



TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
CENTRAL CAMPUS, PULCHOWK

THESIS NO.: 069MSCS655

Visual Cryptography using Image Pixel Transparency

By

Dipesh Shrestha

A THESIS

**SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND
COMPUTER ENGINEERING IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN
COMPUTER SYSTEM AND KNOWLEDGE ENGINEERING**

**DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
LALITPUR, NEPAL**

NOVEMBER, 2014

Visual Cryptography using Image Pixel Transparency

By

Dipesh Shrestha

(069/MSCS/655)

Thesis supervisor:

Sanjeeb Prasad Panday (Ph. D)

M. Sc. Program Coordinator

A thesis submitted in partial fulfillment of the requirements for the
degree of Master of Science in Computer System and Knowledge Engineering

Department of Electronics and Computer Engineering

Institute of Engineering, Central Campus, Pulchowk

Tribhuvan University

Lalitpur, Nepal

November, 2014

COPYRIGHT

The author has agreed that the library, Department of Electronics and Computer Engineering, Institute of Engineering, Central Campus, Pulchowk, may make this thesis freely available for inspection. Moreover the author has agreed that the permission for extensive copying of this thesis work for scholarly purpose may be granted to Assistant Professor Dr. Sanjeeb Prasad Panday, who supervised the thesis work recorded herein or, in his absence, by the Head of the Department, wherein this thesis was done. It is understood that the recognition will be given to the author of this thesis and to the Department of Electronics and Computer Engineering, Pulchowk Campus in any use of the material of this thesis. Copying of publication or other use of this thesis for financial gain without approval of the Department of Electronics and Computer Engineering, Institute of Engineering, Central Campus, Pulchowk and author's written permission is prohibited.

Request for permission to copy or to make any use of the material in this thesis in whole or part should be addressed to:

Head

Department of Electronics and Computer Engineering

Institute of Engineering

Central Campus, Pulchowk

Lalitpur, Nepal

TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
CENTRAL CAMPUS, PULCHOWK
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

The undersigned certify that they have read and recommended to the Institute of Engineering for acceptance, a thesis entitled “Visual Cryptography using Image Pixel Transparency”, submitted by Dipesh Shrestha in partial fulfilment of the requirements for the award of the degree of Master of Science in Computer System and Knowledge Engineering.

Supervisor, Dr. Sanjeeb Prasad Panday
Assistant Professor
Department of Electronics and Computer Engineering
Institute of Engineering
Central Campus, Pulchowk

External Examiner, Er. Krishna Prasad Bhandari
Senior Engineer
IT Directorate, Nepal Telecom

Committee Chairperson, Dr. Shashidhar Ram Joshi
Professor
Department of Electronics and Computer Engineering

Date

DEPARTMENTAL ACCEPTANCE

The thesis entitled “Visual Cryptography using Image Pixel Transparency”, submitted by Dipesh Shrestha in partial fulfillment of the requirements for the award of the degree of Master of Science in Computer System and Knowledge Engineering has been accepted as a bonafide record of work independently carried out by him in the department.

Dr. Dibakar Raj Pant

Assistant Professor and Head of the Department

Department of Electronics and Computer
Engineering

Central Campus Pulchowk

Institute of Engineering

Tribhuvan University

Lalitpur, Nepal.

ABSTRACT

This thesis makes use of transparency of pixels of the shares, the two or more encrypted images, so as to reveal the secret image. The pixels of shares can be generated randomly or the cover image can be used to generate the first share. The encrypted shares generated using cover image seem to be visually less similar to those generated without using cover image. Also, on the basis of image similarity between shares and original image, further encryption of encrypted shares can be performed.

This thesis also compares the outcome when cover image is used and when not used to generate shares. Results show that the latter is more sensitive to the transparency factor (α) than the former encouraging the use of properly selected cover image for visual cryptography using pixel transparency.

Key Words:

Visual Cryptography, Image Transparency

ACKNOWLEDGEMENT

I am very thankful to the Department of Electronics and Computer Engineering for providing the opportunity to conduct this thesis which, indeed, is an important milestone in my research career.

Thesis Supervisor and the Program Coordinator of “Master of Science in Computer System and Knowledge Engineering”, Dr. Sanjeeb Prasad Panday has been very much helpful and deserves an especial vote of thanks. I would like to express my heartfelt appreciation to Dr. Panday for his guidance, cooperation, inspiration, encouragement and constant support since the beginning of the thesis.

I would also like to express my sincere gratitude to Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Subarna Shakya, Dr. Arun K. Timilsina and Dr. Aman Shakya, for their encouragement and precious guidance.

Likewise, I would like to thank all my class mates who shared their views and ideas regarding the thesis and have been great help in this thesis work.

Also, thanks to my family for the moral support during the thesis work and lastly, thanks to my friends Mrs. Anjana Devi Bhandari, Er. Dipendra Kumar Jha, Er. Januka Gyawali, Er. Prakash Shrestha, Er. Sabita Acharya and Er. Yogendra Raj Shrestha for their constant encouragement and support.

Dipesh Shrestha
(069/MSCS/655)

TABLE OF CONTENTS

Copyright -----	ii
Approval Page -----	iii
Departmental Acceptance -----	iv
Abstract-----	v
Acknowledgement-----	vi
Table of Contents -----	vii
List of Tables -----	ix
List of Figures -----	x
Abbreviations -----	xi
CHAPTER ONE: INTRODUCTION -----	1
1.1 Background -----	2
1.2 Problem Statement -----	3
1.3 Objectives -----	3
1.4 Scope of the Work -----	3
1.5 Organization of Report -----	4
CHAPTER TWO: LITERATURE REVIEW -----	5
2.1 Previous Work -----	6
2.1.1 Introduction of Visual Cryptography -----	6
2.1.2 Concept of Half Tone Image -----	7
2.1.3 Extended Visual Cryptography -----	8
2.2 Recent Work on Image Transparency -----	8
CHAPTER THREE: SIMILARITY ANALYSIS TECHNIQUES -----	12
3.1 Cross-Correlation -----	13
3.2 Cross-Correlation of Array of moving average -----	13
3.3 Mean Square Error (MSE) -----	13
3.4 Peak Signal to Noise Ratio (PSNR) -----	14
3.5 Structural SIMilarity (SSIM) -----	14

CHAPTER FOUR: METHODOLOGY -----	16
4.1 Working Principle -----	17
4.2 Generating Shares without using Cover Image -----	19
4.3 Generating Shares by using Cover Image -----	19
 CHAPTER FIVE: RESULTS AND DISCUSSIONS -----	 20
5.1 Outputs -----	21
5.2 Comparison with previous works -----	33
5.3 Complexity Analysis -----	36
 CHAPTER SIX: CONCLUSION AND RECOMMENDATION -----	 37
6.1 Conclusion -----	38
6.2 Recommendation -----	38
 REFERENCES -----	 39
 APPENDIX -----	 40

LIST OF TABLES

<i>Table 5.1: Similarity analysis with various alpha values for Baboon Image</i> -----	24
<i>Table 5.2: Similarity analysis for encryption using pixel swap only</i> -----	27
<i>Table 5.3: Similarity analysis for encryption using cover image only</i> -----	29
<i>Table 5.4: Similarity analysis for encryption using pixel swap and cover image</i> ---	31
<i>Table 5.5: Other Similarity analysis results</i> -----	34
<i>Table 5.6: Sensitivity of Cross-Correlation in different methods with Alpha</i> -----	36
<i>Table 5.7: Sensitivity of SSIM in different methods with Alpha</i> -----	37

LIST OF FIGURES

<i>Figure 2.1: Possible shares(4 sub-pixels) pair of which represents a pixel-----</i>	<i>6</i>
<i>Figure 2.2: Possible Shares to represent White Pixel -----</i>	<i>6</i>
<i>Figure 2.3: Possible Shares to represent Black Pixel -----</i>	<i>6</i>
<i>Figure 2.4: a. Continuous tone b. Halftone -----</i>	<i>7</i>
<i>Figure 2.5: Original image, Halftone, Share 1, Share2 and decrypted image -----</i>	<i>7</i>
<i>Figure 2.6: Extended VC for Natural Image -----</i>	<i>8</i>
<i>Figure 2.7: Illumination declining of light penetrated through two media with different rates of penetration -----</i>	<i>9</i>
<i>Figure 2.8: Experiments of image sharing -----</i>	<i>10</i>
<i>Figure 4.1: Block diagram of VC using Image Pixel Transparency -----</i>	<i>19</i>
<i>Figure 5.1: Encryption without using Cover -----</i>	<i>21</i>
<i>Figure 5.2: Encryption using Cover Image -----</i>	<i>22</i>
<i>Figure 5.3: Cross-Correlation vs Alpha for different methods -----</i>	<i>34</i>
<i>Figure 5.4: SSIM vs Alpha for different methods -----</i>	<i>35</i>
<i>Figure 8.1: Generating shares for image of Dilshobha Shrestha -----</i>	<i>42</i>
<i>Figure 8.2: Generating shares for image of Anuradha Koirala -----</i>	<i>42</i>
<i>Figure 8.3: Generating shares for image of Bill Clinton -----</i>	<i>43</i>
<i>Figure 8.4: Generating shares for image of Ramesh Kharel -----</i>	<i>43</i>
<i>Figure 8.5: Generating shares for image of Baboon -----</i>	<i>44</i>
<i>Figure 8.6: Generating shares for image of Taj Mahal -----</i>	<i>44</i>

ABBREVIATIONS

CTIS	Controllable Transparency Image Sharing
HVS	Human Visual System
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
SSIM	Structural SIMilarity
VC	Visual Cryptography
XCOR	Cross Correlation

CHAPTER ONE
INTRODUCTION

1.1 Background

Secured secret message sharing is one of the major issues today in the field of Computer and Network Security. Visual Cryptography (VC) is one of the approaches of sharing image secretly by computing n number of random images called shares. In VC decryption is a simple mechanical process of just stacking k out of n shares printed on transparent sheets one over another and makes use of Human Visual System (HVS) instead of complex computation. Many new enhancements and extensions on the approach have been made since its introduction in 1994 by *Naor et al.* in [1].

VC is much secured technique as, given just one of the shares; there is no way to determine the other shares and to reveal the secret image. Most of the earlier approaches [2, 3, 4] in VC make use of halftone images introduced by *Zhou et al.* in [2] that produces the noisy shares and final output. This thesis proposes to enhance idea proposed by *Zeng and Tsai* in [5]. The enhancement include the use of cover image for first share and also measure the degree of similarity between original image and the shares so as to lessen the intrusion risk.

The use of cover image secures the information as it makes one share image (encrypted from the original image) to look like another image (cover image) making it much difficult to reveal original image. Also the other encrypted share becomes less similar to original image if the cover image is properly chosen.

Measurement of similarity between shares and original image is also a very important analysis in the field of image cryptography. The degree of similarity between them must be as low as possible so that the intruders may not reveal the secret image. Different techniques can be applied for this measurement. This thesis analyzes the similarity of images using XCOR, PSNR, MSE and SSIM between two images.

1.2. Problem Statement

Human beings share information through messages in the form of text, image or audio. Some of the information is required to be kept secret among certain group of authorized persons but message might have to be transmitted through unsecure medium. So the problem is to share image without revealing it to other unauthorized persons.

1.3. Objectives

The prime objectives of this thesis are

- To determine n images(shares) that individually do not reveal any information about secret but stacking them together reveals high quality original secret image without increasing the original size
- To analyse the visual similarity between Original image and the encrypted Share images so as to check vulnerability of Shares.

1.4 Scope of the Work

Visual cryptography is applicable in number of security related fields. This thesis is especially more beneficial in areas where computer encryption/decryption is infeasible or inapplicable. As the decryption process is completely mechanical and no computation is required, secret messages can be secretly sent to rural areas securely.

Taking an example case, in military, information security is highly sensitive and also computers might not be available in many cases. Transferring an image to some military personnel in some rural area might be risky. Intruder may attack the messenger and take away the confidential photo. In such case, visual cryptography can be very useful. Different shares of image can be sent through different channels or at different time such that only the authorised personnel can receive all the shares and could be able to decrypt the information.

1.5 Organization of Report

The chapter 2 of this thesis report is Literature Review that describes about different previous works done by different researchers in this area of visual cryptography. It focuses on their approaches, advantages and the major drawbacks.

Chapter 3 basically includes the theory on the different image similarity analysis techniques used in the thesis. Chapter 4 is the Methodology section that discuss about the general and specific algorithms followed in this thesis and how the drawbacks of previous works is tried to minimize. It focuses on how the job carries on and how to quantitatively measure the outcome of the thesis.

Chapter 5, the Results and Discussions contains the Output of the thesis work and its comparison with previous works. And finally, Chapter 6 includes the conclusion of thesis and the recommendation for future researches in this area.

CHAPTER TWO
LITERATURE REVIEW

2. Previous Work

2.1.1 Introduction of Visual Cryptography

Naor *et al.* introduced the technique of Visual Cryptography in which the binary image is decomposed into n number of shares [1]. k out of n shares when stacked over one another reveals the original secret image. It is applicable only in binary image in which shares for original image is determined by randomly selecting pairs of subpixel matrices for black and white pixels.

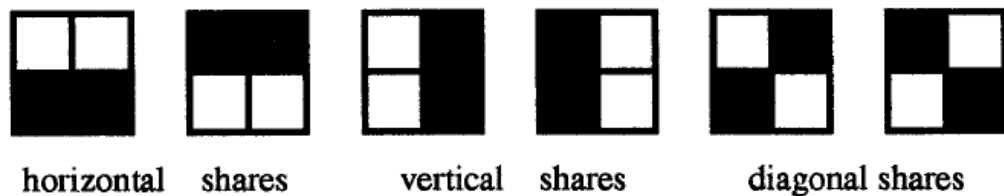


Figure 2.1: Possible shares (4 sub-pixels) pair of which represents a pixel

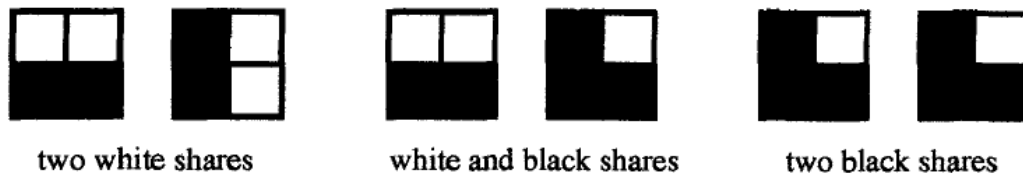


Figure 2.2: Possible Shares to represent White Pixel

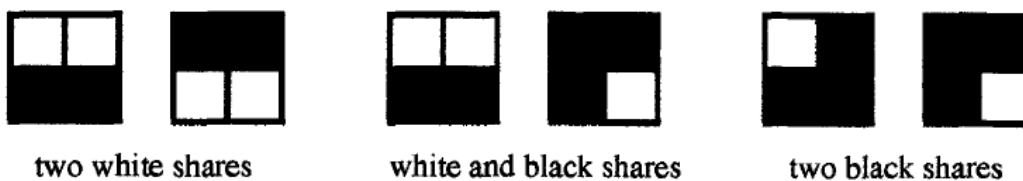


Figure 2.3: Possible Shares to represent Black Pixel

Above Figure 2.1 shows example shares, pair of which is used to represent a pixel. Figure 2.2 and Figure 2.3 shows example of pair of shares used to represent white and black pixels. It is Simple and effective for text sharing, but when it comes to image sharing, it has poor result. Firstly, it is practically applicable only for Black and White (Two Tone) images. Also, the decrypted image looks much degraded in quality.

2.1.2 Concept of Half Tone Image

Later, the concept was extended for greyscale image using the halftone image of the original image [2, 3, 4]. Half-toning technique represents the gray levels with the density of black dots in the white background. Darker grey-level would be represented by dense black dots. That means representation of one grey level pixel requires several black and white pixels.

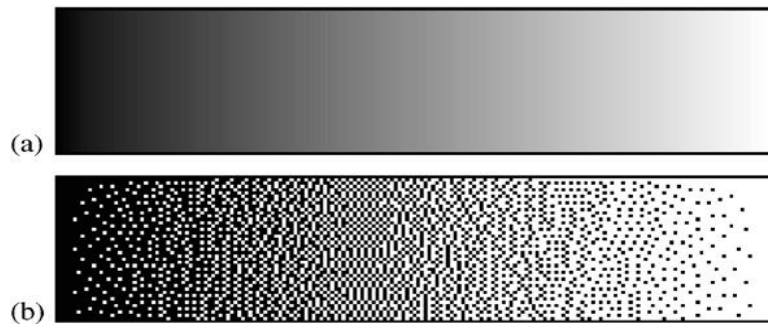


Figure 2.4: a. Continuous tone b. Halftone

Figure 2.4 shows continuous and halftone representations of the greyscale and *Figure 2.5* gives an example of encrypting and decrypting halftone image using Visual Cryptography [6].

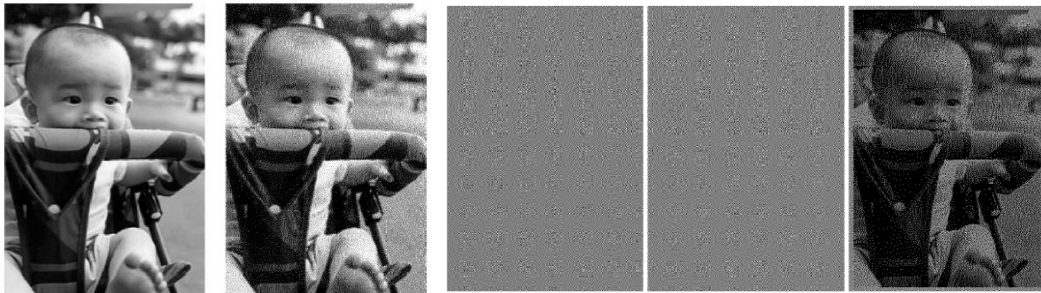


Figure 2.5: Original image, Halftone, Share 1, Share2 and decrypted image respectively.

The introduction of half toning in [2] took the visual cryptography to the greyscale images but it still has the demerit that it increases the size of encrypted image and also the decrypted image degrades in quality than the original secret image. So the new approach to visual cryptography making use of the transparency of the image is studied in [5] that maintain the quality of decrypted image without increasing

the size of encrypted shares. Further description on this approach can be found in Topic 2.2 of this chapter.

2.1.3 Extended Visual Cryptography

Also, as shown in *Figure 2.6*, in Extended Visual Cryptography approach used in [7], the shares are not random images but some meaningful pictures, i.e. meaningful pictures combines to reveal the secret. As, meaningful picture will be transmitted, attacker might not even know about secret image being sent.

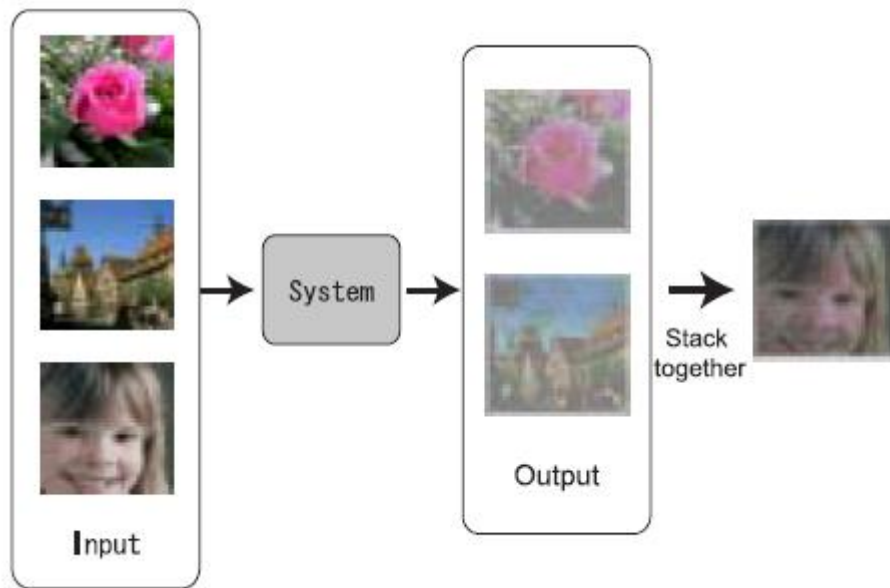


Figure 2.6: Extended VC for Natural Image, source: [7]

But in this approach the quality of reconstructed image is compromised providing the space for further improvement. This thesis intends to use the concept of using cover image from this work and inter-mix the concept with visual cryptography using transparency of image. Further detail is in *Chapter 3*.

2.2 Recent Work on Image Transparency

Aimed at transparency controlling to secret image, *Zeng and Tsai* in [5] proposes an image sharing scheme to encrypt secret image among two or more sharing images. The overall effects of the proposed method are the achievements of controllable transparency of secret image and unexpanded size of sharing images. The controllable transparency image sharing scheme is realized based on the

principle of penetrability. While light passes through a medium, medium declines illumination of light. Pixels are treated as medium and pixels' value of multiple sharing images are adjusted, so that transparency of decrypted-secret image is controllable [5].

The Controllable Transparency Image Sharing (CTIS) scheme, discussed in [5], is realized based on the principle of penetrability. While light penetrates through a medium, it declines illumination of light. A medium with low rate of penetration is more serious than one with high rate of penetration for illumination declining. In the work, researchers treat pixel as medium. White pixel consists of none of ink/powder in printing system, therefore, it carries high rate of penetration. In contrast, black pixel carries low one. *Figure 2.7* depicts illumination declining of light penetrated through two media with different rates of penetration. Let M_1 and M_2 be the first medium and the second medium carried the rates of penetration r_1 and r_2 , respectively. Assume that the denotation I represents the initial light illumination.

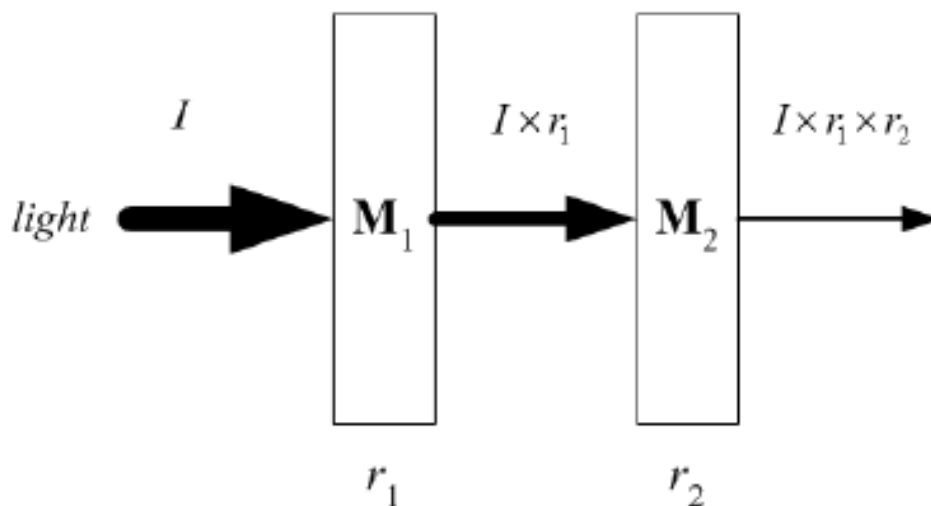


Figure 2.7: Illumination declining of light penetrated through two media with different rates of penetration, Source: [5]

After light penetrates through two media with penetration rates r_1 and r_2 , the resulting illumination, I' is given as:

$$I' = I * r_1 * r_2 \text{ ----- (2.1)}$$

The rate of penetration depends on pixel values of two shares, p_1 and p_2 as:

$$r_1 = p_1 / 255 \text{ and } r_2 = p_2 / 255 \text{ where } 0 \leq p_1, p_2 \leq 255$$

If p_s be pixel value of original image then pixel value of share2, p_2 , can be generated as:

$$p_2 = \text{round}\left(\frac{\alpha \times p_s \times 255}{p_1}\right) \text{ ----- (2.2)}$$

Where, α is the transparency factor, $0 < \alpha \leq 1$

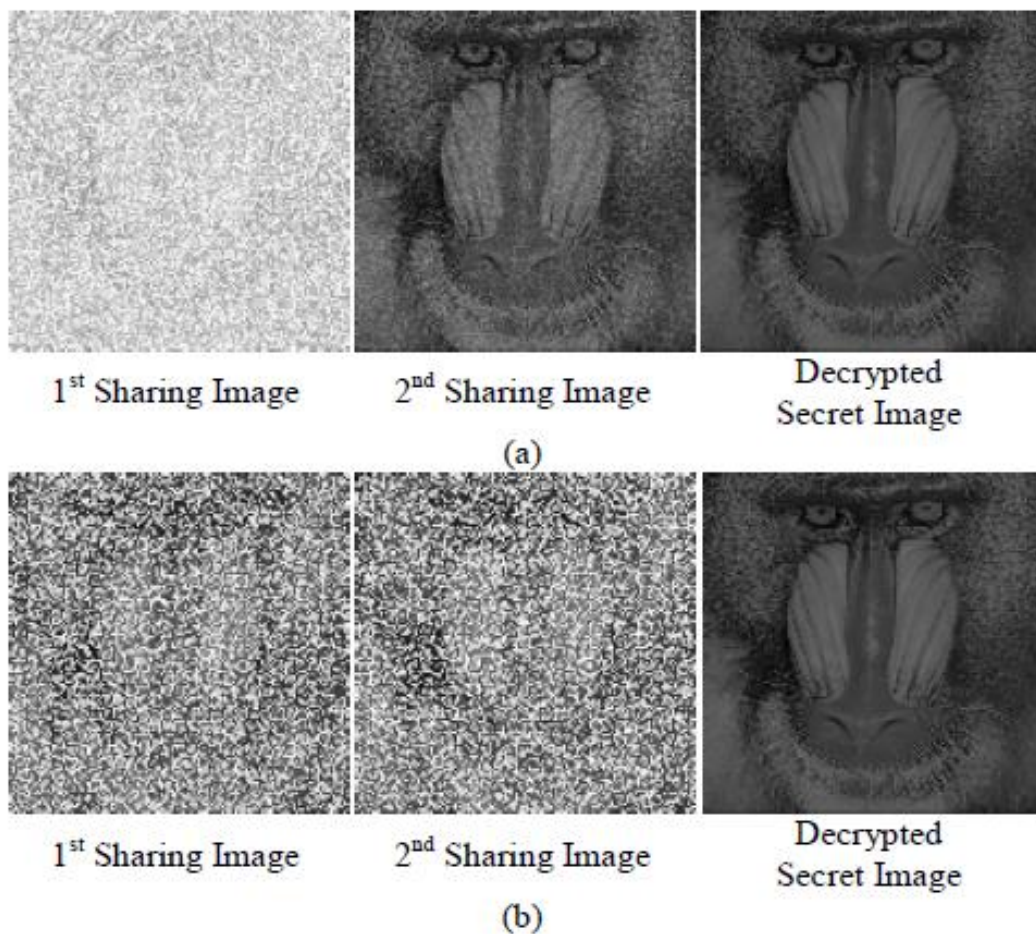


Figure 2.8: Experiments of image sharing (a) without using pixel swapping, and (b) by using pixel swapping. Source: [5]

The paper [5] suggests swapping of the pixel values between the shares for better result. A random number, R is generated such that $0 \leq R \leq 1$. If R is less than 0.5 then p_1 and p_2 are swapped otherwise they are unaltered. The *Figure 2.8* depicts the results of encryption (a) without using pixel swapping and (b) by using pixel

swapping. It can be clearly observed that the implementation of pixel swapping improves the result.

The decrypted image from this approach has better quality than previous methods and also the encrypted shares are of same size as that of original image. But one major drawback of this approach is that the fewer number of encrypted shares tend to be less secured. To gain high security, greater numbers of shares are to be generated, but that will degrade the quality of regenerated image.

To address above drawback, this thesis uses the carefully chosen cover image to generate the first share. Other shares are generated afterwards. Further details are given in Chapter 3.

CHAPTER THREE
SIMILARITY ANALYSIS TECHNIQUES

Similarity analysis is one of the important portions of this thesis. Following approaches have been implemented in this thesis for image comparison:

3.1 Cross-Correlation

To calculate the cross correlation between two images, first we construct two matrices corresponding to pixel intensity values of the images. Say, A and B are the two Matrices both of same dimension of p x q. Then converting them to a long array of numbers (ie, two vectors) of length n = p*q, we apply following formula to calculate cross correlation, r_{ab} .

$$r_{ab} = \frac{\sum_{i=1}^n (A_i - \bar{A})(B_i - \bar{B})}{\sqrt{\sum_{i=1}^n (A_i - \bar{A})^2} \sqrt{\sum_{i=1}^n (B_i - \bar{B})^2}} \quad \text{----- (3.1)}$$

Where, A_i and B_i are i^{th} element of Arrays A and B

\bar{A} and \bar{B} are Mean of the element of Arrays A and B

3.2 Cross-Correlation of Array of Moving Average

Moving average means taking the array of average values of pixels in different regions. If average of each m x n pixels are taken then the overall size of the array used for correlation calculation will be (p/m * q/n) which is much lesser than using entire pixels. The same formula as in eqn 3.1 can be used, just that the array size now will be much smaller.

3.3 Mean Squared Error (MSE)

The mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated.

In this thesis, MSE is used to compare original image and shares. Given a original $m \times n$ monochrome image I and the share generated K , MSE is defined as:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad \text{----- (3.2)}$$

3.4 Peak Signal to Noise Ratio (PSNR)

PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

PSNR is most easily defined via the mean squared error (*MSE*). Equation for MSE is given in *eqn 3.2*. Then, PSNR (in db) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\ &= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE) \end{aligned} \quad \text{----- (3.3)}$$

Where, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

3.5 Structural SIMilarity (SSIM)

The structural similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as reference. SSIM is designed to improve on traditional methods like peak

signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception.

The difference with respect to other techniques mentioned previously such as MSE or PSNR is that these approaches estimate *perceived errors*; on the other hand, SSIM considers image degradation as *perceived change in structural information*. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene [10].

The SSIM metric is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is:

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \text{-----} (3.4)$$

with

- μ_x the average of x ;
- μ_y the average of y ;
- σ_x^2 the variance of x ;
- σ_y^2 the variance of y ;
- σ_{xy} the covariance of x and y ;
- $c_1=(k_1L)^2$, $c_2=(k_2L)^2$ two variables to stabilize the division with weak denominator;
- L the dynamic range of the pixel-values (typically this is $2^{\#bits} \text{ per pixel} - 1$);
- $k_1=0.01$ and $k_2=0.03$ by default.

CHAPTER FOUR
METHODOLOGY

4.1 Working Principle

This thesis uses transparency of pixels of the shares such that shares printed on transparent sheets, when overlaid, reveals the secret image. One of the advantages of this approach is that it will not increase the image size and it also maintains the quality of reconstructed image as no half toning of image will be done.

The general algorithm can be described in steps given below:

1. Generate the 1st share with or without using the cover image from the Original image. 1st share is generated such that none of its Pixel has Intensity value greater than corresponding pixel in Original Image and also has much less similarity with Original Image. The details about the generation will be discussed in topics 4.2 and 4.3 further below.
2. Use the equation (2.2) to calculate the pixel values of 2nd share from the share 1 and original image. 2nd share is such that overlaying it with Share 1 would generate Original Image.
3. Compare Similarity between original image and the shares as the measure degree of security using techniques – Cross Correlation, PSNR, SSIM
4. If they tend to be visually similar then further encryption will be required. So repeat the process for encrypted image as well until all the shares are visually different from original image.

Note that only numerically calculated values might not be enough for similarity assessment human observation might be required.

Thresholds for similarity assessment techniques:

There is no particular threshold for being able to say that “below this threshold the images are similar and above it they are different”. So, it is better to define the range such that below if value lies in the range then other techniques or the human observation is required. Following are the range for different techniques defined after several trials and errors on different images.

XCOR: The Cross-correlation value of below 0.1 generally signifies that two images are visually different whereas value above 0.6 usually means images are similar visually. So, if it is between 0.1 and 0.6 then further analysis is most probably required.

PSNR: The Peak Signal to noise ratio is the ratio of square of peak value in image divided by MSE. It is usually denoted in decibel (db). PSNR greater than 30db signifies that images are similar [9]. For most of the dis-similar images, PSNR value less than 10 db was obtained. So, range of 10 db to 30 db can be said to be range of threshold for PSNR.

SSIM: For exact two images, SSIM index is 1, whereas, SSIM index of less than 0.3 was obtained for many dissimilar images. range of 0.1 to 0.3 can be the threshold range for SSIM index.

Figure 4.1 shows the block diagram of VC using Image Pixel Transparency system as described in steps above.

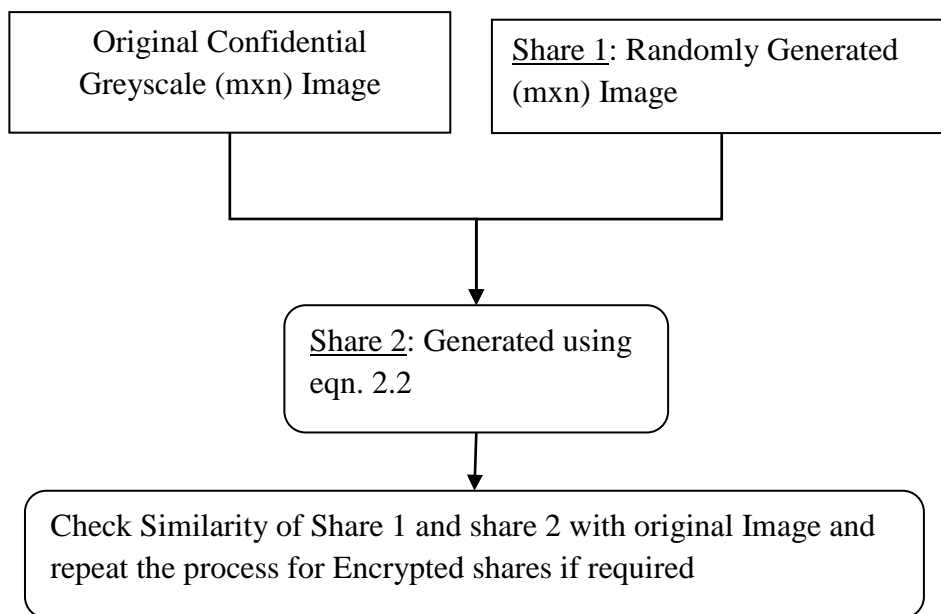


Figure 4.1: Block diagram of VC using Image Pixel Transparency

4.2 Generating Shares without using Cover Image

If the Cover image is not used, the share1 is generated completely randomly such that pixel intensity values of share1 is greater than the corresponding pixel intensity value of original image. This restriction is due to physical limitation that the intensity of darker pixel is not possible to decrease by overlapping with other shares.

After generating share1, the pixel values of share2 are eventually calculated using equation (2.2) and simultaneously random pixels of share2 are swapped with corresponding pixel of share 1 with the pre determined probability (50% is used by default).

4.3 Generating Shares by using Cover Image

The chosen Cover image is resized to match the size of original image and assigned as the share1 after simple contrast adjustment making its minimum and maximum intensity values equal to that of original image. But as in previous case in which cover image was not used, we have to make sure that pixel intensity values of share1 are greater than the corresponding pixel intensity value of original image. To conform this, the corresponding pixel intensities of share1 and original image are compared and if pixel intensity value of share1 is less than that of original, then intensity of that pixel is increased to random value between original pixel intensity and maximum possible intensity value.

After generating share1, the pixel values of share 2 are eventually calculated using equation (2.2) but the pixel swapping is not done in this case. That is because Pixel Swapping tends to increase the image similarity between shares and the original images.

CHAPTER FIVE
RESULTS AND DISCUSSIONS

5.1 Outputs

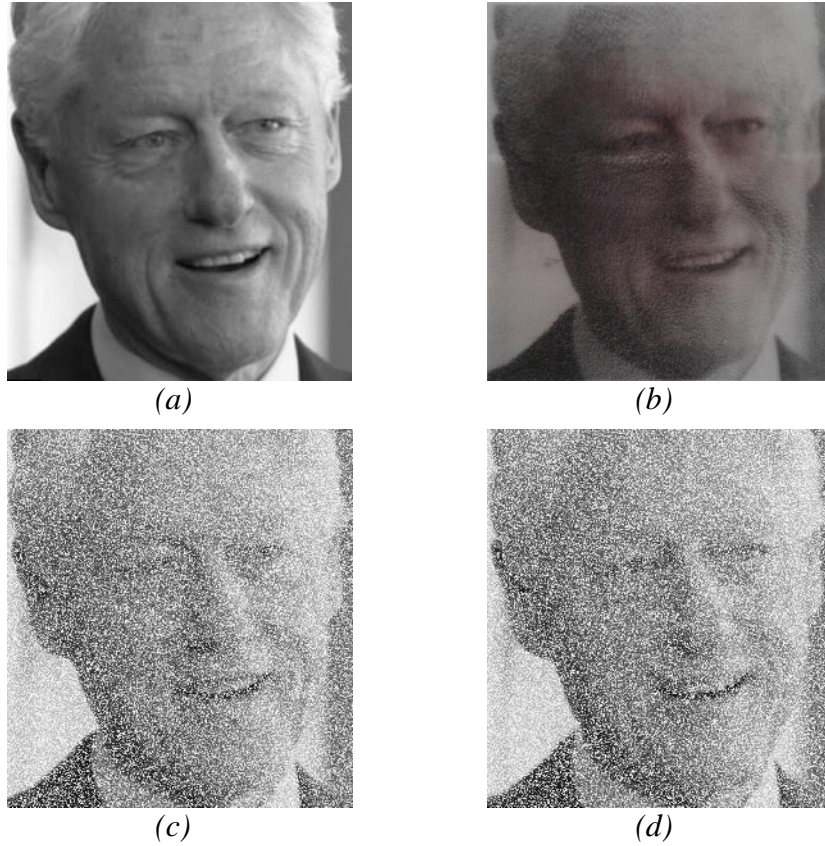


Figure 5.1: Encryption without using Cover Image (a)Original secret image (b)Decrypted image (c)1st Share image (d)2nd share image

The *Figure 5.1* above depicts the result of image encryption without using the cover image. Original secret image used here is that of Bill Clinton which is encrypted to get two share images *c* and *d*. Firstly, 1st Share is randomly generated pixel values such that intensity of certain pixel is not less than corresponding pixel intensity in original image. Then pixel intensities of 2nd Share are evaluated using *a* and *c* and swapped with corresponding pixel in 1st share with 50% probability. Overlapping *c* and *d* results the decrypted image *b*.

The Correlation Coefficients calculated by comparing *a* with *b*, *c* and *d* were 0.89, 0.54 and 0.55 respectively i.e. Although the final decrypted image is much similar to original but the encrypted shares are vulnerable from security point of view. Original image can be guessed visually with any one of the shares. The shares can be further encrypted, but it will degrade the quality of decrypted image. The use of

Cover image helps make the system more secured as shown in the next result below.

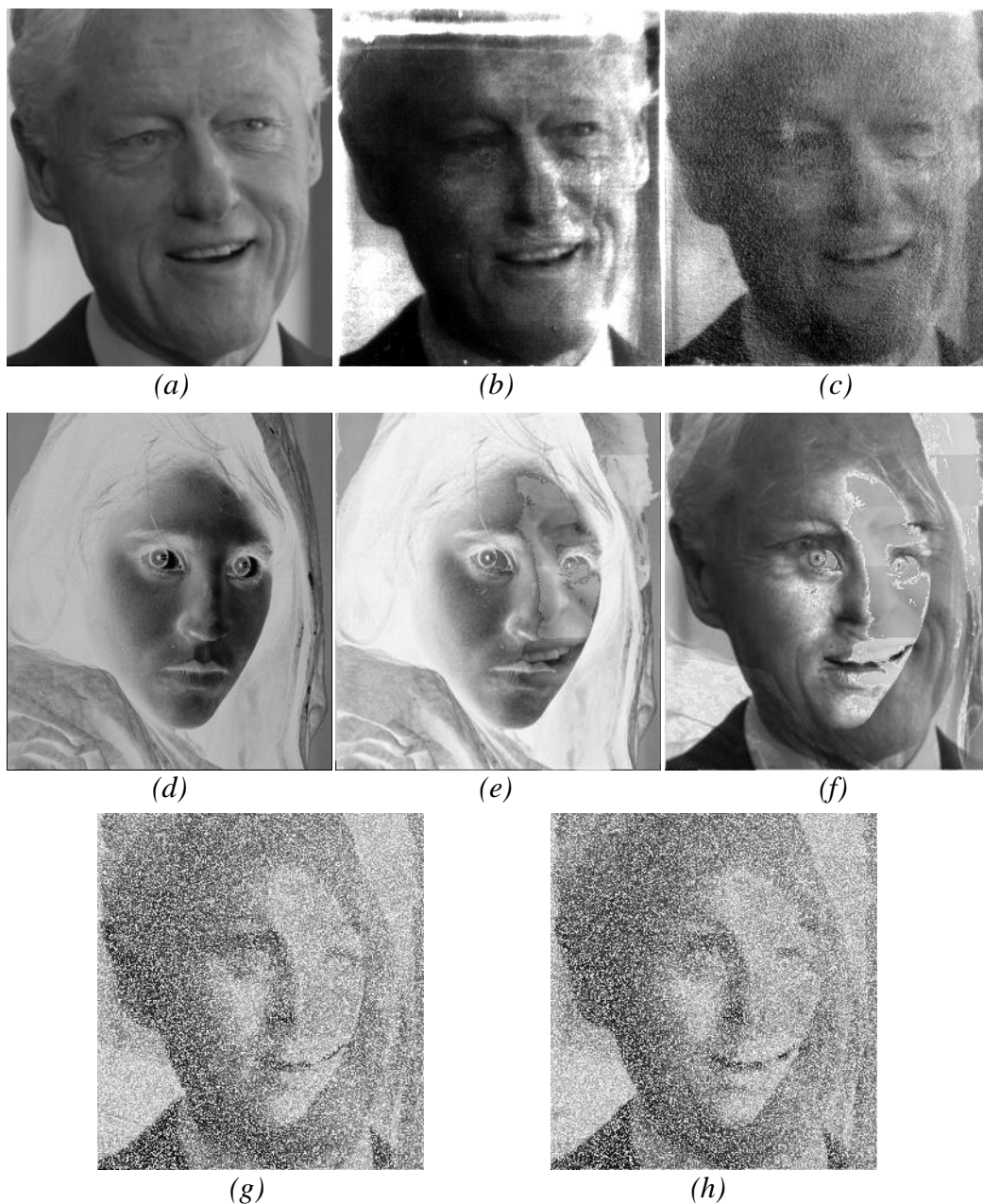


Figure 5.2: Encryption using Cover Image (a) Original secret image (b) Image Decrypted from e and f (c) Image Decrypted from e, g and h (d) Cover Image (e) 1st Share image of a (f) 2nd share of a image (g) 1st Share image of f (h) 2nd share image of f

The *Figure 5.2* above depicts the result of image encryption using the cover image. Original secret image used here is again that of Bill Clinton which is encrypted to get two share images *e* and *f*. Firstly, the Cover image shown in *d* is directly

assigned as 1st Share of a . Then pixels values of 1st share are increased if it is less than the corresponding pixel value in original image. Then pixel intensities of 2nd Share are evaluated using a and e without any pixel swapping. Overlapping e and f results the decrypted image b .

The Correlation Coefficients calculated by comparing a with b , e and f were 0.83, 0.15 and 0.79 respectively. Here we see that one share is much less correlated with original image but other is much correlated. So, further encryption of f is preferable.

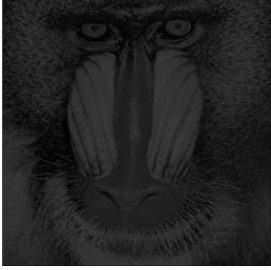
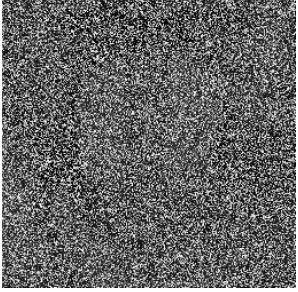
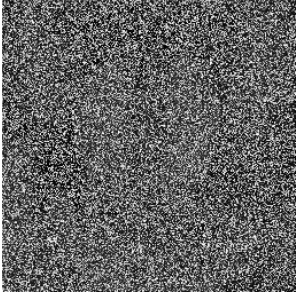

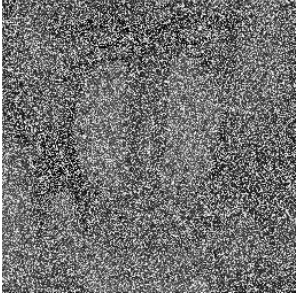
Further encryption of f without using any cover image results the shares g and h and overlapping of e , g and h results the decrypted image c . The Correlation Coefficients calculated by comparing a with c , g and h were 0.75, 0.40 and 0.41 respectively.

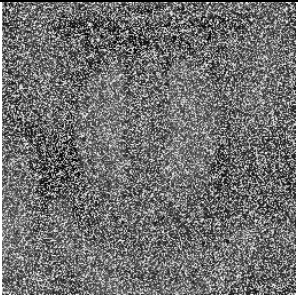

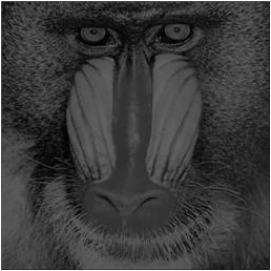


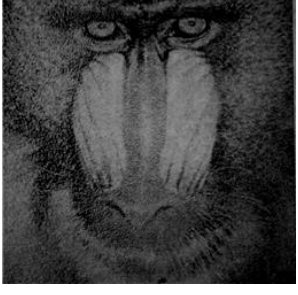
Considering the generation of only two shares, PSNR, MSE and SSIM are also calculated for different images taking different values of Transparency factor (α). *Tables 5.1, 5.2, 5.3, 5.4 and 5.5* give the analysis results of different images with various α values and for different images.

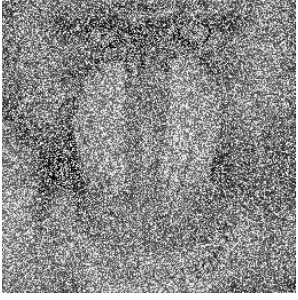
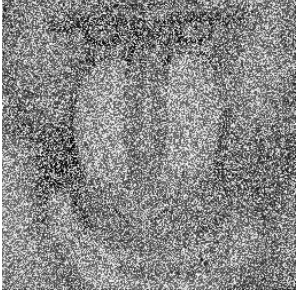

Table 5.1 shows the variation in result for baboon image of low and high contrast and for different α values. We see that, that if the Cover image is not used then the shares generated are highly sensitive to the value of α and the contrast of original image. High Contrast image reveals more information in the shares. Also, using higher values of α generates shares which are more similar to original image. But, it should be noted that if lower value of α is taken then quality of the regenerated image degrades.

Also by analysing *eqn. 2.2*, we can say that, taking lower value of α is like lowering the image contrast of decrypted image, which in turn will degrade the image quality.

Table 5.1: Similarity analysis with various alpha values for Baboon Image

Original Image	Alpha	Shares & Decrypted Image (Every 3 rd)	XC OR	PSNR	MSE	SSIM
 <p>Low Contrast Original Image Baboon (Encrypted using Pixel Swap Only)</p>	0.5		0.07	8	10168	0.02
			0.06	8	10276	0.017
			0.16	19	821	0.318
	0.95		0.15	8	10528	0.04


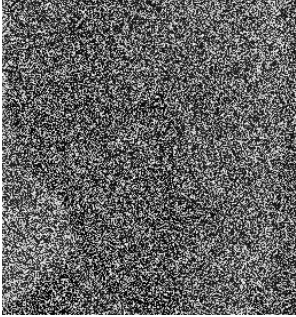
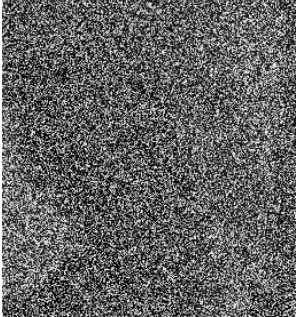
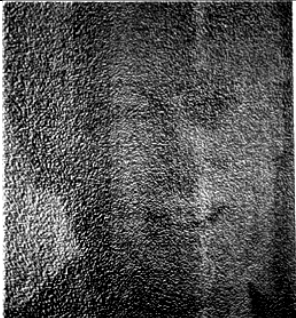
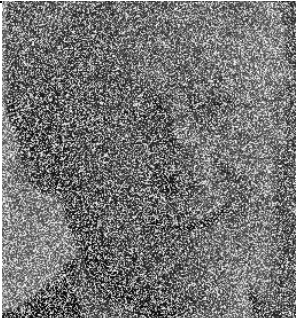
			0.13	8	10635	0.03
			0.32	19	901	0.32
 Low Contrast Original Image Baboon (Encrypted using Pixel Swap Only)	0.95		0.54	11	4947	0.49
			0.53	11	4987	0.49
			0.56	20	566	0.52

			0.28	11	4676	0.26
	0.5		0.28	11	4668	0.26
			0.55	22	390	0.6

Similar result as in *Table 5.1* can be observed in *Table 5.2* in which image of Bill Clinton is encrypted using pixel swapping technique only. For $\alpha = 0.1$, SSIM for shares is a very low value of 0.08. But the decrypted image with 0.25 SSIM index is too unclear. Whereas, For $\alpha = 0.9$, Shares themselves reveals much information about secret image with the SSIM index of 0.3.

So, if only pixel swapping technique is used then we must find the optimum mid-way which is at about $\alpha = 0.5$ i.e. for better encryption, we must negotiate on the quality of the decrypted image. If $\alpha = 0$ is taken then the reconstructed image will be completely dark, so it is very important to choose α at least 0.5. Higher the value of α , greater the quality of decrypted image i.e. the final reconstructed image has more details of original image conserved in it.

Table 5.2: Similarity analysis for encryption using pixel swap only

Original Image	Alpha	Shares & Decrypted Image (Every 3 rd)	XC OR	PSNR	MSE	SSIM
 Bill Clinton (Encrypted using Pixel Swap Only)	0.1		0.11	9	8015	0.08
			0.1	9	8020	0.08
			0.26	16	1570	0.25
	0.5		0.22	9	6784	0.16

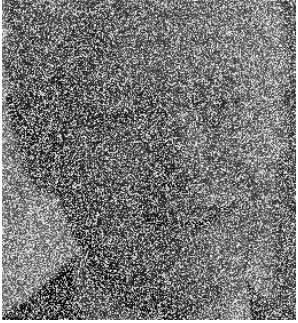













			0.22	9	6701	0.17
			0.29	16	1519	0.27
	0.9		0.4	9	7298	0.3
			0.4	9	7348	0.3
			0.64	19	724	0.6

Table 5.3 shows the result of using Cover Image for generation of shares. We can see that, if Cover image is used then shares are not much affected. Although the SSIM index slightly differs for different alpha value chosen, XCOR for all 2nd shares are the same. Actually, the share 2 only gets dim and we can say shares are almost insensitive to alpha value.

Table 5.3: Similarity analysis for encryption using cover image only


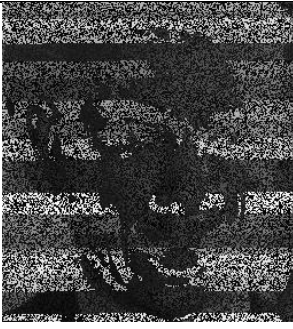
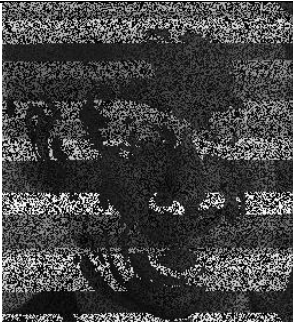
Original Image	Alpha	Shares & Decrypted Image (Every 3 rd)	XCOR	PSNR	MSE	SSIM
 <p>Bill Clinton (Encrypted using Cover Image of Barak Obama)</p>	0.1		0.4	8	10119	0.165
			0.18	11	4582	0.08
			0.2	14	2791	0.164






	0.5		0.4	8	10119	0.165
			0.18	16	1567	0.18
			0.59	16.2	1554	0.41
	0.9		0.4	8	10119	0.165
			0.18	9	8792	0.094



			0.69	18	1059	0.6
--	--	------------------------------------------------------------------------------------	------	----	------	------------

Table 5.4 shows the result of mixing both the techniques of pixel swapping and use of cover image. But results show that this is not a good idea. The random swapping of pixels tends to reveal information on shares even at lower alpha values.

Table 5.4: Similarity analysis for encryption using pixel swap and cover image

Original Image	Alpha	Shares & Decrypted Image (Every 3 rd)	XC OR	PSNR	MSE	SSIM
 Bill Clinton (Encrypted using both Pixel Swap and Cover Image of Barak Obama)	0.1		0.22	11	5230	0.13
			0.22	11	5266	0.12







			0.35	14	2500	0.27
	0.5		0.29	11	5222	0.17
			0.28	11	5236	0.17
			0.62	19	778	0.61
	0.9		0.3	9	8913	0.14





			0.3	9	8881	0.14
			0.66	19	710	0.6

So, we see that the value of alpha and the contrast of original images are important parameters determining the quality of the reconstructed image. Being able to choose higher alpha value without adding up extra information in the share image about secret is advantageous as this will produce the high quality decrypted image. Also, only these indices like XCOR, PSNR, MSE and SSIM are not the perfect measures of the visual similarity between two images. SSIM seems to be near but is still not perfect and so parallel human observation is also required.

Table 5.5 shows other results of visual cryptography using pixel transparency and the cover image. First image is of the Social activist and founder and director of Maiti-Nepal, Anuradha Koirala encrypted using the cover image of another social activist Dilshobha Shrestha. Here the two shares are unrecognizable, SSIM index of shares are also low and overlapping the shares reveals the original image. Similarly, second image of famous superintendent of Nepal Police, Ramesh Kharel encrypted using cover image of famous Nepalese teacher Mahabir Pun. Results shows quiet dissimilarity between original image and shares whereas decrypted image is similar to original.

Table 5.5: Other Similarity analysis results

Original Image and Cover image	Alpha	Shares & Decrypted Image (Every 3 rd)	XC OR	PSNR	MSE	SSIM
 Anuradha Koirala (Original Image)	1.0		0.37	9	8291	0.1
			0.2	6.6	14204	0.04
			0.6	21	424	0.62
 Dilshobha Shrestha (Cover image)						
	1.0		0.45	8	8522	0.25

 <p>Ramesh Kharel (Original Image)</p>			0.4	9	7665	0.2
 <p>Mahabir Pun (Cover image)</p>			0.8	21	464	0.7

5.2 Comparison with previous works

Y.-C. Zeng and C.-H. Tsai [5] also uses the image transparency for visual cryptography but the authors generate first share completely randomly. The second share is generated by calculating each pixel values of second share using *eqn. 2.2*. The main defect in this approach is that the result is highly sensitive to transparency factor (Alpha). The *Table 5.2* and *Table 5.3* shows the Cross Correlation values and SSIM Indices respectively for different alpha values for shares of image of Bill Clinton generated by three different methods.

- Using Pixel Swap Only (ie. completely random generation of share 1)
- Using Cover Image Only
- Using Both Pixel Swap and Cover Image

And *Figure 5.3* and *Figure 5.4* are the line plots of Cross Correlation and SSIM versus the Alpha value as given in *Table 5.2* and *Table 5.3*. Result shows that, if proper cover image is chosen, such that the shares are visually dissimilar to original image, then much higher quality decrypted image is reconstructed. Also, the share images will be insensitive to the value of alpha chosen.

Table 5.6: Sensitivity of Cross-Correlation in different methods with Alpha

Alpha	Using Pixel Swap Only	Using Cover Image Only	Using Both Pixel Swap and Cov. Img.
0.1	0.07	0.18	0.22
0.2	0.1	0.18	0.22
0.3	0.14	0.18	0.25
0.4	0.18	0.18	0.26
0.5	0.2	0.18	0.27
0.6	0.26	0.18	0.29
0.7	0.3	0.18	0.29
0.8	0.35	0.18	0.3
0.9	0.4	0.18	0.3
1	0.44	0.18	0.3

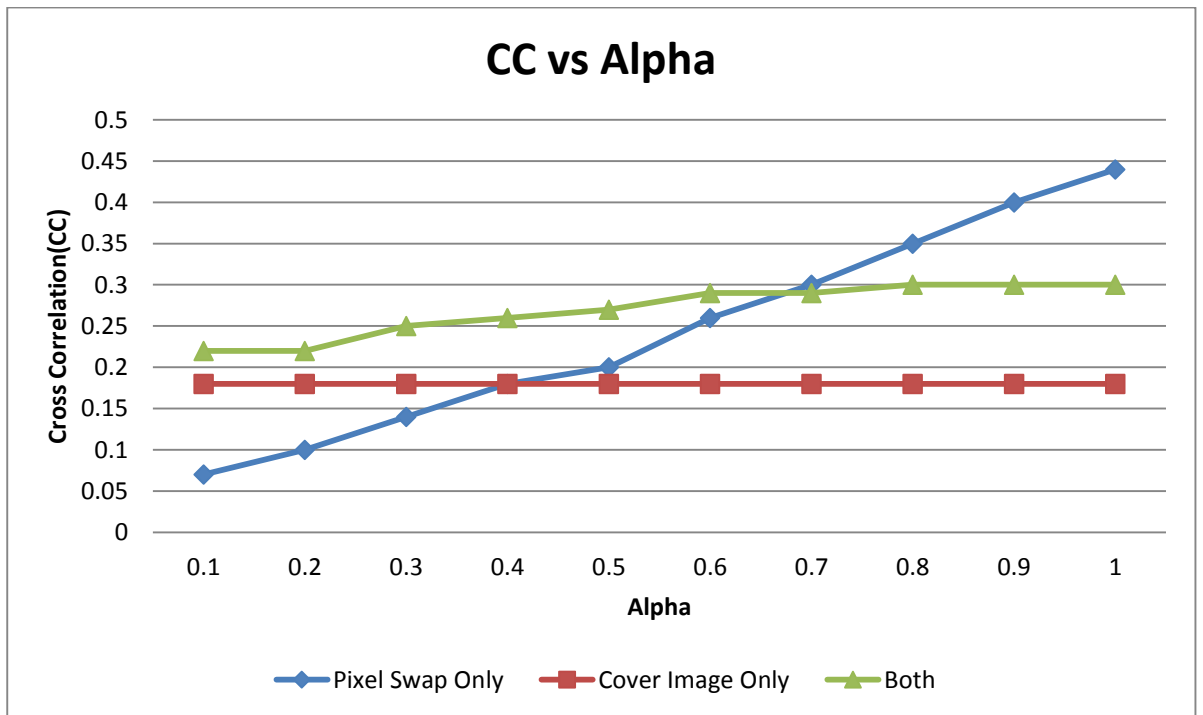


Figure 5.3: Cross-Correlation vs Alpha for different methods

Table 5.7: Sensitivity of SSIM in different methods with Alpha

Alpha	Using Pixel Swap Only	Using Cover Image Only	Using Both Pixel Swap and Cov. Img.
0.1	0.05	0.09	0.13
0.2	0.08	0.17	0.13
0.3	0.1	0.2	0.15
0.4	0.14	0.21	0.15
0.5	0.17	0.18	0.17
0.6	0.2	0.16	0.15
0.7	0.23	0.13	0.16
0.8	0.26	0.11	0.16
0.9	0.29	0.09	0.14
1	0.31	0.08	0.13

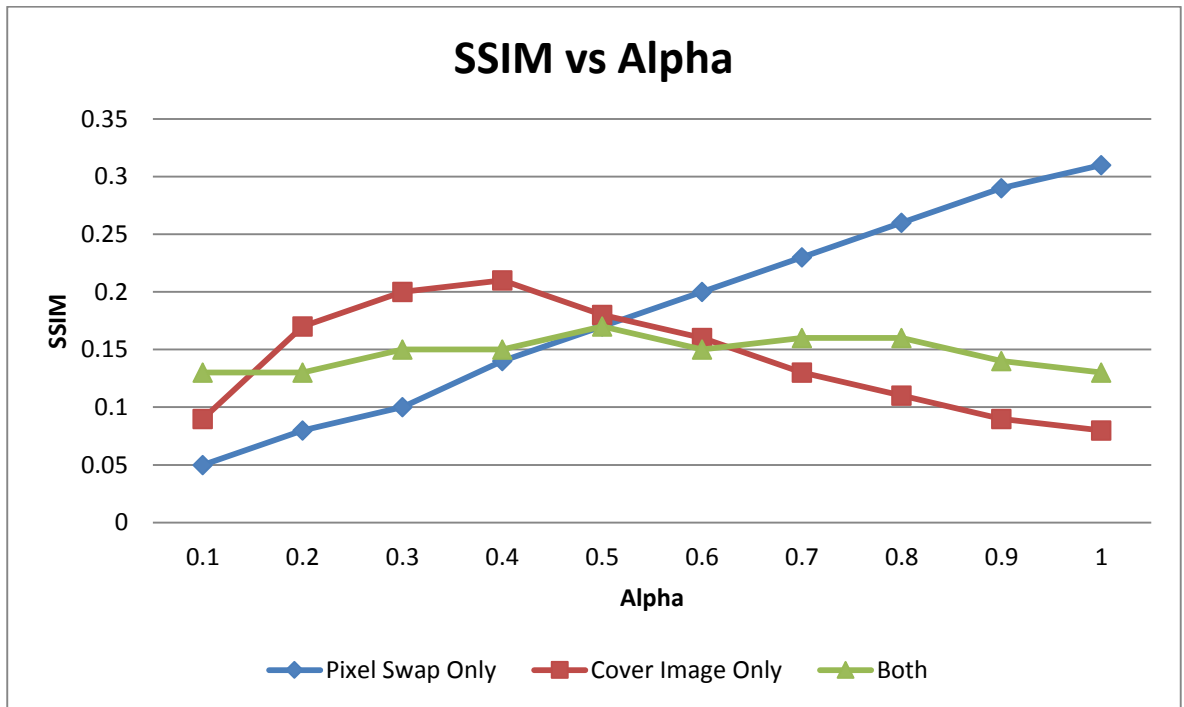


Figure 5.4: SSIM vs Alpha for different methods

5.3 Complexity Analysis

For the generation of shares, the algorithm goes through each pixels of the image. Supposing that the image is of size $m \times n$, then there is a loop to go through each columns and nested loop for each pixels in a row of every columns. As many such loops are there sequentially but no further nested loop, so for just the generation of shares, algorithm complexity is $O(m*n)$.

For the similarity analysis, broadly analysing the equations 3.1, 3.2, 3.3 and 3.4, all of these has loops with maximum $m*n$ steps i.e. similarity analysis also has complexity of $O(m*n)$. So, overall complexity for single run is $O(2*m*n)$ which is again $O(m*n)$

If the system is to be run k times producing $k+1$ Shares, then the complexity will be $O(k*m*n)$. But generating more than 4 shares is not efficient for decryption as the decryption is to be done mechanically. So limiting the value of k to 3, the complexity becomes $O(3*m*n)$, which again gives the complexity of $O(m*n)$.

CHAPTER SIX
CONCLUSION AND RECOMMENDATION

6.1 Conclusion

Many previous researches had been carried out in the field of visual cryptography. The use of pixel transparency in this field reduces the complexity increasing the efficiency in terms of share image size and quality of regenerated image. The generation of share completely randomly has some limitation as it is sensitive to transparency factor (α) chosen.

The proposed technique of generating share using another cover image is insensitive to transparency factor and so it can give better quality decrypted image with share images that do not reveal information about original image.

Thus, Visual Cryptography using pixel transparency and cover image can generate encrypted shares that do not take much space, do not reveal secret information and can regenerate better quality decrypted image.

6.2 Recommendation

In this thesis, cover images are selected in trial and error basis and very less pre-processing is done with cover image. Further enhancement to this work can be done by giving an algorithm to determine best cover image to hide given secret image. Usually, if the cover image is similar to secret image, then the output will be better.

Also, this thesis only does small adjustment in contrast of cover image making the range of intensity of cover image and secret image same. Cover image can be further pre-processed to make it more similar to secret image, provided it does not reveal any secret information.

REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography", *Eurocrypt 1994, Lecture Notes in Computer Science*, vol.950, pp. 1-12, Springer-Verlag, 1994
- [2] Z. Zhou, G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography", *IEEE Trans. Image Process.*, vol. 15, no. 8, pp.2441-2453, 2006
- [3] Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via direct binary search", Proc. EUSIPCO'06, Florence, Italy, Sep. 2006
- [4] T. M. Alkharobi, A. K. Alvi, "New Algorithm For Halftone Image Visual Cryptography", *IEEE 2004*
- [5] Y.-C. Zeng and C.-H. Tsai "Controllable transparency image sharing scheme for grayscale and color images with unexpanded size", *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2013 Asia-Pacif*, pp. 1-4, 2013
- [6] Y.-C. Hou, "Visual cryptography for color images", *Pattern Recognition*, vol. 36, iss. 7, pp. 1619–1629, 2003
- [7] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *Proc. WSCG Conf. 2002*, pp. 303–412, 2002

APPENDIX

Some more results of different image encryptions.

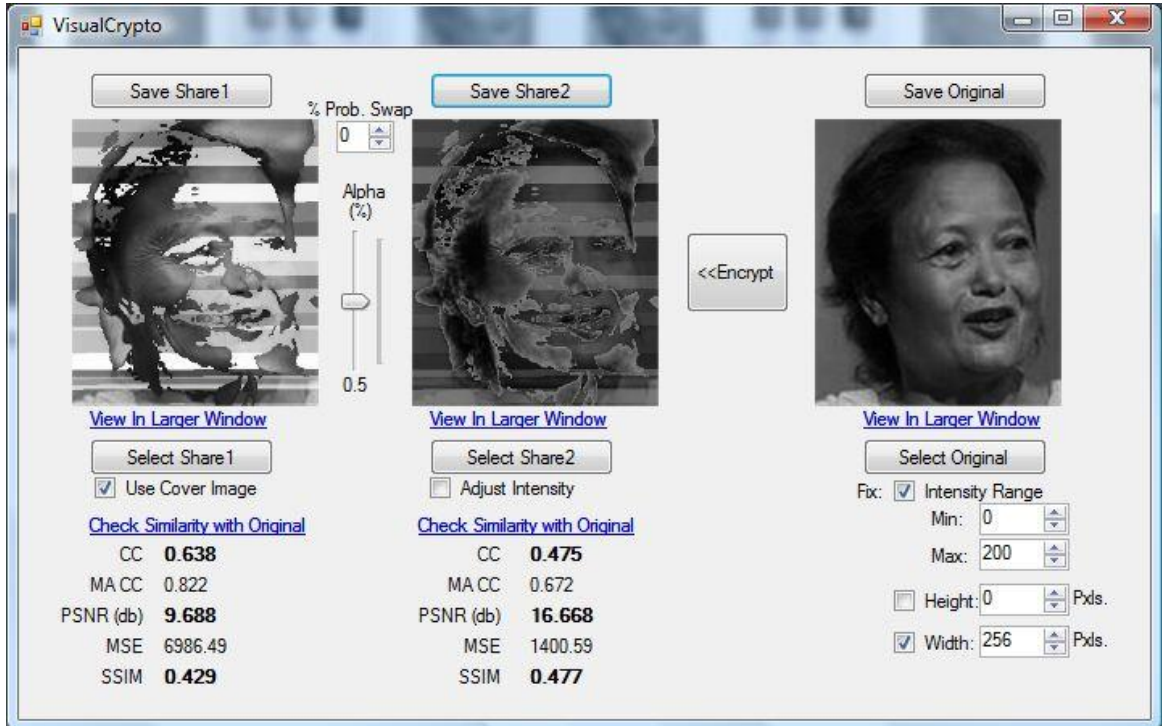


Figure 8.1: Generating shares for image of Dilshobha Shrestha

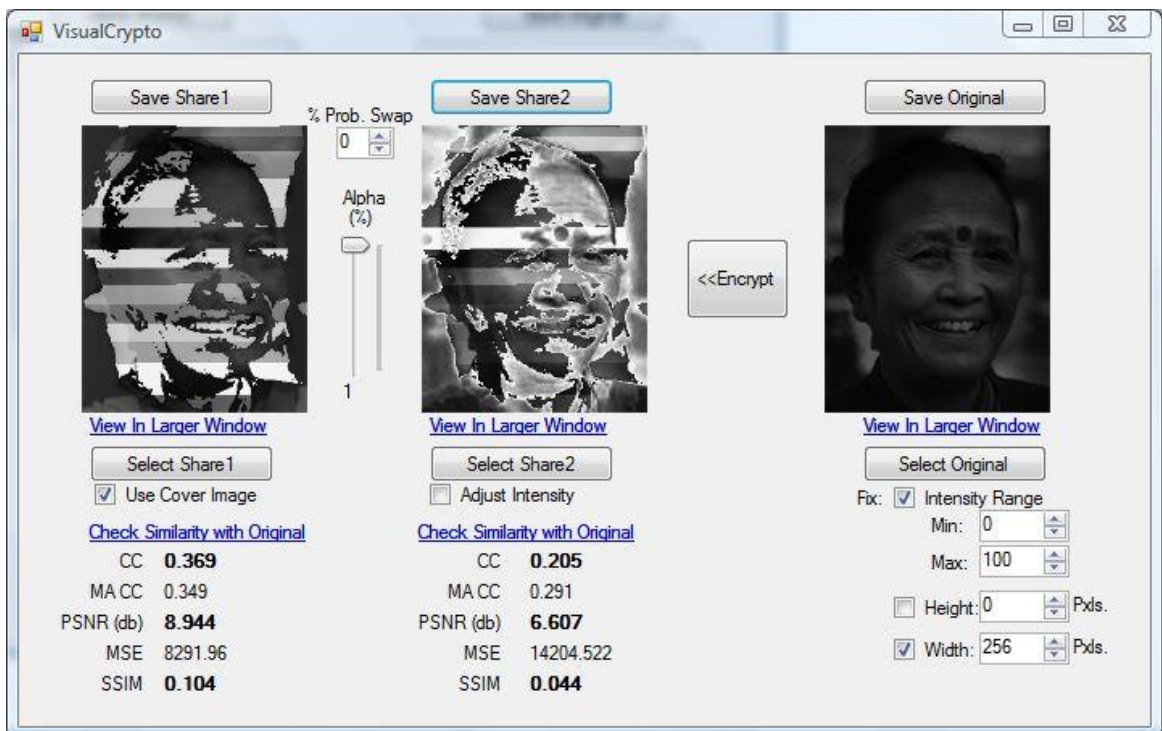


Figure 8.2: Generating shares for image of Anuradha Koirala

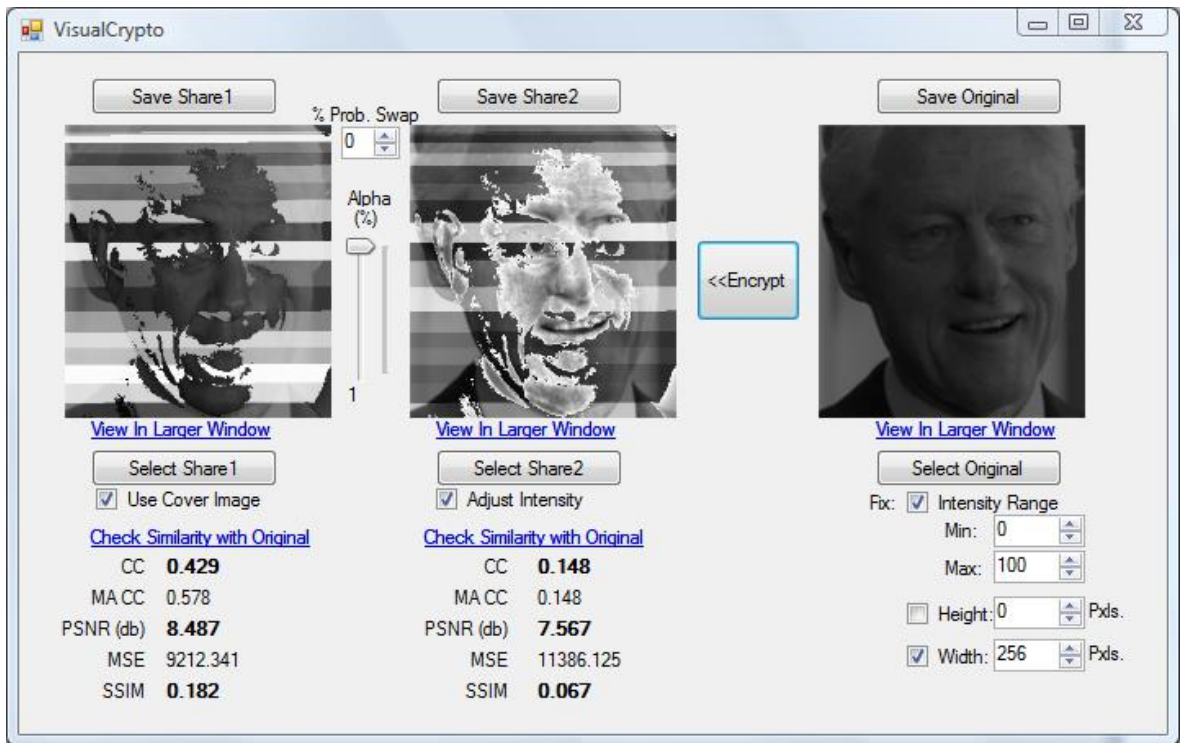


Figure 8.3: Generating shares for image of Bill Clinton

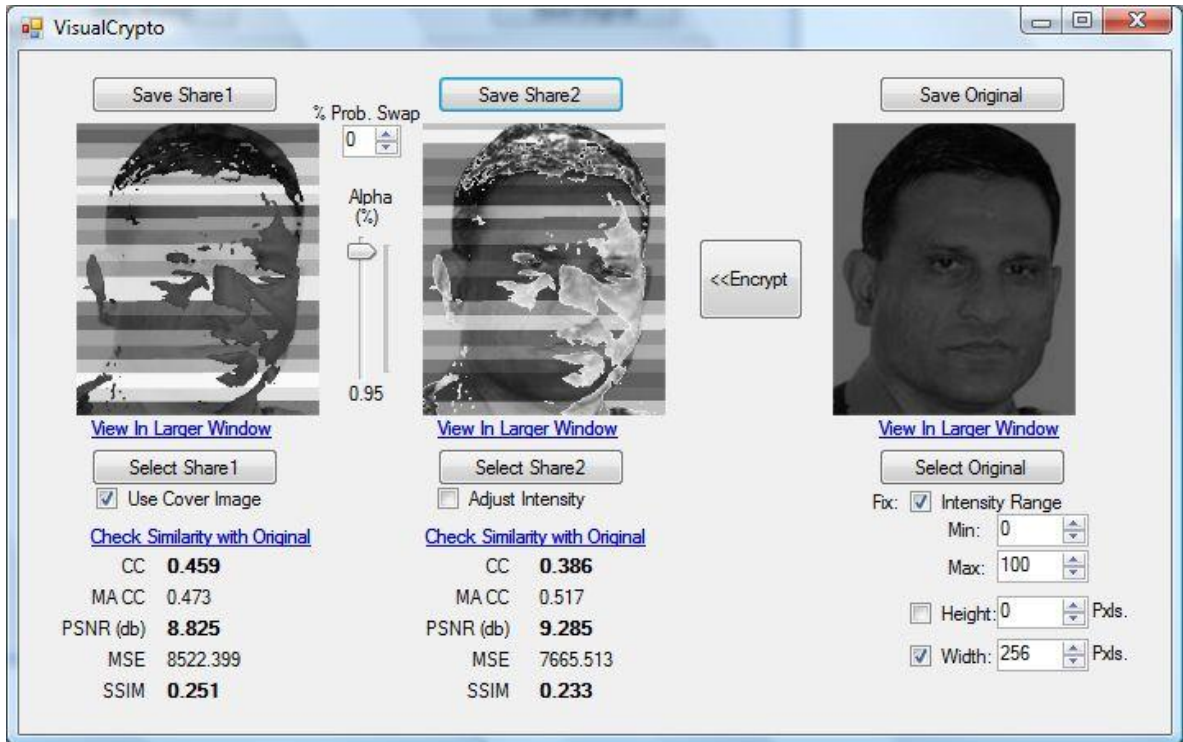


Figure 8.4: Generating shares for image of Ramesh Kharel

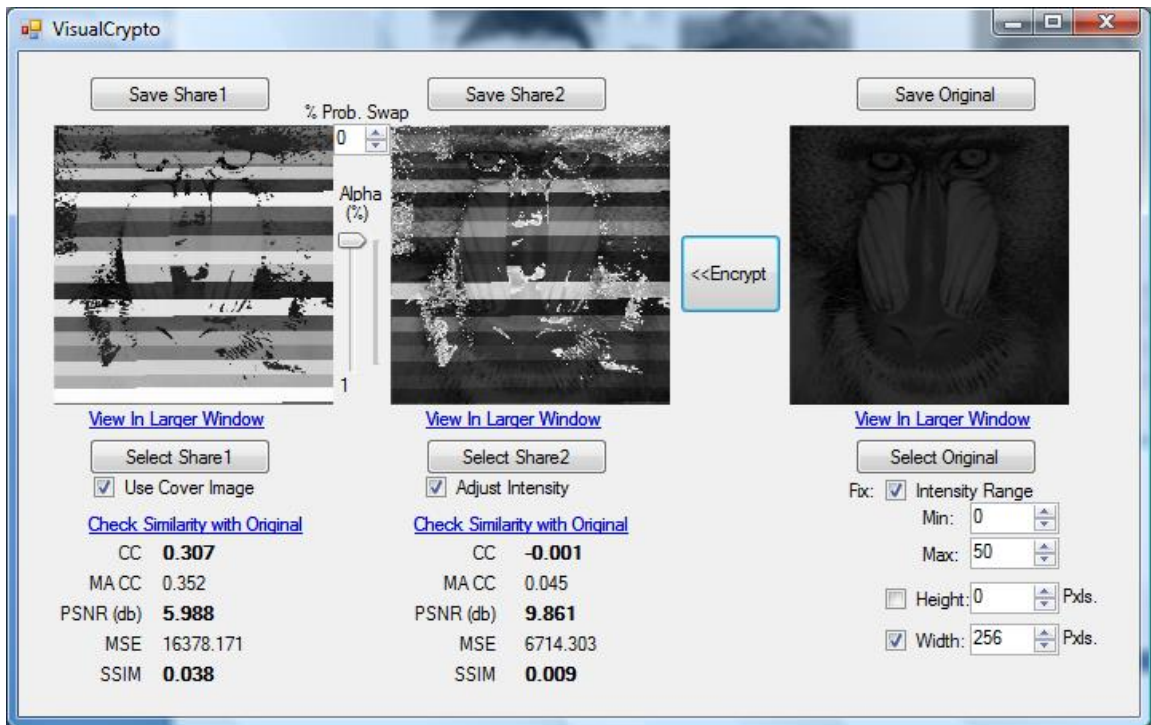


Figure 8.5: Generating shares for image of Baboon

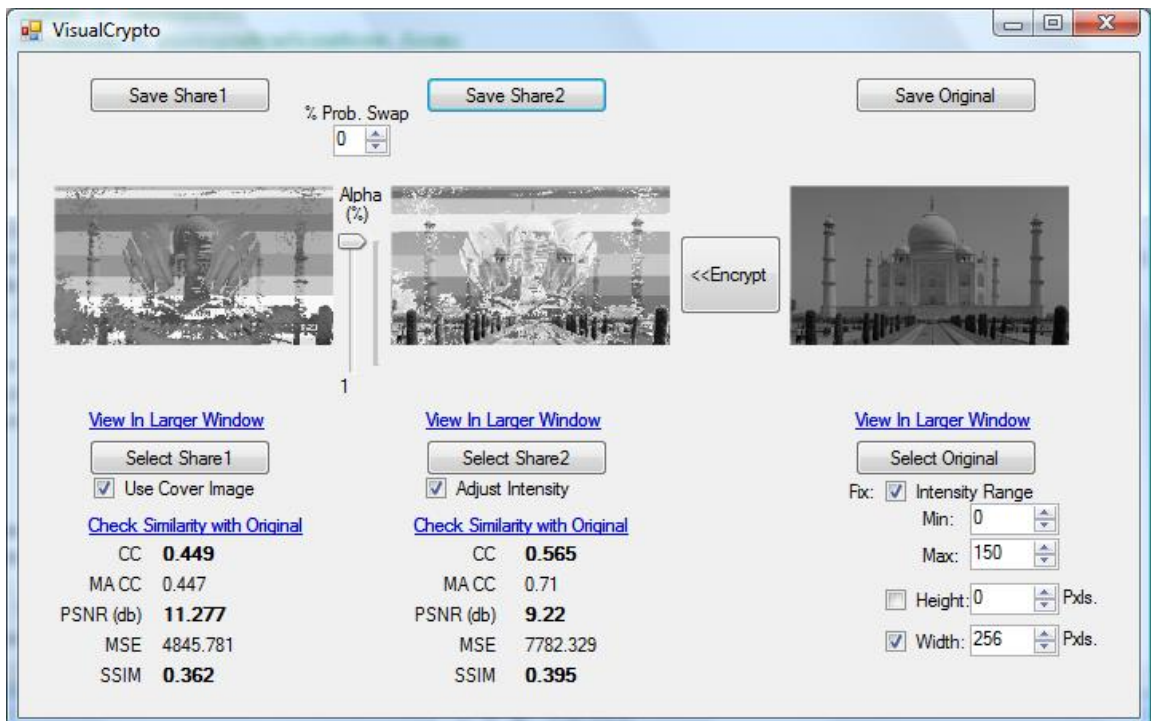


Figure 8.6: Generating shares for image of Taj Mahal