

# CHAPTER 1

## INTRODUCTION

This chapter consists of seven subtopics: (1) rationale which explains the background of this study and the related problem situation; (2) theoretical framework which describes the underlying theories or concepts used in the research; (3) conceptual framework and paradigm which identify and discuss about variable/schematic diagram related to the problem; (4) statement of the problem that describes the research problem to be solved; (5) objective and hypotheses that provide the methods used to solve the problem based on theory or empirical evidence, and they should be measurable; (6) scope and delimitation that indicate the area covered in this research; (7) significance of the study which describes the contribution of the study.

### 1.1 Rationale

Visual cryptography is a cryptographic technique which encrypts written material (printed text, handwritten note, picture, etc) in a perfectly secure way which can be decoded directly by the human visual system [2]. This written material is decomposed into  $n$  shares ( $n$  is the number of members in the group). Furthermore, the  $k$  shares will be stacked for obtaining the written material. In this case, no computation is necessary. The written material can be obtain if and only if  $k$  members stacked their shares together.

Many studies for visual cryptography implementation in real world have been proposed such as the study of Hedge et.al [3] and Hsu et.al [4]. Hedge et.al [3], proposed to use image processing and visual cryptography for secure authentication in banking applications. The Bank decomposes the signature of a customer into shares. One share is stored in the Bank database and the other one is kept by the customer. During the transaction, the customer needs to present his share and stacks with the share of the Bank to get the original signature. Another method was proposed by Hsu et.al [4] which introduced visual cryptography to increase the security of digital watermarking scheme. A watermark is decomposed into two shares. One is embedded into the image

that is copyright wanted to be protected (called as host image) and the other is held by the sender. Thus, the two shares could not leak any information about the watermark. For proving the ownership of the image (the owner is the sender), the sender needs to extract the embedded share from the host image and recover the watermark by stacking the embedded share with his share.

In visual cryptography, visual quality (particularly contrast) and pixel expansion become important parameters to evaluate visual cryptography scheme [2]. The higher contrast make it easier to distinguish colors. Whereas the smaller pixel expansion makes it easier to be transported, storage efficiency, and encoding-decoding process cost efficiency. However, when the sub-pixel size are small, it is hard to align the shares in the right position. Therefore, the number of sub-pixel should be optimized such that it will fulfill the requirement that the complexity of alignment process is small enough while the number sub pixel and size are not large. The alignment process is also hard in the case of non-identical size, shape, orientation, or reference coordinate of shares. The visual cryptography scheme which has non-identical shares is called non-identical mathematical support visual cryptography scheme (*NIMSVCS*).

Alignment problem is not only occurred in manual alignment (print and scan shares) but also occurs in digital alignment. The easiest way for handling the alignment problem in visual cryptography scheme (*VCS*) is by adding the frames or special marks (i.e cross marks, etc) outside the area of shares. The alignment process is done by stacking the frames or special marks. Since the share relies on these frames or marks, the method is not effective when the frames or marks are removed by cropping or localizing image alteration. A method for overcoming the alignment problem was proposed by Liu et.al [1] which modified the basis matrices such that it is not necessary to align the shares precisely. The weakness of this method is that the shares is larger and the time complexity is still high in non-identical mathematical support *VCS* (*NIMSVCS*).

## 1.2 Theoretical Framework

A set of shares is called a qualified set if the stacking of the shares reveal the secret image. In order to stack the shares, each share in qualified set needs to be aligned in their proper position by applying geometrical transformations such as translation, rotation, and scaling over each other until the secret information appears.

Based on section 1.1, there is a trade-off between the size of sub-pixels and the ease to align the shares. The smaller sub-pixel size make it harder to align the shares. Thus, the manual alignment procedure can be tedious particularly for high resolution images [5].

Furthermore, several visual cryptography application requires the printing of the shares on paper which further require share scanning. [5]. The printing and scanning process may introduce noise [1]. This noise may cost alignment difficulties.

According to Yan et.al's study [5], the alignment process of two shares is not easy to perform unless some special alignment marks are provided. The special alignment marks can be frames, cross marks, etc. The decoding process is done by aligning those special alignment marks. Putting alignment marks in the spatial domain is vulnerable for editing and cropping. Thus, this method is not effective for overcoming alignment problem.

In 2009, Liu et.al introduced a method for overcoming the alignment problem [1]. They analyze the structure of basis matrices. By reconstructing and adding  $e$  columns ( $e \geq 1$ ) in the basis matrices, they increase the tolerance of misalignment by  $r$  sub-pixels ( $r \geq 1$ ) in horizontal direction. The secret image is able to be recovered even the pixels are shifted right or left by  $r$  sub-pixels. The contrast of the recovered secret image in shifted sub-pixels has negative value which means that the recovered secret image is complementary to the original. For example, if the secret image has black text and white background, then the recovered secret image with shifted sub-pixels will produce the opposite colors (white text and black background). The human eyes can get information conveyed from the complementary images as well as from the original image. Unfortunately, Liu et.al's method has problem in *NIMSVCS* since there is no information about the proper position and orientation for each share. Therefore, the alignment should be based on brute force method.

### 1.3 Conceptual Framework

The basic idea of alignment process in visual cryptography is finding the patterns or points which indicate the proper orientation of each share while they were stacked. For achieving the objective result, several variables involve in this study. The system of *VCS* is divided into two parts, encoding phase and decoding phase.

The input of encoding phase is the participant  $P_1$  who wants to share the secret image ( $SI$ ). The output of encoding phase is the shares which are distributed among the participants. The dependent variables of encoding phase are pixel expansion, time complexity of encoding phase, and mutual information (between embedded parameters and the secret image). The pixel expansion tells about how big the generated shares. The expansion of the pixel depends on basis matrices chosen by participant  $P_1$  before decomposing the shares. The larger basis matrices make the generated shares larger. So that the independent variables of pixel expansion are basis matrices (black and white matrix). The time complexity of encoding phase tells about how long system generates shares with alignment method. It depends on the chosen basis matrices and the size of shares. The larger basis matrices and size of shares need the higher time complexity for generating shares. Thus, the independent variables for time complexity of encoding phase are the chosen basis matrices and the size of the shares. While mutual information (between embedded parameters and the secret image) tells whether the embedded parameters give information about the secret image and vice versa. The perfect secrecy is influenced by the entropy relation between the secret image ( $SI$ ) and the embedded parameters. Those entropy relation become independent variables for mutual information (between embedded parameters and the secret image).

The input of decoding phase is the shares in qualified set and the participant  $P_2$  who wants to decode the secret image ( $SI$ ). The output of decoding phase is reconstructed image ( $RI$ ). The dependent variables of decoding phase are time complexity of decoding phase. The time complexity of decoding phase tells about how long the system decodes the shares. It depends on the size of the shares and the number of references. Therefore, the independent variables for time complexity of decoding phase are the size of the shares and the number of references.

## 1.4 Problem Statements

Based on the background of this research discussed in on section 1.1 and 1.2, there are two drawbacks of Liu et.al's alignment method.

The first drawback is that Liu et.al's method needs large basis matrices because they modified the structure of the matrix and added two blocks where each block is consisted of  $e$  columns ( $e \geq 1$ ). The larger the basis matrices size produce larger the share size. Thus, larger share size required higher time complexity for conducting decoding process.


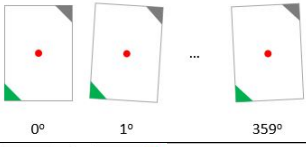
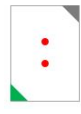
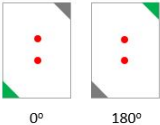

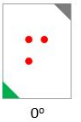
The second drawback is that this method is not effective if implemented in non-identical mathematical support *VCS* (*NIMSVCS*) since there is no information about the proper position and orientation for each share. Thus, the time complexity is still high when stacking non-identical mathematical shares because the alignment should be conducted based on brute force method.

## 1.5 Hypothesis

**The objective of this research is reducing decoding time while maintaining pixel expansion.**

In order to reduce the decoding time (alignment time), some patterns inside the share are necessary. If one point is used, then, the probability for finding the proper orientation is  $\frac{1}{360}$  (in case the smallest unit for each rotation is one degree). In other words, the maximum trial that should be done for obtaining the proper orientation is 360. If two points are used, the probability for finding the proper orientation is  $\frac{1}{2}$ , or in other words the maximum trial that should be done for obtaining the proper orientation was 2. If the third point is added and orthogonal to two others points, then the right orientation can be directly found. The illustration of the finder points can be seen in table 1.1.

TABLE 1.1: The Orientation Possibilities of Finder Pattern in Image

No	Number of Points	Image	Possibilities
1	1 Point		 0°    1°    ...    359°
2	2 Points		 0°    180°
3	3 Points		 0°

Based on table 1.1, the right orientation of the image with three points is marked by orthogonal angle on the top left. Thus, the three orthogonal points (*3OP*) as finder

pattern can identify the orientation of the image as well as if it is implemented in *VCS*. However, the *3OP* in *VCS* should fulfill the following requirements:

1. *3OP* should not interfere the share.
2. *3OP* are invisible. Instead of drawing the *3OP* as a visible points in the shares, it is directed by the coordinates of 3 points which is embedded in the specific location of the shares.
3. *3OP* are inside the shares.

The illustration of the *3OP*'s implementation in *NIMSVCS* can be seen in figure 1.1.

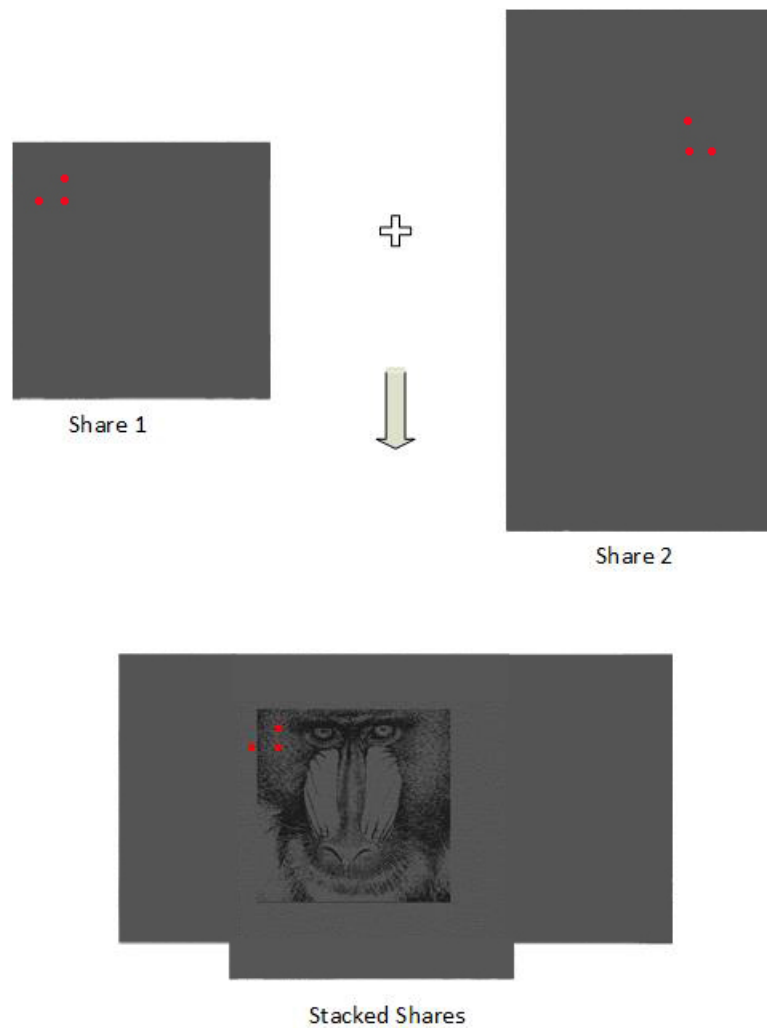


FIGURE 1.1: *3OP* in *NIMSVCS*

By fulfilling the requirements of the  $3OP$ , the basis matrices is not necessary to be reconstructed or modified. Thus, the pixel expansion also be maintained. Finally, it can be concluded that the proposed method is expected to be able overcoming the problem while maintaining pixel expansion, since there is additional information (orientation and position) in the form of  $3OP$  and no modification of basis matrices.

Clearly, there is a benefit for eliminating alignment procedure in decoding phase and adding procedure for calculating  $3OP$  in encoding phase. Usually encoding process is conducted for one time only, while decoding process can be conducted more than one time. Therefore, this idea can exploit the benefit for al parties which has implemented this system.

## 1.6 Assumption

This study assumes that the inputs to the proposed system are as follows:

1. There is no third parties (dealer) in encoding phase who decomposing the secret image.
2. There is no error during communication between encoding and decoding phase
3. The scheme that is used in this study is  $k$  out of  $n$ , where  $k = n$ . Since the minimum  $k$  and  $n$  are 2, then without loss generality, the proposed method is implemented in  $(2,2)$ - $NIMSVCS$ . It can be easily extended to  $k$  and  $n$  more than 2.
4. Color level of the secret image ( $SI$ ) is 1 (black and white) or 8 bits (grayscale).
5. The Chameleon hash function is determined before encoding phase.

## 1.7 Scope and Delimitation

This study formulated the scope and delimitation are as follows:

- This study is focused in spatial domain alignment scheme such that this method can be used in manual or digital alignment. This study also focuses in digital alignment without lose generality, since many shares are generated digitally before printing the shares.

- This study is focused on *NIMSVCS* which has different size, orientation, and reference coordinate. The shape of share is square or rectangle.
- Color level of the reconstructed image (*RI*) is 1 bit (black and white).

## 1.8 Importance of The Study

This study contributes to reduce the time complexity of decoding phase in *NIMSVCS* while maintaining the pixel expansion of the reconstructed image (*RI*) by proposing three-orthogonal-points (*3OP*).