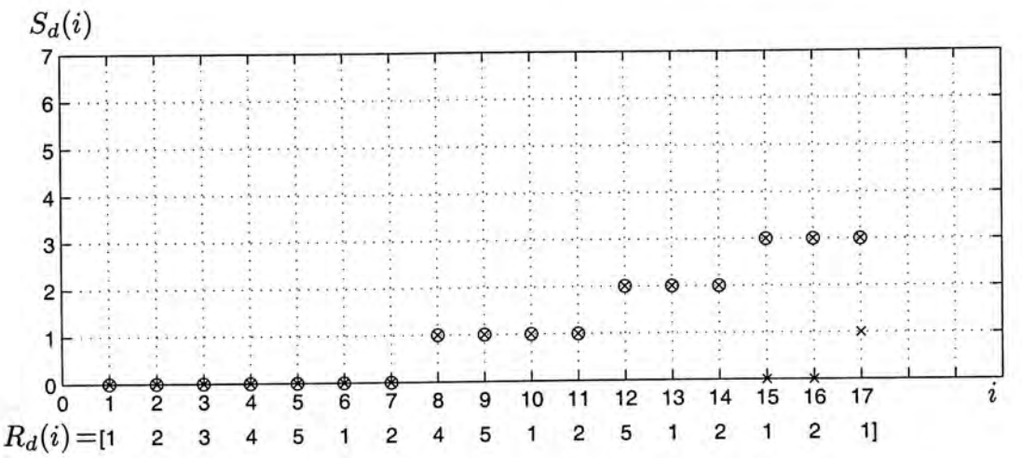
Hence, we can conclude that Type 1 echoes can be avoided if the maximum heights $\bar{s}_e$ attained by the original surfaces $S(x, y)$ are restricted such that Eq. 3.8 holds for all s.m.i. g.

In particular, suppose IS-separation σ is used to generated autostereograms. Substituting the transformation $g(s) = D_S - \frac{D_R\bar{s}}{s}$ into Eq. 3.8, the avoidance condition becomes

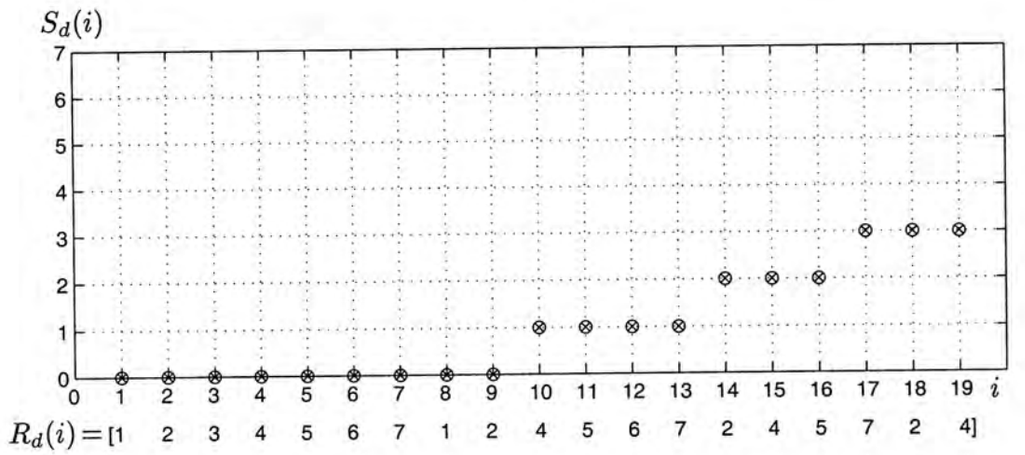
$$\bar{s}_e < \bar{s}/2. \tag{3.9}$$

In contrast, suppose the IS-separation is σ_I, in which $g(s) = s$ is an identity mapping. Then, condition of Eq. 3.8 becomes

$$\bar{s}_e < \frac{\bar{s}D_S}{D_S + D_R}. \tag{3.10}$$



(a)



(b)

Figure 3.3: Demonstrating Type 1 echo and its avoidance; (a) echoes appear when $\bar{s} = 5$; (b) echoes are devoid by increasing $\bar{s}$ to 7.

Example 3.1. In this example, we demonstrate how condition 3.9 successfully avoids Type 1 echoes in an discrete autostereogram. Original surface $S_d(i)$ (in "circles"), with the greatest attained height is $\bar{s}_e = 3$, is encoded in autostereogram $R_d(i)$ with $\bar{s} = 5$. By using Eq. 2.5, the IS-separations are computed using $\sigma(S_d(i)) = 5 - S_d(i)$. For the case shown in Fig. 3.3(a), the sum $\sigma(S_d(17)) + \sigma_d(S(15)) = 4$ is smaller than $\sigma_0 = 5$, which contradicts the condition of Eq. 3.3. Thus Type 1 echoes appear. To avoid those echoes, as shown in Fig. 3.3(b), we increase $\bar{s}$ to 7 such that

$\bar{s}_e < \bar{s}/2 = 3.5$. In this case, Eq. 3.9 is satisfied for all i, and the echoes are avoided.

3.3 Avoidance of Type 2 Echoes

We have concluded in Section 3.1 that Type 2 echoes appear if the copying steps overlap. Referring to Fig. 3.2(b), when the copying steps of x_1 and x_2 overlap, they are copying the same position x_0. In this case, we have the following relation

$$x_1 - \sigma_g(S(x_1)) = x_2 - \sigma_g(S(x_2)), \tag{3.11}$$

for all IS-separations $\sigma_g \in \Sigma(g)$. By rearranging the terms, the relation becomes

$$x_1 - x_2 = \sigma_g(S(x_1)) - \sigma_g(S(x_2)). \tag{3.12}$$

Define an *overlapping set* $\mathcal{O}$ to be the set containing all x-coordinates of positions (x, y) of which the copying steps overlap with that of the preceding positions. In other words, x-coordinates $x_\mathcal{O}$ belongs to the overlapping set $\mathcal{O}$ if there exists a position (x^*, y) on the autostereogram $R(x, y)$ such that the following equality is satisfied

$$x_\mathcal{O} - x^* = \sigma_g(S(x_\mathcal{O})) - \sigma_g(S(x^*)) \tag{3.13}$$

for all IS-separations $\sigma_g \in \Sigma(g)$ and $x_\mathcal{O} > x^*$.

In fact, overlappings of copying steps occur at decreasing surfaces, which is evident in the following. Since we have $x_1 < x_2$, the difference of IS-separations is

$$\sigma_g(S(x_1)) - \sigma_g(S(x_2)) < 0. \tag{3.14}$$

But, since functions σ_g are s.m.d., the above equation implies

$$S(x_1) > S(x_2). \tag{3.15}$$

Actually, this fact depends on the direction of generation. If autostereograms are generated from right to left such that the values of $R(x)$ are assigned by copying from the right, then overlappings will occur at increasing surfaces.

In fact, decreasing surfaces are unavoidable, except in flat surfaces. Therefore, the only way we can do to avoid Type 2 echoes is to remove the copying steps which cause overlapping from the copying procedures. We suggest that the values of $R(x_{\mathcal{O}})$ are not copied from the left for all $x_{\mathcal{O}} \in \mathcal{O}$. Instead, arbitrary real numbers p are assigned to $R(x_{\mathcal{O}})$. The number p should have not appeared on the same row of the autostereograms, namely

$$p \neq R(x) \tag{3.16}$$

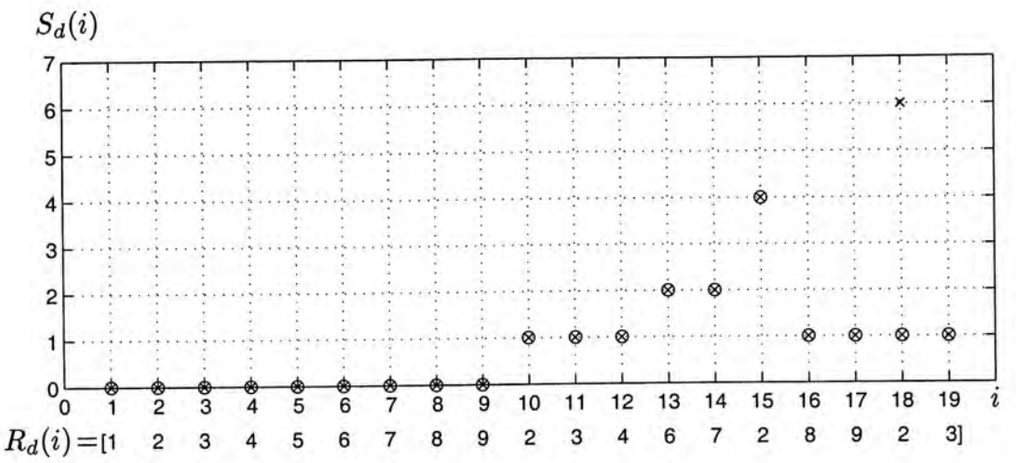
for all $x < x_{\mathcal{O}}$.

Consequently, Eq. 2.6 is modified for Type 2 echo avoidance. For all IS-separations $\sigma_g \in \Sigma(g)$ and positions $(x, y) \in \mathbf{C}$

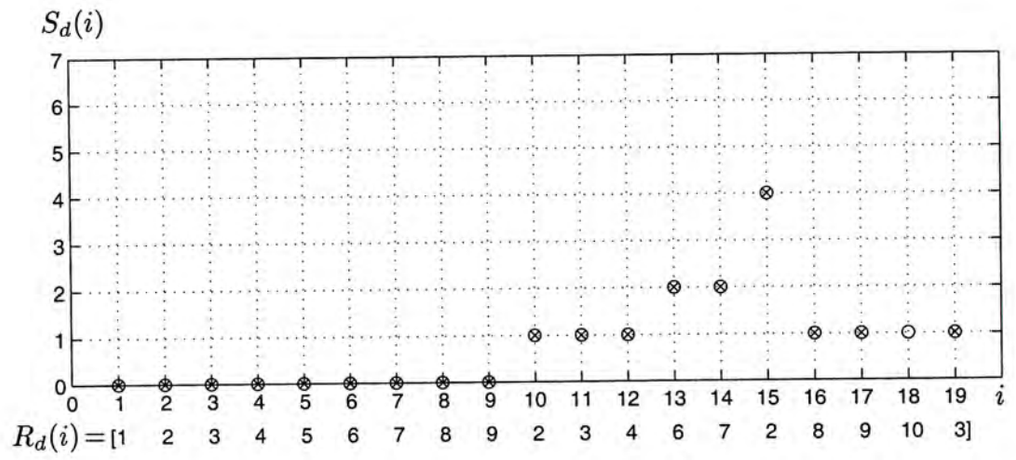
$$R(x,y) = \begin{cases} P(x,y), & 1 \leq x \leq \sigma_0 \\ p, & \sigma_0 < x \leq x_s,\ x \in \mathcal{O} \\ R(x - \sigma_g(S(x,y)), y), & \text{otherwise.} \end{cases} \tag{3.17}$$

where $p \neq R(x', y)$ for all $x' < x$.

Example 3.2. In this example, we illustrate Type 2 echoes and their avoidance using Eq. 3.17. Given that the maximum height attained ($\bar{s}_e = 4$) by the surface $S_d(i)$ is smaller than one half of bound $\bar{s} = 9$, so that the condition to avoid Type 1 echoes is satisfied. Therefore, any echo appearing on the autostereogram is solely caused by overlapping of copying steps. For the autostereogram shown in Fig. 3.4(a), the difference $\sigma(S_d(18)) - \sigma(S_d(15))$ is equal to 3, therefore the copying steps of $i = 18$ and $i = 15$ copy the same position $i = 10$. By definition, the coordinate $i = 18$ belongs to overlapping set $\mathcal{O}$. Consequently, echo appears at $i = 18$. In contrast, as



(a)



(b)

Figure 3.4: Demonstrating Type 2 echo and it avoidance: (a) overlapping of copying steps is not avoided, in which $i = 18$ belongs to the overlapping set; (b) echoes are devoid by avoiding the overlappings using Eq. (3.17).

shown in Fig. 3.4(b), the echo can nevertheless be avoided by removing the copying step of $i = 18$. By Eq. 3.17, $R_d(18)$ is then assigned with $p = 10$ which have not appeared for $i = 1, 2, \ldots, 17$. Then, the reconstructed surface $\tilde{S}_d(i)$ is free of echo.

Before the end of this section, few remarks have to be made regarding the avoidance of Type 2 echoes:

1. Autostereograms $R(x)$ are free of Type 2 echoes by using Eq. 3.17. However,

there are disadvantageous effects resulted from such removal of copying steps. We have seen that $R(x_{\mathcal{O}})$ are assigned with p, which have not appeared on the left, i.e. $p \neq R(x)$ for all $x < x_{\mathcal{O}} \in \mathcal{O}$. Thus, there is no corresponding position on the left so that by Eq. 3.17, reconstructed surface $\tilde{S}(x)$ is undefined at $x_{\mathcal{O}}$. For instance, $\tilde{S}_d(18)$ in Fig. 3.4(b) is not defined. As the consequence, visual artifacts are created if too many copying steps are removed.

2. In the circumstances of item 1, $\tilde{S}(x_{\mathcal{O}})$ are undefined due to echo avoidance. Therefore, the depth information of original surfaces $S(x)$ is lost at $x_{\mathcal{O}}$. Nonetheless, the lost information can be recovered for some surfaces having special "shapes". If we have a surface $S(x)$ such that $S(x_{\mathcal{O}} + 1) = S(x_{\mathcal{O}})$ for all $x_{\mathcal{O}} \in \mathcal{O}$ and $\tilde{S}(x_{\mathcal{O}}+1)$ is unique, then the height of $S(x_{\mathcal{O}})$ can be recovered by obtaining from $\tilde{S}(x_{\mathcal{O}}+1)$. For example, in Fig. 3.4(b), the height of $\tilde{S}_d(18)$ can be obtained from $\tilde{S}_d(19)$, which is 1. Since $\tilde{S}_d(19) = S_d(18)$, then the height of $S_d(18)$ is recovered.

3. In fact, echoes avoided by Hidden Surface Removal are Type 2. Our method is similar to HSR in a sense that some copying steps are removed to avoid overlappings. However, we have proven that HSR indeed removes excessive amounts of copying steps in a sense that copying steps which do not cause overlapping are also removed. This results in visual artifacts if the positions, of which copying steps are unnecessarily removed, are not strictly hidden (i.e. visible) to the viewers. The proof is stated in Appendix A.

3.4 Autostereogram Encoding Any Surface

We have seen from the previous section that, for some surfaces, the depth information of some positions on the original surfaces are lost due to the avoidances of

Type 2 echoes. The lost depth information is nevertheless recoverable, if the surfaces satisfy certain criterion as shown in the previous section. Otherwise, the lost depth information is not recoverable, and we have no way to reconstruct the original surfaces exactly. This definitly limits the prospects of autostereograms. We believe that the prospects of autostereograms can be widened if the exact reconstruction of *any* original surface from autostereogram is proven feasible.

Since avoidance of Type 2 echoes result in losses of depth information, here we do not suppress overlappings of copying steps. But we will show that any echo of Type 2 can be nonetheless made distinguishable from the original surfaces $S(x)$, so that the original surfaces can be figured out unambiguiously. But we indeed suppress Type 1 echoes.

Let $x_1, x_2 \in \mathbf{X}$ be the x-coordinates of autostereograms $R(x)$ such that $x_2 < x_1$. Suppose x_1 and x_2 are the corresponding positions and the value of $R(x_1)$ is copied from $R(x_2)$, hence x_2 is

$$x_2 = x_1 - \sigma_g(S(x_1)). \tag{3.18}$$

for all IS-separations $\sigma_g \in \Sigma(g)$

First of all, we aim at finding the possible values of IS-separation $\sigma_g(S(x_1))$ under condition 3.8 of Type 1 echo avoidance. Since σ_g are s.m.d., thus IS-separations for $S(x_1)$ are bounded such that

$$\sigma_g(\bar{s}_e) \leq \sigma_g(S(x_1)) \leq \sigma_0. \tag{3.19}$$

By condition 3.8, to suppress Type 1 echoes, we limit the maximum heights $\bar{s}_e$ of the original surfaces such that

$$\bar{s}_e < g^{-1}\left(D_S - \frac{2D_R}{1 + D_R(D_S - g_0)^{-1}}\right) \tag{3.20}$$

for all s.m.i. g. Furthermore, by the monotonic property of IS-separations, we get

$$\sigma_g(\bar{s}_e) > \sigma_g\left(g^{-1}\left(D_S - \frac{2D_R}{1 + D_R(D_S - g_0)^{-1}}\right)\right) \tag{3.21}$$

$$= \sigma_0/2. \tag{3.22}$$

Finally, substituting Eq. 3.22 into Eq. 3.19, the possible values of IS-separations $\sigma_g(S(x_1))$ are

$$\sigma_0/2 < \sigma_g(S(x_1)) \leq \sigma_0. \tag{3.23}$$

Next, we show that $R(x_2)$ copied by $R(x_1)$ is indeed the pre-defined patterns $\Pi(x_2)$ under an assumption on x_s. By the results in the previous paragraph and Eq. 3.18, the possible x_2 are

$$x_1 - \sigma_0 < x_2 \leq x_1 - \sigma_0/2. \tag{3.24}$$

For a special case, let x_1 to be the rightmost position on the autostereogram $R(x)$, i.e. $x_1 = x_s$. Therefore, Eq. 3.24 becomes

$$x_s - \sigma_0 < x_2 \leq x_s - \sigma_0/2. \tag{3.25}$$

This situation is shown in Fig. 3.5. The arrows on the left and the right show the copying steps of the maximum and minimum value of x_2, respectively. Actually, the crucial element for the following derivation is x_s. Assume that $x_s \leq \frac{3}{2}\sigma_0$, then from Eq. 3.25, the possible x_2 are

$$1 \leq x_2 \leq \sigma_0. \tag{3.26}$$

Finally, as seen from Eq. 2.6, $R(x_2)$ are the pre-defined patterns, i.e.

$$R(x_2) = \Pi(x_2) \tag{3.27}$$

for all $1 \leq x_2 \leq \sigma_0$.

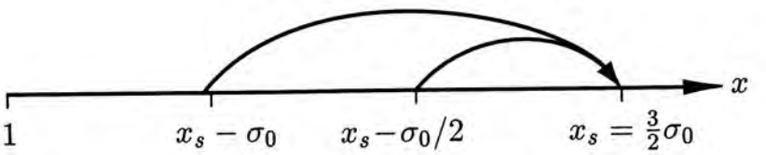


Figure 3.5: Illustration for Eq. 3.25.

Using the above results, we now show that Type 2 echoes are distinguishable from the original surfaces $S(x)$, under the assumption that $x_s \leq \frac{3}{2}\sigma_0$. Since predefined patterns $\Pi(x)$ are horizontally uncorrelated, false matches only occur in the interval $(\sigma_0, x_s]$. The distance between any pair of falsely matched positions is $0 < d < x_s - \sigma_0 = \sigma_0/2$. Since echoes are reconstructed surface segments, they can be determined using the surface reconstruction formula in Eq. 2.9. Denoted by $\tilde{S}_e(x)$, the echoes are

$$\tilde{S}_e(x) = \sigma_g^{-1}(d) \tag{3.28}$$

for $0 < d < \sigma_0/2$. By the monotonic property of $\sigma_g(s)$, we have

$$\sigma_g^{-1}(\sigma_0/2) < \tilde{S}_e(x) < \sigma_g^{-1}(0). \tag{3.29}$$

Finally, the echoes $\tilde{S}_e(x)$ are bounded by

$$\bar{s}_e < \tilde{S}_e(x) < \bar{s}. \tag{3.30}$$

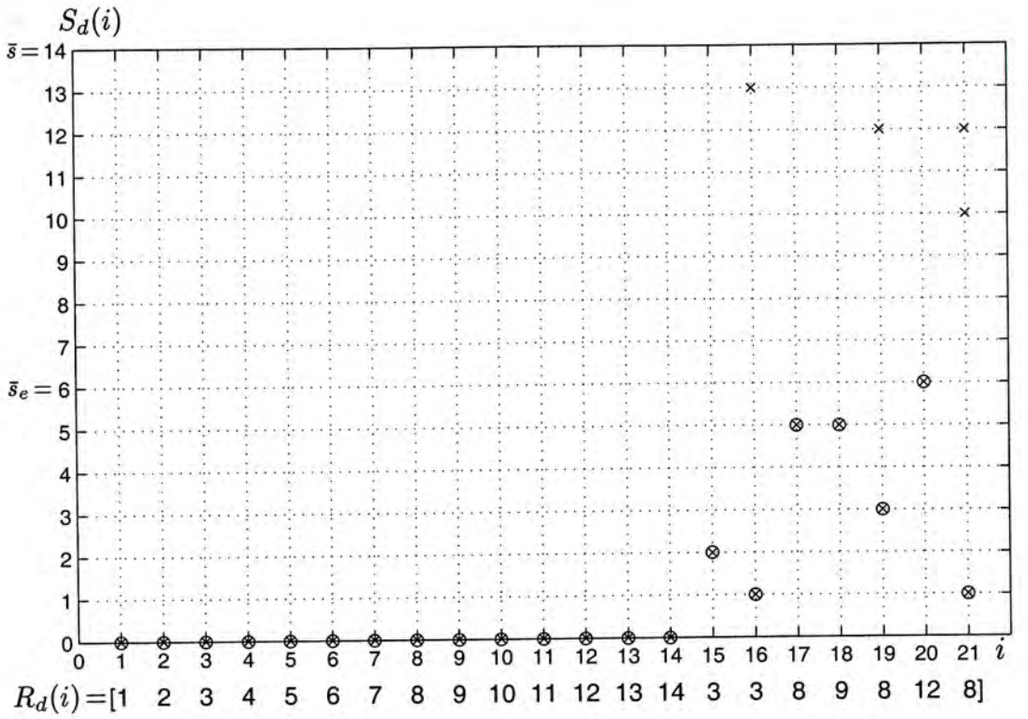
Since the attained heights of the original surfaces are $1 \leq S(x) \leq \bar{s}_e$, then the echoes $\bar{s}_e < \tilde{S}_e(x) < \bar{s}$ are nowhere lower than original surfaces $S(x)$, so that they can be distinguished from them. An example is shown to demonstrate the idea.

Example 3.3. In this example, we demonstrate that an arbitrary surface $S_d(i)$ can be exactly reconstructed from discrete autostereogram $R_d(i)$ by setting L_1 sufficiently large. Echoes of Type 1 are avoided by setting the maximum height ($\bar{s}_e = 6$) smaller than half of the upper bound ($\bar{s} = 14$). To make Type 2 echoes distinguishable, we set $L_1 = 21$ which is equal to $\frac{3}{2}\sigma_0 = 21$. Consequently, Type 2 echoes

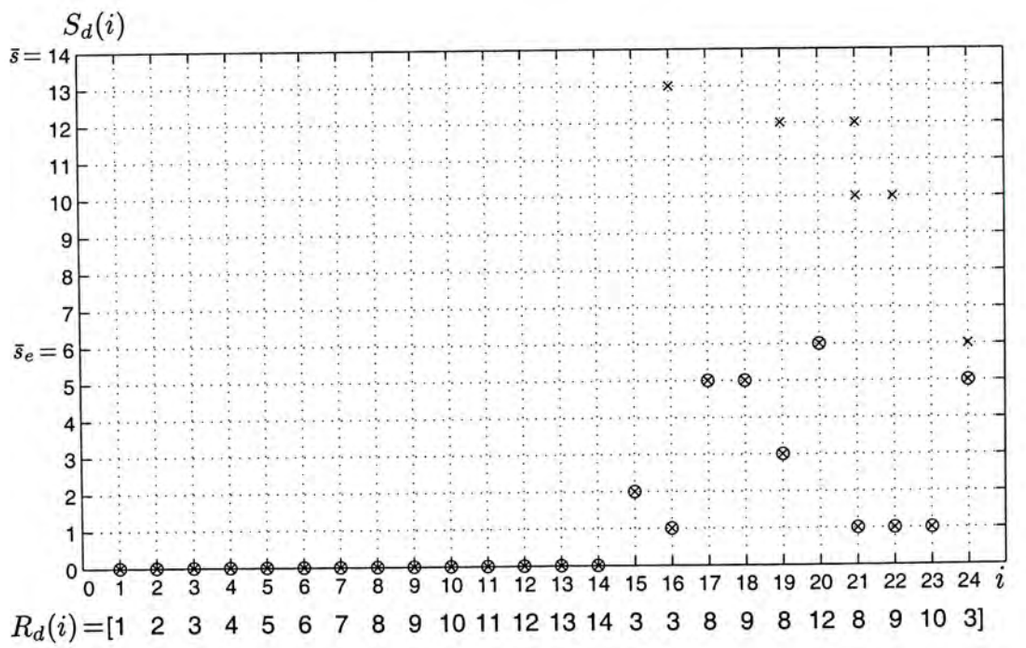
are forced to appear at the heights greater than $\bar{s}_e$ for all i. Thus, original surface $S_d(i)$ can be recovered by just taking the reconstructed surface segments having the heights smaller than or equal to $\bar{s}_e = 6$.

Finally, we demonstrate how digital gray images can be encoded in autostereograms, which in turn can be exactly reconstructed.

Example 3.4. Images are two-dimensional functions. As mentioned, by considering the intensity (or grayscale) as the height of surfaces, images can be indeed encoded in autostereograms. Using the technique described above, any encoded image can be exactly reconstructed to the original one. This is demonstrated in Fig. 3.7. The digital image shown in Fig. 3.7(a) consists of 255×255 pixels. For the image used in this example, the grayscales of the pixels are in 256 (from 0 to 255) quantized levels, hence we let $\bar{s}_e = 255$. Then, we let the bound $\bar{s} = 512 > 2\bar{s}_e$. We adopt IS-separation σ with the bound $\bar{s} = E$, therefore the IS-separations are computed using $\sigma(S_d(i,j)) = E - S_d(i,j)$. To ensure that the encoded surface $S_d(i,j)$ can be exactly reconstructed, we let $L_1 = \frac{3}{2}\sigma_0 = \frac{3}{2} = 768$. Consequently, the resulting autostereogram $R_d(i,j)$, as shown in Fig. 3.7(b) is an image consisting of 768 pixels. As expected, the original image can exactly reconstructed.



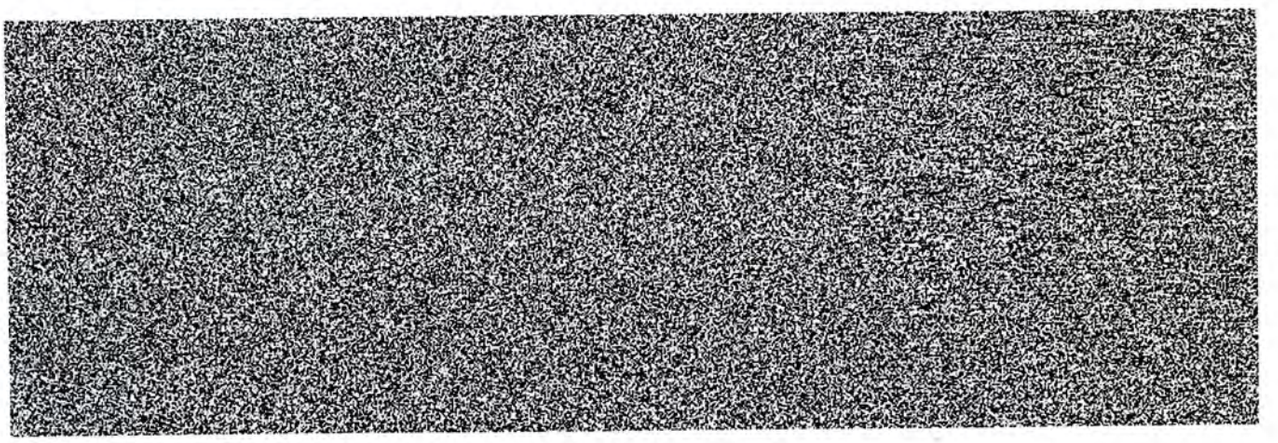
(a)



(b)

Figure 3.6: Demonstrating exact reconstruction of surface; (a) echoes are distinguishable from the original surface $S_d(i)$ when $L_1 = 21$; (b) echoes are indistinguishable when $L_1 = 24 > 3/2\sigma_0$.

(a)



(b)

Figure 3.7: Demonstrating image encoding using autostereogram (not to scale). (a) The image being encoded; (b) the autostereogram encoding the image in Fig. 3.7, which can be uniquely reconstructed.

Chapter 4

Autostereogram as A Cryptosystem

Seeming to be pieces of completely scrambled data, autostereograms appear to be meaningless to the observers. Moreover, the contents of autostereograms are, in some extent, independent of the surfaces being encoded. These features indeed are attractive for cryptographic applications, in which secret messages are encoded such that unauthorized receivers are unable to read them.

A crucial requirement for all cryptosystems is that the original messages can be uniquely reconstructed at the recipients' end using the keys. Otherwise, the reconstructed messages are ambiguous. We have shown in Chapter 3 that any original surface can be exactly reconstructed from the autostereogram under some conditions. We may consider the process to encode surfaces into the autostereograms as an encoding function, which have an unique inverse such that the original surfaces can be exactly reconstructed. When the secret messages are represented by the original surfaces, we will show that autostereogram ensembles an cryptosystem.

In this chapter, we show how autostereograms can be applied in cryptography. The first section is devoted to the introductions of cryptography, the mathematical structure and a classical cryptosystem, namely *Substitution Cipher*. Examples are

given to illustrate the notions. Afterwards, we show that by using the technique in Section 3.4, autostereograms are obtained by the function Π of the pre-defined patterns taking the co-ordinates and the values of IS-separations as the arguments. If function Π is one-to-one, then the original surfaces can be exactly reconstructed by the inverse function Π^{-1}. We show that autostereograms fit the mathematical structure of cryptosystems. Furthermore, we demonstrate that autostereogram indeed is a variation of Substitution Cipher. Finally, we discuss various issues in applying autostereogram as an cryptosystem, including the security, key managements and encryption/decryption computations.

4.1 Introduction to Cryptography

Cryptography is a technology of encoding secret information so that it cannot be read by an unauthorized person. The information, known as *plaintext*, consists of discrete symbols of a finite set, which can be English alphabets or numerical data for instance. The act of converting plaintext into code or *ciphertext* using a key, so that an unauthorized person is unable to read, is called *encryption*. The key is needed to decode or *decrypt* the ciphertext back to the plaintext. Some of the earliest use of cryptography date back to the fifth century BC [8].

The schematic diagram of a general cryptosystem is shown in Fig. 4.1. The key source produces a particular key from among those possible in the system. Plaintext produced by the sender is encrypted using this key to produce the ciphertext which is then sent over an insecure channel to the recipient. The key is delivered to the recipient's end by a secure method, which is supposed to be not interceptible. Upon receiving the ciphertext, the recipient decrypt the ciphertext using this key to the plaintext. In the insecure channel, the opponent or enemy may have been

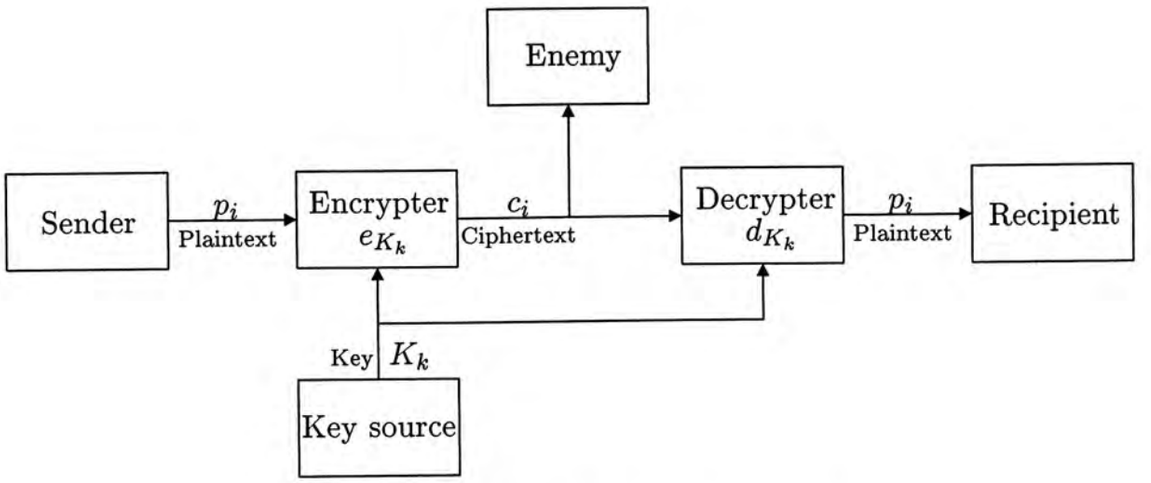


Figure 4.1: A general cryptosystem.

intercepted the ciphertext. However, if the system is secure, the enemy have no way to reconstruct the plaintext in some senses.

4.1.1 Mathematical Structure of Cryptosystems

The notions of cryptosystems can be formally formulated. Let

1. $\mathcal{P}$ be a finite set of plaintext;
2. $\mathcal{C}$ is a finite set of ciphertext; and
3. $\mathcal{K}$ is a finite set of key.

For each $K \in \mathcal{K}$, there exists an encryption function $e_K : \mathcal{P} \to \mathcal{C}$ and a corresponding decryption function $d_K : \mathcal{C} \to \mathcal{P}$ such that $d_K(e_K(p)) = p$ for every plaintext $p \in \mathcal{P}$. Suppose there are n possible keys $K_k \in \mathcal{K}$ for $k = 1, 2, \ldots, n$, then the n encryption functions e_{K_k} forms a family of function $e_{\mathcal{K}}$. Similarly, the n corresponding decryption functions d_{K_k} forms a family of functions $d_{\mathcal{K}}$. Each key K_k is associated with a priori probability Pr_k such that key K_k is chosen with probability Pr_k.

Suppose two parties, namely the sender and the recipient want to communicate secretly through an insecure channel. A particular key K_k is generated by the key

source with a prior probability Pr_k. The key K_k is known only to the sender and the recipient. The knowledge of the key is kept secretly from the opponent by accessing a secure channel which is assumed to be uninterceptible.

Suppose the message communicating between the sender and the recipient is a concatenation of l plaintext symbols $p_i \in \mathcal{P}$, i.e.

$$\mathbf{p} = p_1 p_2 p_3 \cdots p_l \tag{4.1}$$

for some integer $l > 0$. Before sending to the recipient, message $\mathbf{p}$ is encrypted using the encryption function e_{K_k} to produce the cipher message $\mathbf{c}$ using the encryption function e_{K_k}. Then, the cipher message $\mathbf{c}$ is

$$\mathbf{c} = c_1 c_2 c_3 \cdots c_l \tag{4.2}$$

where $c_i = e_{K_k}(p_i)$ for $i = 1, 2, \ldots, l$. The resulting cipher message $\mathbf{c}$ is sent over the insecure channel. Upon receiving, the recipient decrypt the cipher message $\mathbf{c}$ using the decryption function d_{K_k} to recover the original message $\mathbf{p}$, such that

$$p_i = d_{K_k}(c_i) \tag{4.3}$$

for $i = 1, 2, \ldots, l$.

Clearly, the ciphertexts have to be uniquely reconstruct to the plaintexts by the recipient without any ambiguity. Therefore, we may consider the decryption function d_{K_k} as the unique inverse of the encryption function e_{K_k} for all $k = 1, 2, \ldots, n$. Then, e_{K_k} is a one-to-one mapping.

4.1.2 A Classical Cryptosystem—Substitution Cipher

In this section, we introduce a classical cryptosystem, namely Substitution Cipher, which has been used for hundreds of years. The notions of this cryptosystem will be

useful in the following sections. Nevertheless, there are several other cryptosystems worth discussing for introductory purposes, reader may refer to [6].

For simplicity, the index k and i in the notations K_k, p_i and c_i are skipped in the following discussions. Then, the symbol K refers to a particular key drawn from $\mathcal{K}$ unless specified. Similarly, the symbols p and c refer, respectively, to a particular plaintext symbol and cipher symbol.

Before introducing the cryptosystem, we first define the set $\mathbf{Z}_m$ to be the set $\mathbf{Z}_m$ containing m discrete symbols $z_0, z_1, \ldots, z_{m-1}$, i.e. $\mathbf{Z}_m = \{z_0, z_1, \ldots, z_{m-1}\}$. The symbols z_i can be English alphabets or numerical data. For instance, if the symbols are English alphabets, disregarding the cases, we have $\mathbf{Z}_m = \{A, B, \ldots, Z\}$. We can nevertheless set up the following correspondences between English alphabets and integers: $A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$; in this case, set $\mathbf{Z}_m$ of English alphabets is equivalent to the set of integers $\mathbf{Z}_m = \{0, 1, \ldots, 25\}$.

Substitution Cipher

We are now ready to introduce Substitution Cipher. Let the sets of plaintexts and ciphertexts be set $\mathbf{Z}_m$ of discrete symbols, so that we have $\mathcal{P} = \mathcal{C} = \mathbf{Z}_m$. The key $K \in \mathcal{K}$ is a permutation function $\pi : \mathbf{Z}_m \to \mathbf{Z}_m$. For a particular key $\pi \in \mathcal{K}$ and any plaintext $p \in \mathcal{P}$, the ciphertext c is obtained by encryption function e_π such that $c = e_\pi(p)$. For Substitution Cipher, we let the encryption e_π be the permutation π; hence, the ciphertexts are

$$c = \pi(p) \tag{4.4}$$

for all $c \in \mathcal{C}$, $p \in \mathcal{P}$.

Upon receiving, the plaintext p is uniquely reconstructed from the ciphertext c by the decryption function d_π such that $p = d_\pi(c)$. In fact, the decryption function

is the inverse permutation π^{-1}, hence

$$p = \pi^{-1}(c) \tag{4.5}$$

for all $p \in \mathcal{P}$, $c \in \mathcal{C}$.

Example 4.1. Here is an example of Substitution Cipher. Suppose $m = 25$ and $\mathbf{Z}_{25}$ is the set of English alphabets. As a convention, plaintext symbols are written in lower case while ciphertext symbols are written in upper case. Suppose the sets of plaintexts and ciphertexts are, respectively, $\mathcal{P} = \{a, b, c, \ldots, z\}$ and $\mathcal{C} = \{A, B, C, \ldots, Z\}$. Let $\pi \in \mathcal{K}$ be a permutation function $\pi : \mathbf{Z}_{25} \to \mathbf{Z}_{25}$. Suppose a particular key $\pi \in \mathcal{K}$ is generated such that for all $p \in \mathcal{P}$

p	a	b	c	d	e	f	g	h	i	j	k	l	m
$\pi(p)$	K	M	G	J	X	Y	H	L	C	N	O	D	Z
p	n	o	p	q	r	s	t	u	v	w	x	y	z
$\pi(p)$	F	R	Q	B	U	W	P	E	S	A	T	V	I

(4.6)

Thus, the encryption function is $e_\pi = \pi$, so that $e_\pi(a) = K, e_\pi(b) = M, \ldots, e_\pi(z) = I$.

Suppose the following message

$$\mathbf{m} = thisisasubstitutioncipher \tag{4.7}$$

is to be sent to the recipient secretly over an insecure channel. By Eq. 4.6, the message $\mathbf{m}$ is encrypted to a cipher message $\mathbf{c}$

$$\mathbf{c} = PLCWCWKWEMWPCPEPCRFGCQLXU. \tag{4.8}$$

Upon receiving the cipher message $\mathbf{c}$, it is decrypted by the recipient using the decryption function d_π which is simply the inverse permutation π^{-1}. Thus, for all ciphertext $c \in \mathcal{C}$

c	K	M	G	J	X	Y	H	L	C	N	O	D	Z
$\pi^{-1}(c)$	a	b	c	d	e	f	g	h	i	j	k	l	m
c	F	R	Q	B	U	W	P	E	S	A	T	V	I
$\pi^{-1}(c)$	n	o	p	q	r	s	t	u	v	w	x	y	z

(4.9)

By using Eq. 4.9, the recipient can exactly recover the plaintext message **p** from the cipher message **c**.

From this example, we see that each plaintext is mapped to a unique ciphertext. For that reason, Substitution cipher is called *monoalphabetic*.

Cryptanalysis

The attack to determine the key that was used for the ciphertexts in a cryptosystem is know as *cryptanalysis*. If the opponent has made a successful attack on the cryptosystem to reveal the key being used, he or she can uniquely decrypt the ciphertexts as the recipients do. Usually, it is assumed that the opponent knows the cryptosystems being used. Cryptanalysis techniques have been proposed for different types of cryptosystems.

In fact, it is well known that Substitution Cipher is vulnerable to *frequency analysis* (see [1] and [6] for details). Suppose the opponent knows the possible plaintext symbols being used in the cryptosystem; and he or she has the knowledge of the probability distribution of the occurrences of such plaintext symbols. We clarify that using English alphabets as an example. For English Language, it has been reported by Beker and Piper that for instance, "E" have the probability of occurrence about 0.120; and both probabilities for "D" and "L" are around 0.040. Suppose the alphabet "E" appears most frequently. In the insecure channel, the opponent has observed the ciphertexts and performed frequency analysis on them. If it is found that the probability of occurrence of a cipher symbol, say c_0, resembles that of "E", he or she may guess that the ciphertext c_0 corresponds to "E" in the

cryptosystem. Other correspondences can be found using similar technique. If the observed cipher message is long enough, the key of permutation can be uniquely determined.

Indeed, the power of such frequency analysis depends on the entropy of the plaintexts. The higher the entropy is, the more the opponent is uncertain about the occurrences of symbols. Hence, the power of such attack decreases as the entropy grows.

4.2 Autostereogram as a Cryptosystem

In this section, first of all, we extend the results in Chapter 3. We show that under the conditions stated in Section 3.4, autostereograms $R(x)$ can be obtained by function Π of the pre-defined patterns taking the co-ordinates and the values of IS-separations as the arguments. Using this result, we show that autostereogram is a variation of Substitution Cipher. Also, issues regarding this variation is discussed.

In the followings, we aim at the exact reconstruction of *any* discrete original surface $S_d(i)$ from autostereogram $R_d(i)$. To accomplish that, the following assumptions have to be made. First of all, IS-separation σ should be adopted in order to avoid the truncation problem. Further, we assume bound $\bar{s}$ is equal to the eye separation E, i.e. $\bar{s} = E$. Thus, the expression for IS-separations is

$$\sigma(S_d(i)) = E - S_d(i) \tag{4.10}$$

for all $i = 1, 2, \ldots, L_1$; and the IS-separations at zero height is $\sigma_0 = \sigma(0) = E$.

Secondly, we have to guarantee that any original surface $S_d(i)$ can be uniquely reconstructed without any loss due to avoidance of Type 2 echoes. By Section 3.4, length L_1 of the autostereogram is restricted such that $L_1 \leq \frac{3}{2}\sigma_0 = \frac{3}{2}E$. Furthermore, Type 1 echoes are avoided by restricting the maximum height $\bar{s}_e$ of $S_d(i)$ such

that $\bar{s}_e < \bar{s}/2$.

With those recipes, we now move to the main part of the derivation. From Eq. 2.35, autostereograms $R_d(i)$ are generated by

$$R_d(i) = R_d\big(i - Q_I\big[\sigma(S(i))\big]\big) \tag{4.11}$$

for $i = E+1, \ldots, \frac{3}{2}E$. We assume E is an integer, and substitute Eq. 4.10 into Eq. 4.11, which becomes

$$\begin{aligned} R_d(i) &= R_d\big(i - Q_I\big[E - S_d(i)\big]\big) && (4.12)\\ &= R_d(i - E + S_d(i)). && (4.13) \end{aligned}$$

But the argument $i - E - S_d(i)$ on the right hand side of Eq. 4.13 is confined such that

$$1 \leq i - E + S_d(i) < E \tag{4.14}$$

for the fact that $0 \leq S_d(i) \leq \bar{s} < E/2$ for all $E+1 \leq i \leq \frac{3}{2}E$. Since the leftmost positions of autostereograms $R_d(i)$ are the pre-defined patterns, i.e. $R_d(i) = \Pi(i)$ for $i = 1, 2, \ldots, E$, thus we have

$$R_d(i - E + S_d(i)) = \Pi(i - E + S_d(i)). \tag{4.15}$$

Finally, by Eq. 4.13, the autostereograms $R_d(i)$ are

$$R_d(i) = \Pi(i - E + S_d(i)) \tag{4.16}$$

for $i = E+1, E+2, \ldots, \frac{3}{2}E$. In this case, the autostereograms $R_d(i)$ are indeed the images of function Π. If Π is a one-to-one mapping, original surface can be uniquely reconstructed by

$$S_d(i) = \Pi^{-1}\big(R_d(i)\big) + E - i. \tag{4.17}$$

for all $i = E+1, E+1, \ldots, \frac{3}{2}E$.

4.2.1 Autostereogram as a Variation of Substitution Cipher

Suppose the function Π of pre-defined pattern is a one-to-one mapping, such that Π maps each $z \in \mathbf{Z}_{E-1}$ to a unique element of its image. Clearly, the pre-defined pattern Π is horizontally uncorrelated if and only if it is one-to-one. Further assume that the image of Π is also $\mathbf{Z}_{E-1}$, i.e.

$$\Pi : \mathbf{Z}_{E-1} \rightarrow \mathbf{Z}_{E-1}. \tag{4.18}$$

Under such assumptions, Π is a permutation function of the set $\mathbf{Z}_{E-1}$.

Suppose the message $\mathbf{p}$ to be communicated between the sender and recipient is somehow represented in $S_d(i)$. Let $p_i \in \mathcal{P}$ and $c_i \in \mathcal{C}$ be the plaintexts and ciphertexts of the proposed cryptosystem, such that

$$p_i = i + S_d(i + E), \quad \text{and} \quad c_i = R_d(i + E) \tag{4.19}$$

for all $i = 1, 2, \ldots, E/2$. Consequently, we have

$$\begin{aligned} c_i &= R_d(i + E) && (4.20)\\ &= \Pi(i + S_d(i + E)) && (4.21)\\ &= \Pi(p_i) && (4.22) \end{aligned}$$

for $i = 1, 2, \ldots, E/2$. The steps from Eq 4.20 to Eq. 4.21 are evident in Eq. 4.16.

From the definition of the plaintexts p_i shown in Eq. 4.19, there are $E-1$ possible values of p_i (which are $1, 2, \ldots, E-1$). Thus, we let the set of plaintext be $\mathcal{P} = \mathbf{Z}_{E-1}$. Furthermore, from Eq. 4.22, c_i belong to the image of Π, which is $\mathbf{Z}_{E-1}$; hence, the set of ciphertext is again $\mathcal{C} = \mathbf{Z}_{E-1}$. Let the permutation function $\Pi \in \mathcal{K}$ be the key of the cryptosystem. For each permutation Π, we define the encryption function and decryption function, respectively, as

$$e_\Pi(p_i) = \Pi(p_i), \tag{4.23}$$

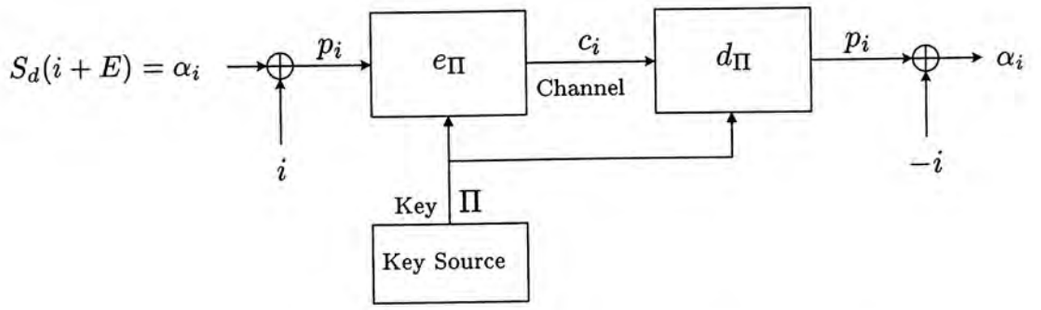


Figure 4.2: Schematic diagram of Substitution Cipher using autostereograms.

$$d_\Pi(c_i) = \Pi^{-1}(c_i) \tag{4.24}$$

for all $i = 1, 2, \ldots, E/2$.

Clearly, autostereogram $R_d(i)$ is a variation of Substitution Cipher. The schematic diagram of the cryptosystem using autostereograms is shown in Fig. 4.2. Under this scheme, the data α_i to be communicated with the recipient is represented in $S_d(i)$ such that $S_d(i+E) = \alpha_i$ for all $i = 1, 2, \ldots, E/2$. The plaintexts p_i are obtained by adding i to $S_d(i+E)$, i.e. $p_i = i + S_d(i+E)$. For a particular key Π generated by the key source, the plaintexts p_i are encrypted by the encryption function e_Π to obtain the ciphertexts c_i, which are transmitted over the channel to the recipient. At the recipient's side, the ciphertexts c_i are decrypted back to the plaintexts p_i by decryption function d_Π. The data α_i is then extracted from p_i by $\alpha_i = p_i - i$.

Example 4.2. Suppose the message to be transmitted by sender to the recipient is

thisisamessage.

By using the correspondences of integer numbers and English alphabets, the message can be rewritten as an array

$$[\ 19\ \ 7\ \ 8\ \ 18\ \ 8\ \ 18\ \ 0\ \ 12\ \ 4\ \ 18\ \ 18\ \ 0\ \ 6\ \ 4\ ].$$

Then, each entry of the array is represented such that

$$S_d(1) = 0,\ S_d(2) = 0,\ \ldots,\ S_d(E+1) = 19,\ S_d(E+2) = 7,\ \ldots,\ S_d(14+E) = 4.$$

Since the maximum number corresponding to English alphabet "z" is 25, therefore the maximum value of $S_d(i)$ is $\bar{s}_e = 25$. We let $E = 52$ so that $\bar{s}_e < E/2$ holds. Let the sets of plaintext $\mathcal{P}$ and ciphertext $\mathcal{C}$ be the set of discrete symbols $\mathbf{Z}_{51}$. Then, the key $\Pi \in \mathcal{K}$ is the permutation function $\Pi : \mathbf{Z}_{51} \to \mathbf{Z}_{51}$.

By Eq. 4.19, the plaintexts p_i are

$$p_i = i + S_d(i + 52) \tag{4.25}$$

for all $i = 1, 2, \ldots, E/2 = 25$. Then, the plaintext message to be encrypted by the encryption function e_Π is the concatenation of p_i, i.e.

$$\mathbf{p} = \begin{array}{cccccccccccccc} 20 & 9 & 11 & 22 & 13 & 24 & 7 & 20 & 13 & 28 & 29 & 12 & 19 & 18 \end{array}. \tag{4.26}$$

Suppose the key is the permutation Π such that for any plaintext p_i

p_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\Pi(p_i)$	13	26	1	15	27	11	38	3	19	47	14	29	6	39	16	2	37
p_i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$\Pi(p_i)$	28	17	40	22	48	30	42	4	36	18	5	31	41	46	43	23	7
p_i	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
$\Pi(p_i)$	34	24	8	32	20	9	45	49	12	35	0	33	25	10	50	44	21

(4.27)

Then, the ciphertexts are obtained by the encryption function $e_\Pi = \Pi$. The cipher message is

$$\mathbf{c} = \begin{array}{cccccccccccccc} 22 & 47 & 29 & 30 & 39 & 4 & 3 & 22 & 39 & 31 & 41 & 6 & 40 & 17 \end{array}. \tag{4.28}$$

Upon receiving at the recipient side, the plaintext message can be obtained using the decryption function d_Π which is the inverse permutation Π^{-1}. Finally, the original data can be read by subtracting i from the plaintexts p_i.

4.2.2 Practical Considerations

1. In the proposed cryptosystem, the sets of plaintexts and ciphertexts are the set of $E-1$ discrete symbols, i.e. $\mathcal{P} = \mathcal{C} = \mathbf{Z}_{E-1}$. In order to avoid Type 1 echoes,

the maximum value $\bar{s}_e$ of $S_d(i)$ is restricted such that $\bar{s}_e < E/2$. Therefore, the possible values of data are $\alpha_i = 0, 1, 2, \ldots, E/2 - 1$ which accounts less than half of the size of $\mathcal{P}$. The extra plaintext symbols in $\mathcal{P}$ are due to the redundant information of i carried by the plaintext p_i, where by Eq. 4.19,

$$p_i = i + S_d(i + E)$$

for $i = 1, 2, \ldots, E/2$. Therefore, the number of possible plaintexts is $E - 1$

2. One of the drawbacks of item 1 is the increase in key length. We can consider the permutation Π and inverse permutation Π^{-1} in Example 4.2 as arrays

$$\Pi = \begin{bmatrix} 13 & 26 & 1 & 15 & 27 & 11 & 38 & \cdots \end{bmatrix}, \tag{4.29}$$

$$\Pi^{-1} = \begin{bmatrix} 44 & 2 & 15 & 7 & 24 & 27 & 12 & \cdots \end{bmatrix} \tag{4.30}$$

such that $p_i = \Pi^{-1}\big[\Pi[p_i]\big]$ for all $p_i \in \mathcal{P}$. Then length of the key is the length of the array Π. Since the length of Π equals to the size of $\mathcal{P}$ and $\mathcal{C}$, therefore, the problem mentioned in remark 1 leads to unnecessary increases of the key length. But in fact, the number of possible key grows with the key length, which increases the average amount of ciphertext required for an enemy to be able to uniquely compute the key using techniques as such frequency analysis. The amount of such ciphertext is known as the *unicity distance* of the cryptosystem. Nevertheless, increasing key length induces key management problems. Such problems can be evident from a cryptosystem known as *One Time Pad.* Though it has been proven to be theoretically secure, it has limited use in commercial applications.

3. For each key Π, the maximum length L_1 of the autostereogram $R_d(i)$ encoding $S_d(i)$ is restricted to be smaller than or equal to $3/2E$. Otherwise, Type 2

echoes are not distinguishable from the original surface $S_d(i)$. For messages longer the $3/2E$ symbols, they have to be split up into several sub-messages and encrypted individually with different keys before transmission.

4. Since the proposed cryptosystem is a variation of Substitution Cipher, the security analysis of Substitution Cipher can be applied. A well known cryptanalysis of Substitution Cipher is the frequency analysis. Nevertheless, i carried in the plaintext p_i increases the difficult of such cryptanalysis, in sense that the entropy of the plaintext is increased. The entropy can be further increased by a permutation of i so that

$$p_i = \hat{\Pi}(i) + S_d(i + E).$$

However, the additional permutation $\hat{\Pi}$ worsens the key management problems.

Chapter 5

Conclusion and Future Works

In this thesis, various aspects of autostereograms are studied. By using a new configuration to generate autostereograms, a general expression for IS-separations have been obtained. We have proposed an expression for IS-separations, which is advantageous to computer generations and echo analysis. A new algorithm for autostereogram generations and surface reconstructions have been proposed, which is better than the conventional methods in terms of computer generations and echo avoidance due to the incorporation of the proposed IS-separation. Then, the visual distortions of the perceived surfaces have been studied. We have observed that there are two types of distortions, namely vertical and lateral distortions. The relations between the parameters and the visual distortions have been obtained. In addition, the problem of echo has been studied. We have categorized echoes into Type 1 and Type 2, which are caused by, respectively, insufficient lengths of periods of the repeating patterns and overlappings of copying steps. Accordingly, conditions have been derived to avoid them. Further, we have imposed restrictions on the generations of autostereograms such that any original surfaces can be exactly reconstructed from autostereograms. We have demonstrated that autostereogram can be applied in image coding, from which any encoded image can be uniquely

reconstructed. Finally, we have extended the application of autostereogram to cryptography. We have shown that under some conditions, autostereogram is indeed a variation of Substitution Cipher. Issues regarding this application have been posted and discussed.

5.1 Future Works

- The security aspects of the proposed cryptosystem using autostereograms have not been addressed. The studies on the security issues are significant for evaluating the usefulness of this cryptosystem. Further, although key management seems to be a problem, it is nevertheless worth investigating for the other variations of this cryptosystem, which may find useful in other areas.

- We have noted that pre-defined patterns have influences on the quality of the perceived surfaces. When the same original surfaces and parameters are used, some patterns seem to have poorer quality than others, which appear to be corrupted with "noise". We guess that this problem relates to the characteristics of the human visual systems such as frequency and luminance sensitivity. It will be significant if the relations between such characteristics and the quality of the perceived surfaces are revealed. This helps in creating visually pleasant autostereograms in a more systematic way.

- In this thesis, the distortions are analyzed on a functional level, without considering the psychological aspects on the problem. We believe that the human visual system have certain tolerances, such that the original surfaces, in most of the case, can be recognized from the perceived surfaces easily. But the study of the problem is nevertheless beneficial to both autostereogram and vision research communities.

Appendix A

Excessive Removal of Copying Steps

The followings are based on the autostereogram generation algorithm developed in [10]. We show that, under Hidden Surface Removal, some copying steps are unnecessarily removed to avoid overlapping of copying steps. To simplify discussions, one-dimensional case is considered.

Referring to Section 1.2, as suggested in [10] point $x \in \mathbf{X}$ on a surface $S(x)$ is hidden to the viewer if and only if there exist a point $x^* \in \mathbf{X}$ such that

$$S(x^*) - S(x) \geq \frac{2\,|x^* - x|\,(D_S - S(x))}{E}. \tag{A.1}$$

After rearranging the terms, Eq. A.1 becomes

$$|x^* - x| \leq \frac{E\,(S(x^*) - S(x))}{2(D_S - S(x))}. \tag{A.2}$$

Since $|x^* - x| > 0$, therefore the right hand side of Eq. A.2 is always positive. Hence, it can be inferred that $S(x^*) > S(x)$ when the copying steps of position x^* and x overlap. Assuming $S(x^*) > S(x)$, let us consider the following two cases:

Case One

Assume $x^* < x$, and condition of Eq. A.2 becomes

$$x - x^* \leq \frac{E\left(S(x^*) - S(x)\right)}{2(D_S - S(x))} \tag{A.3}$$

for all $x \in \mathbf{X}$.

Case Two

Assume $x^* > x$, and condition of Eq. A.2 becomes

$$x^* - x \leq \frac{E\left(S(x^*) - S(x)\right)}{2(D_S - S(x))} \tag{A.4}$$

for all $x \in \mathbf{X}$.

If the autostereograms are generated from left to right, increasing surfaces do not cause overlapping of copying step, and hence Type 2 echoes do not appear. Therefore, the removal of the copying steps in case two will be nevertheless unnecessary.

In the algorithm developed in [10], to encode $S(x)$, the value of $S(x-\sigma_g(S(x))/2)$ is copied to $S(x+\sigma_g(S(x))/2)$. Using a similar argument in Section 3.3, the copying steps of x^* and x overlap if and only if there exist $x^* < x$ such that

$$x - \frac{\sigma_g(S(x))}{2} = x^* - \frac{\sigma_g(S(x^*))}{2}, \tag{A.5}$$

or,

$$x - x^* = \frac{E\left(S(x^*) - S(x)\right)}{2(D_S - S(x))} \times \frac{D_R}{D_S - S(x^*)} \tag{A.6}$$

for all $x \in \mathbf{X}$.

In particular, let $x_\mathcal{O} \in \mathbf{X}$ satisfy Eq. A.6, i.e.

$$x_\mathcal{O} = \frac{E\left(S(x^*) - S(x_\mathcal{O})\right)}{2(D_S - S(x_\mathcal{O}))} \times \frac{D_R}{D_S - S(x^*)} + x^*. \tag{A.7}$$

Assume $x_\mathcal{O}$ also satisfy Eq. A.3 such that

$$x_\mathcal{O} < \frac{E\left(S(x^*) - S(x_\mathcal{O})\right)}{2(D_S - S(x_\mathcal{O}))} + x^* \tag{A.8}$$

Substituting $x_{\mathcal{O}}$ into Eq. A.7, we get

$$\frac{E\left(S(x^*) - S(x_{\mathcal{O}})\right)}{2(D_S - S(x_{\mathcal{O}}))}\left(\frac{D_R}{D_S - S(x^*)} - 1\right) < 0 \tag{A.9}$$

Since $S(x) < \bar{S} = D_S - D_R$ for all $x \in \mathbf{X}$, we have

$$\frac{D_R}{D_S - S(x^*)} < 1, \tag{A.10}$$

and thus Eq. A.9 holds. This result agrees with our assumption, which implies that any copying step which overlapping with the preceding copying steps is removed by HSR, and hence Type 2 echoes are avoided.

Conversely, it is obvious that some positions $x \in \mathbf{X}$ satisfying Eq. A.3 do not necessarily satisfy Eq. A.6. This fact implies that HSR remove excess copying steps, in a sense that some copying steps, which are not causing overlappings, are also removed by HSR.

Appendix B

Publications Resulted from the Study

1. Mark S. K. Lau and C. P. Kwong, "Analysis of Echoes in Single-Image Random-Dot-Stereograms," *to appear in Journal of Mathematical Imaging and Vision.*

2. Mark S. K. Lau and C. P. Kwong, "Analysis of Echoes in Single-Image Random-Dot-Stereograms," *to appear in Proceedings of ICASSP2001.*

Bibliography

[1] A. G. Konheim, *Cryptography: A Primer*, John Wiley & Sons, 1981.

[2] B. Julesz, "Binocular Depth Perception of Computer-Generated Patterns," *The Bell System Technical Journal*, vol. 39, pp.1125-1162, 1960.

[3] C. W. Tyler and M. B. Clark, "The Auto-stereogram," *SPIE Stereoscopic Displays and Applications*, vol. 1258, pp.182-196, 1990.

[4] D. Marr and T. Poggio, "Cooperative Computation of Stereo Disparity," *Science*, vol. 194, pp.283-287, 1976.

[5] D. Marr and T. Poggio, "A Computational Theory of Human Stereo Vision," *Proceedings of the Royal Society of London*, B 204, pp301-328.

[6] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

[7] H. W. Thimbleby and Claire Neesham, "How to play tricks with dots," *New Scientist*, pp.26-29, October, 1993.

[8] S. Singh, *The Code Book*, Doubleday.

[9] W. A. Steer, `http://www.ucl.ac.uk/~ucapwas/stech.html`.

[10] H. W. Thimbleby, S. Inglis, and I. H. Witten, "Displaying 3D Images: Algorithms for Single-Image Random-Dot Stereograms," *IEEE Tran. Computer*, pp.38-48, October, 1994.