SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

College of graduate studies

College of Computer Science and Information Technology

Visual Cryptography Scheme for Color Images Using Arnold Mapping and Modified RSA Algorithm

مشروع التشفير المرئي للصور الملونة بإستخدم خرائط أرنولد المعدلةRSA و خوارزمية

A Thesis Submitted In Partial Fulfillment of the
Requirements of Master Degree in Computer Science

Proposed by:	**Supervision:**
Mai Omer Alsadeg Ali	Dr. Faisal Mohammed Abdallah Ali

December 2018

الآيـــــــــــــــــة

قال الله تعالى: ((قَالُواْ سُبْحَانَكَ لاَ عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ)).

صدق الله العظيم

سورة البقرة الآية (32)

الإهـــــــداء

إلى تلك التي تتقاصر دونها كل عبارات الوصف القلمية

أمي.....

إلى الذي إجتاز بي كل صعوبات الطريق وظل يكدح لأنال رضاه

أبي.....

Acknowledgements

To

My beloved parents, a precious thought to me.

To my brother and sister, whose cheerful patience

and constant encouragement made this project

Possible.

To my supervisor Dr. Faisal Mohammed Abdallah Ali

on the continuous support and his patience, motivation and knowledge, His guidance helped me in all the time to writing research.

also pleased to thank all those who contributed to the output of this work, especially my beloved friend Fatima Abdalla Elhag .

I dedicate this work to them all for the support,

encouragement, love and prayers that they have

always had for us.

My Allah blesses them all and grants them happiness

all through.

Abstract

Visual cryptography is one of the best techniques used to secure information. It uses the human vision to decrypt the encrypted images without any cryptographic computations, the basic concept of visual cryptography is splitting the secret image into shares such that when the shares are stacked, the secret image is revealed.

The Proposed Architecture extended visual cryptographic scheme for color images use Arnold Mapping to ensure that the share pixels are thoroughly scrambled and the random diffusion thoroughly scrambled to remove any correlation with the original image contents, thus it enhances the security of the proposed method.

Public key encryption technique makes image shares so secure that it becomes very hard for a third party to decode the secret image information without having required data that is a private key(attacker). Results show that the proposed method suggest an efficient way to encrypt a secret color image with better level of security and with a better value of Peak signal to noise ratio (PSNR), histogram comparisons were also deployed to show the robustness of the proposed cipher.

المستخلص

يعد التشفير البصري أحد أفضل التقنيات المستخدمة لتأمين المعلومات، ويستخدم الرؤية البشرية لفك تشفير الصور المشفرة دون أي حسابات تشفير، المفهوم الأساسي للتشفير البصري هو تقسيم الصورة السرية إلى طبقات بحيث عندما تكدس الطبقات يتم الكشف عن الصورة السرية.

البنية المقترحة هي تمديد نظام التشفير البصري للصور الملونة بأستخدم خرائط أرنولد للتأكد من أن كل بكسل فى الطبقات خلط بدقة وتوزع عشوائآ لإزالة أي علاقة مع محتويات الصورة الأصلية، وبالتالي فإنه يعزز أمن الطريقة المقترحة.

تعمل تقنية تشفير المفتاح العام على جعل طبقة الصور آمنة إلى الحد الذي يجعل من الصعب جدًا لطرف ثالث(المهاجم) فك تشفير معلومات الصور السرية دون الحاجة إلى بيانات مطلوبة وهي مفتاح خاص. وقد أظهرت النتائج أن الطريقة المقترحة والمحسنة فعالة لتشفير صورة ملونة سرية بمستوى أمان أفضل وبقيمة أفضل لنسبة الإشارة إلى الضوضاء، كما بينت مقارنات المدرج التكراري متانة التشفير المقترح.

Table of Contents

List of Tables

List of Figures:

List of Abbreviations

2D	Two dimensions
3D	Three dimensions
BMP	Windows Bitmap
GIF	Graphics Interchange Format
JPEG	Joint Photographic Experts Group format.
MSE	Mean Square Error
PK	Public Key
PNG	Portable Network Graphics
PPM	Portable Pix Map
PPM	Portable Pix Map format.
PSNR	Peak Signal to Noise Ratio
TIFF	Tagged Image File
VC	visual cryptography
`XWD	X Window Dump

Chapter One

Introduction

CHAPTER I

Introduction

1.1 Overview

The Internet is the fastest growing communication medium and essential part of the infrastructure, nowadays. To cope with the growth of internet it has become a constant struggle to keep the secrecy of information and when profits are involved, protect the copyright of data. To provide secrecy and copyright of data, many of the Cryptography techniques have been developed. But each of the technique has their respective pros and cons. Where one technique lacks in payload capacity, the other lacks in robustness. So, the main emphasis of cryptography is to overcome these shortcomings.

Pioneering innovation in securing and encrypting secret data against hacking are Naor and Shamir [1] In 1994, they proposed a visual cryptography(VC) scheme, which can decode concealed images without any complex cryptographic computations. Their basic model was used for black and white images where it generates n transparencies of the original secret image. Stacking only k (or more) of the n transparencies can reveal the original secret image. This model suffers from pixel expansion, where the size of the recovered secret image is not the same as the size of the original one. Many VC techniques have been proposed to recover black and white images and color images [1]. Moreover, several studies employ both cryptography and steganography to provide a high level of security for data transmission.

1.2 Research Significance

Enhance in the area Visual Cryptography Schemes for Image cryptography, which would require less computation and less storage.

1.3 Research Problem

Color images represent one of the most popular types of files transmitted on the Internet. Images contents require sufficient level of confidentiality to protect the images content from unauthorized use, violate privacy and theft attack, Visual cryptography is a common method, but it’s not robust and efficient to secure color pictures.

1.4 Research Objectives

This proposed presents an improved algorithm based on visual cryptography and Arnold Transform and modified RSA algorithm for colored image cryptography. This scheme to make visual cryptography algorithm more strong for image encryption and decryption process and lossless recovery and reduces the noise in images without adding any computational complexitys.

1.5 Research Methodology

The proposed method is a combination approach of Visual Cryptography and Arnold Transform and modified RSA algorithm, where we take the color image and changing the properties of the image itself and encrypting the produced parts of the images.

Five major steps are used followed in changing the image properties, firstly Extract the RGB components from the original image so as to produce three shares from that image, secondly Arnold Mapping is used to ensure that the share pixels are thoroughly scrambled and the random diffusion thoroughly scrambled after Visual step to remove any correlation with the original image contents, thus it enhances the security of the proposed method, thirdly Using RSA public key algorithm, and then this matrix is converted into aHexadecimal code that represents a color, to generate cipher share, fourthly decrypted cipher convert Hex code image to decimal and recovery Arnold transform and using RSA private key algorithm, finally used stack to get generate secret image.The proposed method is implemented in Java and Matlab for analysis.

1.6 Research Scope

Research activities in enhancement of algorithms have become more active research area, in this research select Visual cryptography scheme and Arnold transform and modified RSA algorithm as improvement algorithm.

In this research area there are many proposed method to implement to visual cryptography. The areas that contribute to the development of image encryption include the cryptography and Digital image Processing.

Employed for the encryption and the decryption process of the a color mages, in 2D.

1.7 Research Organization

Contain this research on the following chapters :

Chapter Two: Provides the critical literature review and comprehensive reports on the other works related to the topic of the thesis .We review the basic concepts of encryption schemes , RSA cryptosystem , visual cryptography and Arnold mapping technique.

Chapter Three: In this chapter we explain the basic concepts of digital images , specifically the colored images. In addition, this chapter included the proposed method used to encrypt the color image based on modified RSA and Arnold mapping technique .

Chapter Four : This chapter illustrate the implementation work done by Java` programming tool , also show the discussion of the important results of our thesis .

Chapter Five: This chapter concludes the results and analyzes whether the primary set up aims and objectives were met. Basically this chapter summarizes the thesis's achievements and findings.

Chapter Two

Literature Review and Related Works

CHAPTER II

Literature review and related works

2.1 Introduction

Security of data to maintain its confidentiality, proper access control, integrity and availability is a major issue in data communication. As soon as a sensitive message was etched on a clay tablet or written on the royal walls, then it must have been foremost in the sender's mind that the information should not get intercepted and read by a rival.

Today in the e-age, the need to protect communications from prying eyes is greater than ever before. Cryptography, the science of encryption plays a central role in mobile phone communication, electronic commerce, pay television , sending private e-mails, transmitting financial information and touches on many aspects of daily lives.

Today's technology can be traced back to earliest ciphers, and have grown as a result of evolution. The initial ciphers were cracked, so new, Stronger ciphers emerged.

Code breakers set to work on these and eventually found flaws, forcing cryptographers to invent better ciphers and so on. The significance of key is an enduring principle of cryptography. With the advent of the computer age, the mechanical encryption techniques were replaced with computer ciphers .They operated according to the same principles of substitution and transposition (where the order of letters or bits is altered). Again each cipher depended on choosing a key, known only by the sender and the receiver which defined how a particular message would be. This meant that there still was a problem of getting the key to the receiver so that the message could be deciphered. This had to be done in advance, which was an expensive slow and risky process

For years, this key distribution problem haunted code makers i.e. if you want to decipher a scrambled text you have to know the key in advance. But there was revolution in cryptography known as public key cryptography, which destroyed the key distribution problem. This was a technology tailor made for the internet. Customers could send credit card details and send them to retailers on the other side of the planet. It formed the basis of all kinds of modern day communications .

2.2 Overview

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication, so the main goals of cryptography are privacy or confidentiality, data integrity, authentication and non-repudiation[2].

Privacy or confidentiality is the service used to keep the content of information secret from all but those authorized one to have it. Secrecy, confidentiality and privacy are synonymous terms. There are number of approaches to providing conf identiality through mathematical algorithms which render data unintelligible.

Data integrity refers to the unauthorized manipulation of data. Data manipulation includes such things as insertion, deletion and substitution. It ensures the ability of detecting data manipulation by unauthorized parties.

Authentication is a service related to identification. This function applies to both entity authentication and data origin authentication. Two parties entering into a communication should identify each other. Moreover, information delivered over a channel should be authenticated as to origin of data, data content,time sent etc

Non-repudiation is a service which prevents an entity from denying previous commitments or action. When disputes arise due to an entity denying that certain actions are to be taken, a means to resolve the situation is necessary.

The term information security is much broader, encompassing such things like authentication and data integrity. The basic terms of information security areAn information security service is a method to provide some specific aspects of security. For example, integrity of transmitted date is a security objective, and a method to ensure this aspect is an information security service.

Breaking an information security service (which often involves more than simply encryption) implies defeating the objective of the intended service.

A passive adversary is an adversary who is capable only of reading information from an unsecured channel.

An active adversary is an adversary who may also transit, alert, or delete information on an unsecured channel.An encryption scheme is said to be breakable if a third party, without prior knowledge of the key, can systematically recover plaintext from corresponding cipher text within some appropriate time frame. An appropriate time frame will be a function of the useful life span of the data being protected[2].

2.2.1 Symmetric-key cryptography algorithms

Are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption)[4].

There are many examples of the public key cryptography such as RSA cryptosystem, Hellman cryptosystem and ElGamal cryptosystem.

Encryption and decryption with a symmetric algorithm

$$EK(M) = C \qquad (1)$$

$$DK(C) = M \qquad (2)$$

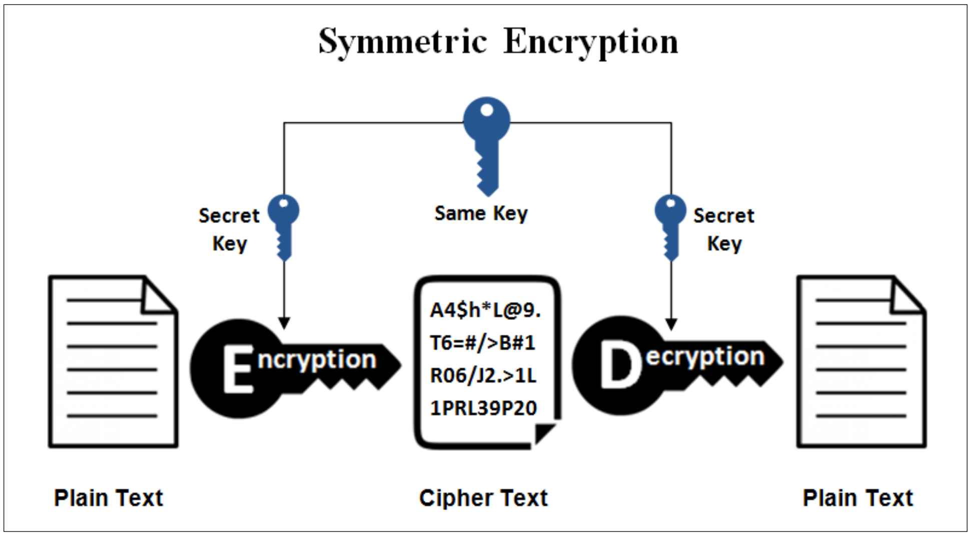


Figure2.1: Symmetric-key cryptography algorithms[3]

Symmetric algorithms can be divided into two categories. Some operate on the plaintext a single bit (or sometimes byte) at a time; these are called *stream algorithms* or *stream ciphers*. Others operate on the plaintext in groups of bits. The groups of bits are called *blocks*, and the algorithms are called *block algorithms* or *block ciphers*. For modern computer algorithms, a typical block size is 64 bits—large enough to preclude analysis and small enough to be workable. (Before computers, algorithms generally operated on plaintext one character at a time. You can think of this as a stream algorithm operating on a stream of characters)[3].

2.2.2 Asymmetric cryptography algorithms

Asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

In a public key encryption system, any person can encrypt a message using the receiver's public key. That encrypted message can only be decrypted with the receiver's private key. To be practical, the generation of a public and private key -pair must be computationally economical. The strength of a public key cryptography system relies on the computational effort (work factor in cryptography) required to find the private key from its paired public key. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security[3].

Encryption using public key K is denoted by

$$EK(M) = C \qquad (3)$$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by:

$$DK(C) = M \qquad (4)$$

Sometimes, messages will be encrypted with the private key and decrypted with the public key; this is used in digital signatures. Despite the possible confusion, these operations are denoted by, respectively

$$EK(M) = C \qquad (5)$$

$$DK(C) = M \qquad (6)$$

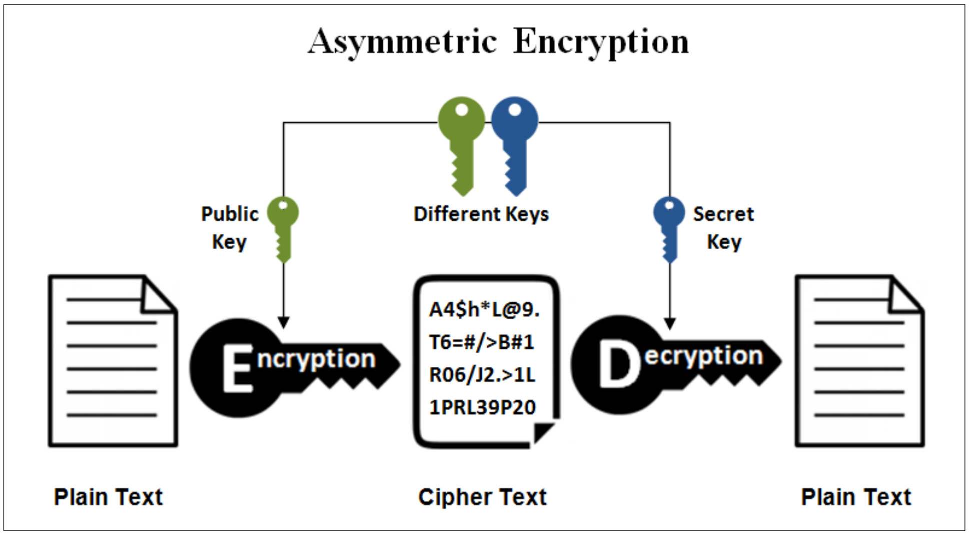


Figure 2.2 : Asymmetric cryptography algorithms[3]

2.3 Encryption

Encryption is covered by information science (which is simple text when stored on different storage media or when transferred on plaintext networks so that it becomes unreadable to anyone other than those who have special knowledge or special key to restore) Converting encrypted text into readable text , This decryption process is performed by the so-called cryptographic key, which, as a result of the encryption process, becomes encrypted and is not available to anyone for military, political or security purposes.

2.3.1 Classical Encryption Techniques

The techniques are the basic approaches to conventional encryption today. the two basic components of classical ciphers are substitution and transposition. then other systems described that combines both substitution and transposition.

- Substitution techniques

In this technique letters of plaintext are replaced by or by numbers and symbols.If Plain text is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

-Caesar Cipher

Caesar Cipher replaces each letter of the message by a fixed letter a fixed distance away e.g. uses the third letter on and repeatedly used by Julius Caesar.

- Playfair Cipher

The Playfair is a substitution cipher invented by Charles Wheatstone in around 1854. It was developed for telegraph secrecy and it was the first literal digraph substitution cipher.

This method is quite easy to understand and learn but not easy to break, because you would need to know the “keyword” to decipher the code. the system functions on how letters are positioned in a 5*5 alphabet matrix, a“KEYWORD” sets the pattern of letters with the other letters the cells of the matrix in alphabetical order (I and j are usually combined in one cell)[4].

- Poly-alphabetic Cipher

A poly-alphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. Mono-alphabetic Cipher can be broken. the reason is same plain letters are encoded to same cipher letters; the underlying letter frequencies remain unchanged.

Cryptographers have tried to overcome this dilemma simply by assigning various cipher letters or symbols to same plain letters. Such ciphers are called Poly-alphabetic Ciphers, The most popular of such ciphers is the “Vigenère Cipher”[4].

- Vigenère algorithm

The Vigenère cipher, proposed by Blaise de Vigenère from the court of Henry III of France in the sixteenth century, the Vigenère cipher is an improvement of the Caesar Cipher key is multiple letters long K=k1, K2, k3….kd [4].

2.3.2 Transposition Ciphers

The transposition cipher , the characters remain unchanged but their positions are changed to creat the cipher text transposition cipher is also not avery secure approach . the attacker can find the plain text by trial and error utilizing the idea of the frequency of occurrence of characters[4].

2.4 RSA Cryptosystem

The RSA cryptosystem is a public key cryptosystem, invented by three cryptologists who are Ron Rivest, Adi Shamir, and Len Adleman in 1970s , The RSA is used for providing privacy, ensuring authenticity of digital data, electronic credit and debit cards payment systems, and commercial systems such as Web servers and browsers to secure Web traffic. Therefore, RSA is used in many applications where the security of digital data in the concern [5].

The RSA cryptosystem has two corresponding keys that are a public key and a private key. The public key can be announced publicly and is used for encrypting a plaintext or image. However, the corresponding secret key will be used to decrypt the cipher text [5].

2.4.1 The RSA Keys Generated

- Each person chooses two large prime numbers p and q to form R=pq.
- Find the Euler's phi-function $\varphi(R) = \varphi(pq) = \varphi(p)\,\varphi(q)=(p-1)(q-1)$.
- Everyone chooses two positive integers e and d such that d is an inverse of e modulo $\varphi(R)$.
- Everyone announces the pair (e, R) to be their public key and keeps is the pair (d, R) secret, which is their private key.

2.4.2 The Encryption RSA

The intended receiver's public key (e, R) is used by a sender.

To encrypt a plaintext that could be a message or an image, the sender translates the letters into their numerical equivalents (if needed) and then forms plaintext blocks, X, such that a nonnegative integer X less than R.

Sender uses the following encryption algorithm to encrypt X: E(X) =Y≡ X^e (mod R). This Y is the corresponding ciphertext to X and is sent to the receiver

2.4.3 The Decryption RSA

To decrypt the ciphertext block Y, the following decryption algorithm is applied on every block Y: D(Y)=X≡ (Y)d (mod R).

2.4.4 The Security RSA

The security of the RSA cryptosystem relies on the integer factorization problem to find the secret key (d, R), which many cryptologists try to recover [5]. If anyone can get the factors p and q of R, then it is so easy to find φ (R) and d and since e is known. Many studies showed that if R is a large composite number, then it is hard to obtain the prime factors of R. Thus, hacking or cracking the RSA cryptosystem by factoring R would not be easy, and it is a conjecture in mathematics. Nevertheless, there might other ways to obtain d. It can be obtained by finding φ(R) from R, such that find φ(R)= φ(pq)= φ(p) φ(q)=(p-1)(q-1). Then p and q , that factorize R, can be found easily. Note that finding φ(R) is not easier that factoring R. Moreover, when p and q both have approximately 300 decimal digits, R=pq has approximately about 600 decimal digits. Using the fastest factorization algorithm to factor an integer of this size, more than millions of years of computer time are required to factor it[5].

2.5 Visual Cyptography Background

The initial awareness of Visual Cryptography VC was raised by Naor and Shamir in 1995. As a powerful technique for information security, VC indicates the possibility of visually protecting crucial secrets from the view of secret sharing . Unlike commonly used security methods which tend to hide information by applying mathematical transformation on secret in the format of plain text, Visual Cryptography Scheme VCS is defined as an activity that a secret is stored in an image (usually black and white). In VC secret image is split into several images called VC shares. Different from traditional secret sharing where each of participants has the knowledge of part of the secret, every piece of VC shares has no indication of the original secret image while viewers are solely able to clearly perceive the secret by simply overlaying these shares[6] .

The visual cryptography schemes VCS describe the way in which an image is encrypted and decrypted. There are different types of visual cryptography schemes . For example, there is the k-out-of n scheme that says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image. If the number of shares stacked is less than k, the original image is not revealed. The other schemes are 2-out-of-n and n-out-of-n VCS. The most of the constructions of visual cryptography schemes are realized using two n × m matrices. The general method for the construction is discussed below.

2.5.1 Visual Cyptography Basic Model

The basic model of visual cryptography proposed by Naor and Shamir [8]. accepts binary image 'I' as secret image, which is divided into 'n' number of shares. Each pixel of image 'I' is represented by 'm' sub pixels in each of the 'n' shared images. The resulting structure of each shared image is described by Boolean matrix 'S' Where S=[Sij] an [n x m] matrix Sij=1 if the jth sub pixel in the ith share is Black Sij=0 if the jth sub pixel in the ith share is White When the shares are stacked together secret image can be seen but the size is increased by 'm' times. The grey level of each pixel in the reconstructed image is proportional to the hamming weight H(V) of the OR – ed Vector 'V', where vector 'V' is the stacked sub pixels for each original pixel. A solution of the 'n' out of 'n' visual secret sharing consists of two collections of n x m Boolean Matrices C0 and C1 .To share a white pixel, randomly choose one of the

matrices from C0, and to share a black pixel, randomly choose one of the matrices from C1.The following conditions are consideredfor the construction of the matrices:

1. For any 'S' in C0, the OR-ed 'V' of 'n' rows satisfies H(V) _n-_m.

2. For any 'S' in C1, the OR-ed 'V' of any 'n'

rows satisfies H(V) _n.By stacking fewer than 'n' shares, even an

infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black. Let us describe the construction of matrix for (n, n) visual cryptography for n=3. C0= {all the matrices obtained by permuting the columns complement of [BI]} C1= {all the matrices obtained by permuting the columns of [BI]}Where,B is the matrix of order n x (n-2) which contains only ones

I is the identity matrix of order n x n

For n =3 B $\begin{vmatrix}1\\1\\1\end{vmatrix}$ and I = $\begin{vmatrix}1&0&0\\0&1&0\\0&0&1\end{vmatrix}$

Hence C1= $\begin{vmatrix}1&1&0&0\\1&0&1&0\\1&0&0&1\end{vmatrix}$

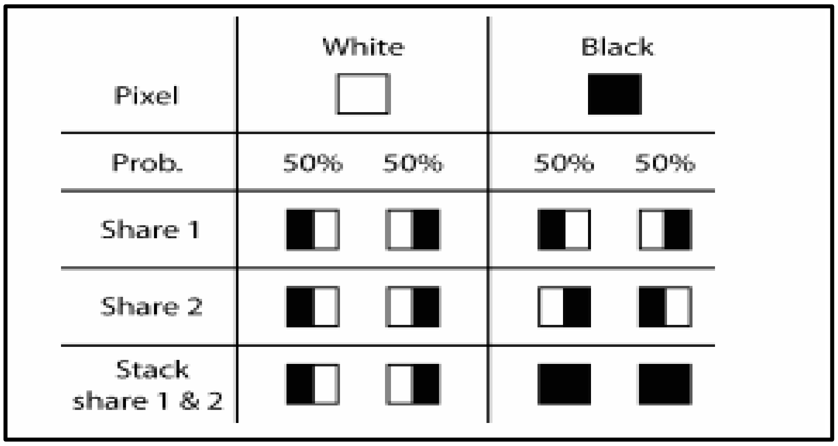
and C0 = $\begin{vmatrix}0&1&1&1\\0&1&0&1\\0&1&1&1\end{vmatrix}$

The basic model was then extended to (k, n) threshold cryptography where any ‘k’ or more shares will reveal the secret image. The construction of ‘k’ out of ‘n’ visual secret sharing is similar to the basic model with one difference. That is in basic model the threshold value is n where as here it is k which is the subset of n.

2.5.2 k out of k visual cryptography scheme

In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption process is performed by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic

computations. In the above basic VC scheme each pixel ‘p’ of the secret image is encrypted into a pair of sub pixels in each of the two shares. If ‘p’ is white, one of the two columns under the white pixel in Fig. 1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image. By stacking the two shares as shown in the last row of Fig. 1, if ‘p’ is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If ‘p’ is black, it outputs two black sub pixels[6].

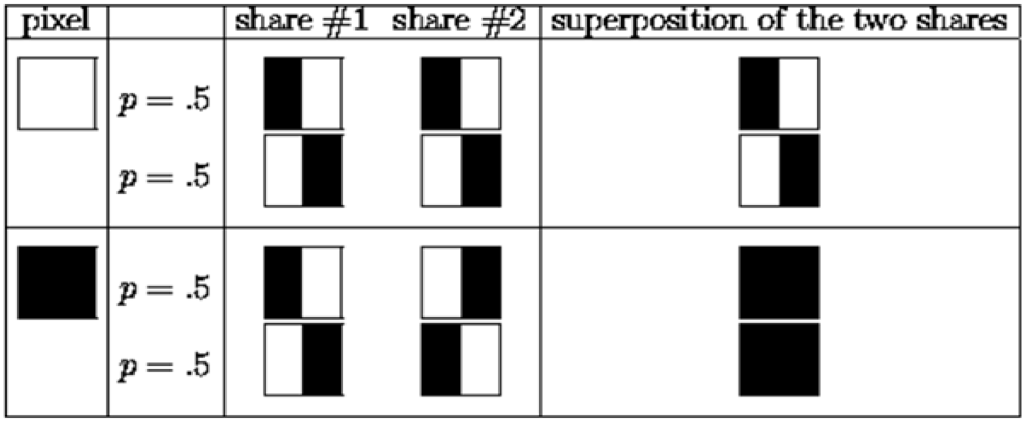


Pixel	White □		Black ■	
Prob.	50%	50%	50%	50%
Share 1	◧	◨	◧	◨
Share 2	◧	◨	◨	◧
Stack share 1 & 2	◧	◨	■	■

Figure 2.3: Construction of (2, 2) VC Scheme

2.5.3 k out of n visual cryptography scheme

In (2, 2) visual cryptography, both the shares are required to reveal secret information.Due to some problem if one share gets lost then the secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal the secret information and user can not a_ord to lose a single share. Naor and Shamir generalized basic model of visual cryptography into a visual variant of k out of n visual cryptography scheme to give some exibility to user. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares superimposed, where value of k is between 2 to n. If less than k shares stacked together, secret original image cannot be revealed. It gives exibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained. It also ensures the security as to know the secret information you have to have more than k shares out of n secret shares.



pixel		share #1	share #2	superposition of the two shares
□	$p = .5$	■□	■□	■□
	$p = .5$	□■	□■	□■
■	$p = .5$	■□	□■	■■
	$p = .5$	□■	■□	■■

Figure 2.4: Construction of a (2, 2) VC Scheme with 2 Subpixels

2.5.4 General Visual Cryptography Scheme

In (k,n) Basic model any ‘k’ shares will decode the secret image which reduces security level.To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson,where an access structure is a specification of all qualified and forbidden subsets of ‘n’ shares . Any subset of ‘k’ or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of k out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion than [7].

2.5.5 Half tone Visual Cryptography Scheme

The meaningful shares generated in Extended visual cryptography proposed by Mizuho nakajima and Yasushi yamaguchi , was of poor quality which again increases the suspicion of data encryption. zhi zhou, gonzalo r. arce, and giovanni di crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel 'P'is encoded into an array of Q1 x Q2 ('m' in basic model) sub pixels, referred to as halftone cell, in each of the 'n' shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security[7].

2.5.6 Visual Cryptography Scheme for Grey images

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. chang- chouLin, wen-hsiangtsai, proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256[7].

2.5.7 Visual cryptography Scheme for color images

The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of color image .F.Liu,C.K. Wu X.J. Lin proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows:

- The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded color image.

- The second approach converts a color image into black and white images on the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels.This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.

- The third approach utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level. This results in better quality but requires devices for decryption[7].

2.6 Arnold Map

Arnold Mapping was discovered by Valdimir Arnold in 1960. it takes the logics from linear algebra and uses them to change the pixel positions with respect to the original image. The Arnold Mapping is a discrete system that stretches and folds its trajectories in phase space.

According to Arnold’s transformation, an image is hit with the transformation that apparently randomizes the original organization of its pixels. However, if iterated enough times, eventually the original image reappears. The number of considered iterations is known as the Arnold’s period. The period depends

on the image size; i.e., for different size images, Arnold’s period will be different

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ N) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\ N)$$

where N is the size of the image, p and q are positive integer and det(A)=1. (xn, yn) is the position of samples in the N * N data such as image, so that

$$(x_n, y_n) \in \{0, 1, 2, \ldots, N-1\}$$

Is the transformed position after Arnold map, Arnold map has two typical factors, which bring chaotic movement:

tension (multiply matrix in order to enlarge x, y) and fold (taking mod in order to bring x, y in unit matrix).

Is used to transform each and every pixel coordinates of the image. When all the coordinates are transformed, the image resulted is a scrambled image. At a certain step of iterations, if the resulted image reaches our anticipated target

(i.e. up to secret key), we have achieved the requested scrambled image. The decryption of image relies on the transformation periods (i.e. the number of iterations to be followed= Arnold's period - secret ke)[8].

2.7 Related Works

Paper name	Data	Techniques	Result	Open Issues
Modified Visual Cryptography Scheme for Colored Secret Image Sharing[9]	2013	The purpose of using is a scheme which encodes a secret image into several shares. Here we are working with (2, 2) VCS	This proposed method can deal with both grey level and colored images	image which should be in rgb color model
RGB Based Secret Sharing Scheme in Color Visual Cryptography[10]	July-2015	In the proposed method, the RGB color image is taken for the information sharing. the RGB color code is separated into 16 standard color code formats	ensures best reconstruction of images	the proposed method constructs a 16 color code
Enhancement of Security in Visual Cryptography using DES Algorithm (Data Encryption Standard) [11]	July-2016	This concept is enhanced by the transformation of meaningless to eaningful shares and the security is enhanced by using DES algorithm with the help of which shares of secret image are encrypted.	shows the secret message is extracted from the stegnographic image. And enhancing the quality of the extracted image approximately equal to that of original secret image.	proposed methodology ,it is necessary that the size of the secret and cover image must be same
A secure visual cryptography scheme using private key with invariant share sizes[12].	2017	The proposed method is used to encrypt halftone color images by enerating two shares, random and key shares which are the same size as the secret color image. The two shares are generated based on a private key	we produce an enhanced form of the proposed method by modifying the encryption technique used to generate the random and the key shares	Key size

Chapter Three

Tools and Methodology

CHAPTER III

Tools and Methodology

3.1 Intodcation

An important type of digital media is images, and for many scientists, it is an essential tool. In astrophysics data from both satellites and distant stars and galaxies is collected in the form of images, and information extracted from the images with advanced image processing techniques. Medical imaging makes it possible to gather different kinds of information in the form of images, even from the inside of the body. By analysing these images it is possible to discover tumours and other disorders .

A digital image is a numeric representation, normally binary, of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to raster images or bitmapped images (as opposed to vector images) .

The digital image is sampled and mapped as a grid of dots or picture elements (pixels). Each pixel is assigned a tonal value (black, white, shades of gray or color), which is represented in binary code (zeros and ones). The binary digits ("bits") for each pixel are stored in a sequence by a computer and often reduced to a mathematical representation (compressed). The bits are then interpreted and read by the computer to produce an analog version for display or printing .

3.2 Digital image

Digital image is a representation of two dimensional image using ones and zeros (binary). Digital image in the computer is an array of numbers that represent light intensities at various points (pixels).

The images types we will consider are:

- Binary image
- Gray scale image
- Color image
- Multispectral image

3.2.1 Binary images

Binary images are the simplest type of images and can take on two values, typically black and white, or 0 and 1. A binary image is referred to as a 1-bit image because it takes only 1 binary digit to represent each pixel. These types of images are frequently used in applications where the only information required is general shape or outline, for example optical character recognition (OCR).

Binary images are often created from the gray-scale images via a threshold operation, where every pixel above the threshold value is turned white (‘1’), and those below it are turned black (‘0’). In the figure below see examples of binary images.

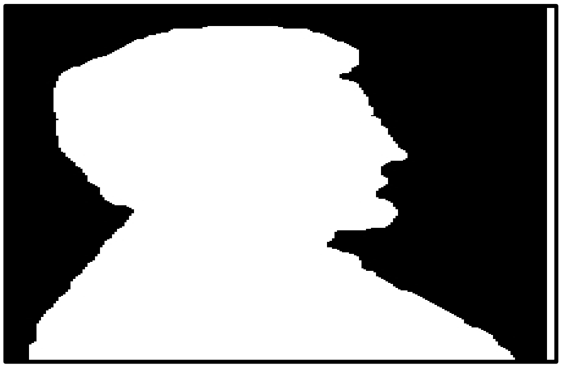


Figure: 3.1 Examples Binary images[13]

3.2.2 Gray-scale images

Gray-scale images are referred to as monochrome (one-color) images. They contain gray-level information, no color information. The number of bits used for each pixel determines the number of different gray levels available. The typical gray-scale image contains 8bits/pixel data, which allows us to have 256 different gray levels. The figure below shows examples of gray-scale images.

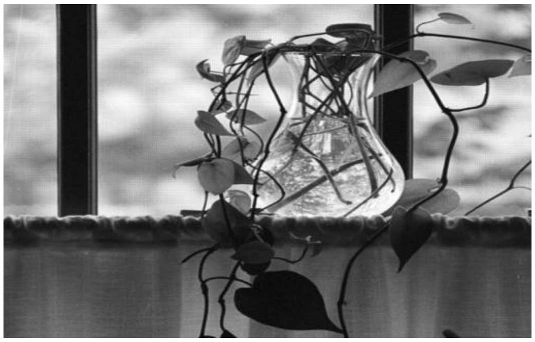


Figure: 3.2 Examples of gray-scale images[13]

In applications like medical imaging and astronomy, 12 or 16 bits/pixel images are used. These extra gray levels become useful when a small section of the image is made much larger to discern details.

3.2.3 Color images

Color images can be modeled as three-band monochrome image data, where each band of data corresponds to a different color. The actual information stored in the digital image data is the gray-level information in each spectral band. Typical color images are represented as red, green, and blue (RGB images). Using the 8-bit monochrome standard as a model, the corresponding color image would have 24-bits/pixel (8-bits for each of the three color bands red, green, and blue). The figure below illustrates a representation of a typical RGB color image.

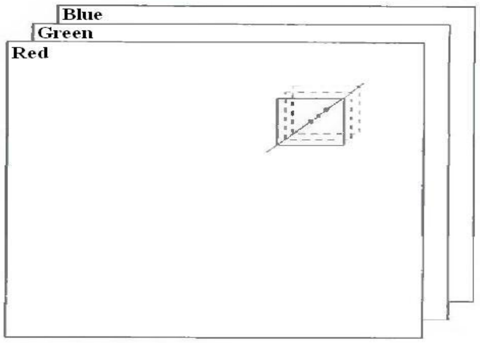


Figure:3.4 Representation of a typical RGB color image[13]

3.2.4 Multispectral images

Multispectral images typically contain information outside the normal human perceptual range. This may include infrared, ultraviolet, X-ray, acoustic, or radar data. These are not images in the usual sense because the information represented is not directly visible by the human system.

However, the information is often represented in visual form by mapping the different spectral bands to RGB components.

3.3 Digital Image File Formats

Types of image data are divided into two primary categories, bitmap and vector.

Bitmap images (also called raster images) can be represented as 2-dimensional functions f(x,y), where they have pixel data and the corresponding gray-level values stored in some file format.

Vector images refer to methods of representing lines, curves, and shapes by storing only the key points. These key points are sufficient to define the shapes. The process of turning these into an image is called rendering. After the image has been rendered, it can be thought of as being in bitmap format, where each pixel has specific values associated with it.

Most of the types of file formats fall into the category of bitmap images, for example:

- **PPM** (Portable Pix Map) format.
- **TIFF** (Tagged Image File Format).
- **GIF** (Graphics Interchange Format).
- **JPEG** (Joint Photographic Experts Group) format.
- **BMP** (Windows Bitmap).
- **PNG** (Portable Network Graphics).
- **XWD** (X Window Dump).

3.4 Proposed Method

The proposed visual cryptography method is used to send an original image from the transmitter to the receiver with the secret.

From the original image the pixel values are extracted and we separately create the red–green–blue (RGB) pixel matrix . The proposed method is used to create the shares from their pixel values. The extracted pixel values are used to create the multiple shares (share 1, share 2, share 3). each share encrypted by Arnold Transform and using RSA public key algorithm and and convert to Hex code image. To generate cipher shares image .

Decrypted, each cipher Hex share convert to decimal and Recovery in Arnold Scrambling Algorithm and using RSA private key Algorithm. Finally used stack to get generate secret image.

As show blow Fig:3.5 on (Pi) is the plain image and Extract the RGB components by Visual Cryptography to share (1), share (2), share(3). Arnold Transform and RSA public key use in the encryption process.

Convert Arnold Transform and RSA Privat key use in the decryption process. Enc.Alg is the encryption algorithm and Dec. Alg is the decryption algorithm employed.

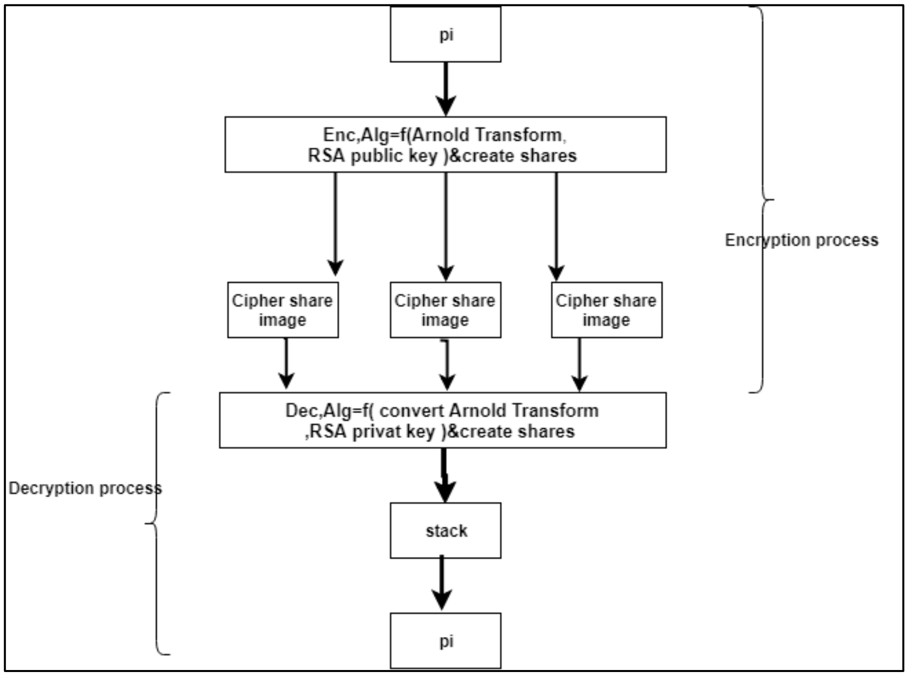

pi
Enc,Alg=f(Arnold Transform, RSA public key)&create shares
Cipher share image
Cipher share image
Cipher share image
Encryption process
Dec,Alg=f(convert Arnold Transform ,RSA privat key)&create shares
Decryption process
stack
pi

Figure:3.5 The encryption and the decryption process

3.5 Proposed Algorithm implementation

A) Algorithm for Encoding Data

Start

Step 1: Select plain image.

Step 2: extract share1(R) and share2(G) and share3(B) .

Step 3: each share pixels are thoroughly scrambled by Implement Arnold Transform

Step 4: In put primer Key.

Step 5: calculated of RSA Public Key

Step 6: RSA Cryptography – Encryption Process

Step 7: convert each share to Hexadecimal code image that represents a colour,

Step 8: Result cipher shares

Step 9: Transfer three cipher image Receiver

Stop

B) Algorithm for Decoding Data

Start

Step 1: Upload cipher image share1

Step 2: Upload cipher image share2

Step 3: Upload cipher image share3

Step 4: convert each share to decimal code matrix.

Step 5: Input of RSA privet Key

Step 6: RSA Cryptography – Decryption Process

Step 7: each share convert Arnold Transform

Step 8: used stack to get generate secret image

Step 9: Preview of Decoded image

Stop

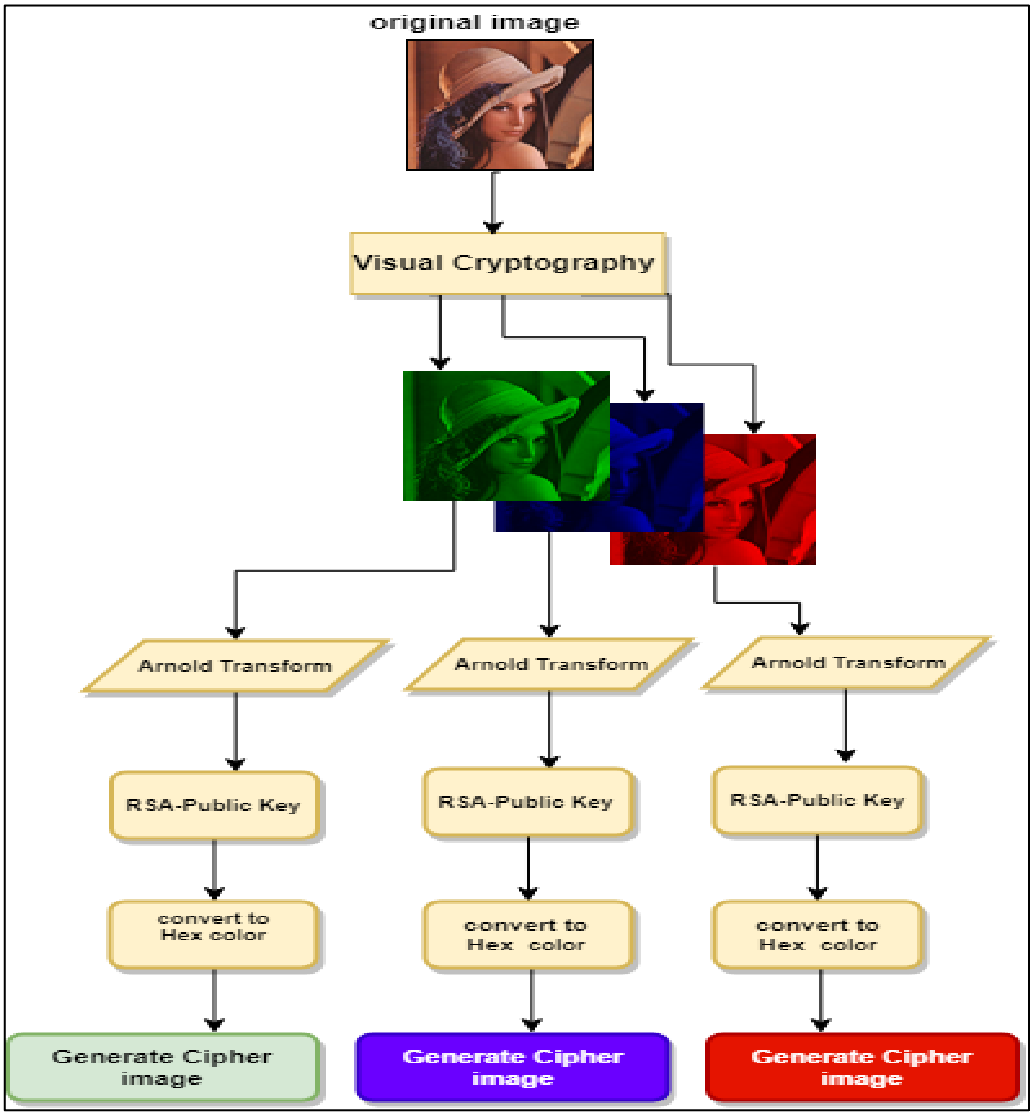


Figure:3.6 Flow chart for RGB share (VC) and Arnold ,RSA

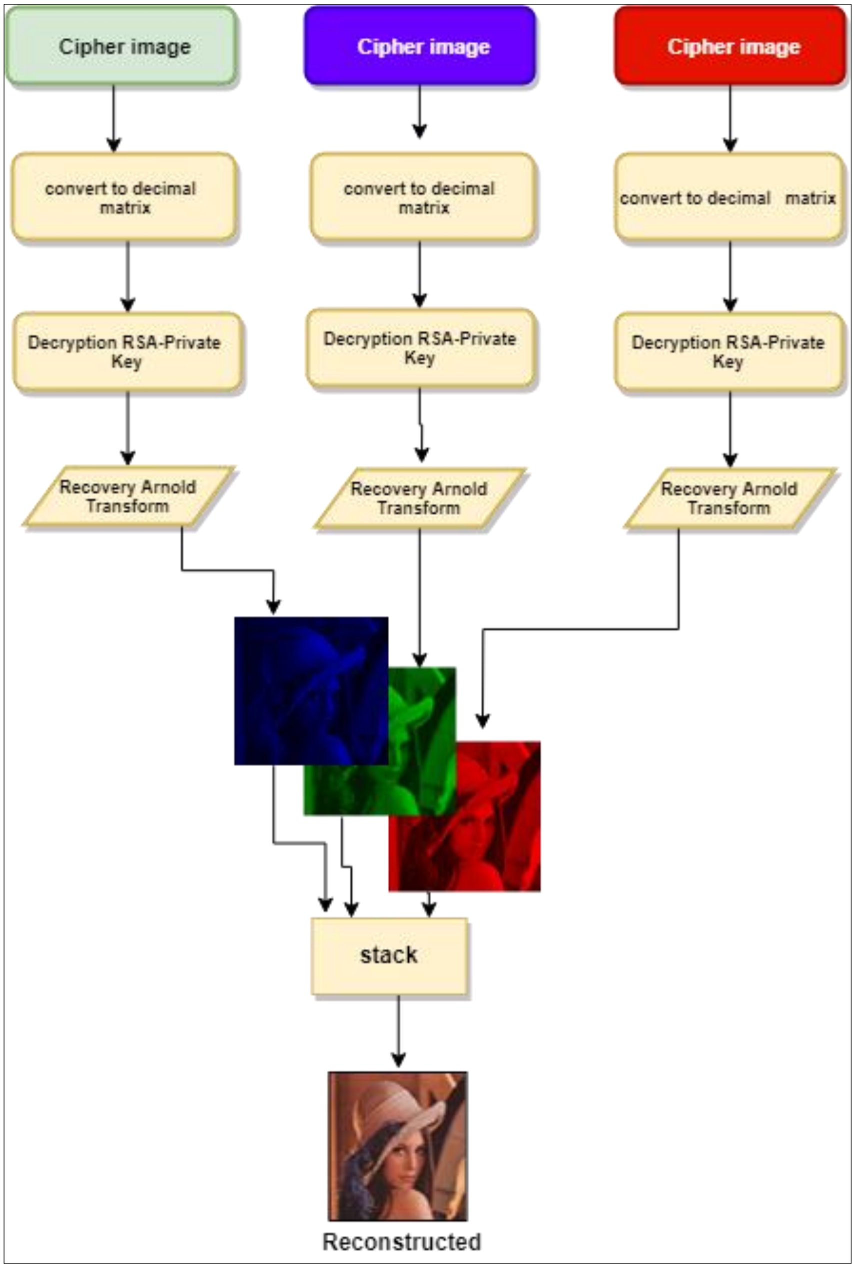

Cipher image
Cipher image
Cipher image
convert to decimal matrix
convert to decimal matrix
convert to decimal matrix
Decryption RSA-Private Key
Decryption RSA-Private Key
Decryption RSA-Private Key
Recovery Arnold Transform
Recovery Arnold Transform
Recovery Arnold Transform
stack
Reconstructed

Figure:3.7 Flow chart for Decryption Cipher share

3.5.1 Share diagram

Figure (3.6) shows the share diagram of the proposed method of the visual cryptography and its each share are explained in the following.

3.5.2 Secret image

The pixel values of the secret color image (original image) are extracted and taken as RGB pixel values and these values are separately indicated as the matrices Rc,Gc and Bc and their sizes are same as the size of the original image (P * Q). The original pixel values of the image are

$$\text{Pixel} = \sum Rc+Gc+Bc; \qquad (1)$$

Where “Pixel” denotes the total value of Rc, Gc and Bc. (P *Q) is the size of the original image size and the colors are speci-ed as red, green and blue. Every pixel from the secret image is encoded into multiple subpixels in each share image using a matrix to determine the colors of the pixels.

3.5.3 Share creation

Each original pixel of the secret image is appearing in n modi-ed versions called shares. Each share is a collection of subpixels of the RGB image.

3.6 Method Encryption Algorithms Arnold Map

- chosen share 1,share 2,share 3 for the process of encryption.
- Pixel extraction is done of the input image (share) by taking the image dimension i.e. Height and Width of the share.
- Pixel shuffling of pixels of the input image is done by using the Arnolds map which is chaotic in nature.
- Input Key number

- Cipher image or Encrypted image (share) is done successfully .

3.7 Method Decryption Algorithms Arnold Map

- The cipher image (share) which got from the process of encryption is chosen for the process of decryption.
- Pixel extraction is done of the cipher image by taking the image dimension i.e. Height and Width of the cipher image.
- Pixel shuffling of pixels of the cipher image isDone by using the Arnolds map which is chaotic in nature.
- Input Key number.
- Original image is brought back from the cipher image successfully.

3.8 RSA

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.in this thesis amodified version of RSA is used.

3.8.1 key-Generation Modified RSA

- Select k large prime numbers (p, q, f,…., r) to form (R =p*q*f…*r).
- Compute t = (p-1) *(q-1)* (r-1)
- Choose (e) such that (1 < e < t)
- Find d such that (e*d ≡ 1(mod t))
- Announce (e, n) as the public key
- Keep (d) as the secret key.
- To calculate the value of C,

C=M^e(mod N) where M is the text to be encoded and C is the cipher text.

To calculate the value of M,

M=C^d (mod N)

where M is the decrypted original pixel.

3.8.2 Encryption method

In the encryption method, every share encryption by the Arnold Transform and using RSA public key algorithm. To generate cipher share image.

C=M^e(mod N)

In this process, each share represented input for the encryption process .

3.8.3 Decryption method

Decryption is the converse methodology of encryption, which is the procedure of shifting over the encrypted content into the unique plain content. In the decryption process

M=C^d (mod N)

The private key (d) is employed to decode the cipher image.

3.9 Application And Tools

3.9.1 Java programming Language

Nowadays, Java is often the default choice for scientific applications, including natural language processing. The main reason for this is because it is safe, portable, maintainable and comes with better high-level concurrency tools than any other language.

Sun microsystem released the first public implementation as Java 1.0 in 1995.it promised "Write Once, Run Anywhere" (WORA), providing no-cost run-times on popular platforms[14]

Significant Language Features are:

- Simple Java is an extension of C and C++ with added feature of garbage collection and improved memory management**.**
- High Performance Java code is compiled into bytecode which is highly optimized by the Java compiler, so that the Java virtual machine (JVM) can execute Java applications at full speed. In addition, compute-intensive code can be re-written in native code and interfaced with Java platform via Java Native Interface (JNI) thus improve the performance.
- Secure The Java platform is designed with security features built into the language and runtime system such as static type-checking at compile time and runtime checking (security manager), which let you creating applications that can't be invaded from outside.
- Platform Independence Java code is compiled into intermediate format (bytecode), which can be executed on any systems for which Java virtual machine is ported. That means you can write a Java program once and run it on Windows, Mac, Linux or Solaris without re-compiling.
- Robust Java is intended for writing programs that must be reliable in a variety of ways. Java puts a lot of emphasis on early checking for possible problems, later dynamic (runtime) checking, and eliminating situations that are error prone.
- Object-oriented Object oriented programming deals with objects and there behaviors and hence an analogy of real world can be found in programs.

3.9.2 MATLAB

MATLAB, the product of Mathworks Company, is the general purpose computing software. It contains a vast range of specialized toolboxes and also works as the computer algebra system through its symbolic math toolbox. This toolbox performs symbolic algebraic/mathematical manipulative operations with a lot of built-in interactivity. MATLAB undoubtedly is popular among computer and multi-disciplinary scientists, engineers and particularly with experts in the area of computational mathematics. It integrates numerical, symbolic and the state-of-the-art graphic visualization capabilities with quite intuitive computer programming environment[15].

Chapter Four

Design and Implementation

CHAPTER IV

Desing and Implementation

4.1 Introduction

This chapter includes the detailed design phase to all documentation of the main interfaces of the system designed using Java language, data input (plain image), encryption and decryption algorithm, overview of the results that are obtained after implementing the proposed cryptographic.

4.2 Implementation

Figure 4.1 Show System main screen. of include the encryption and decryption botton

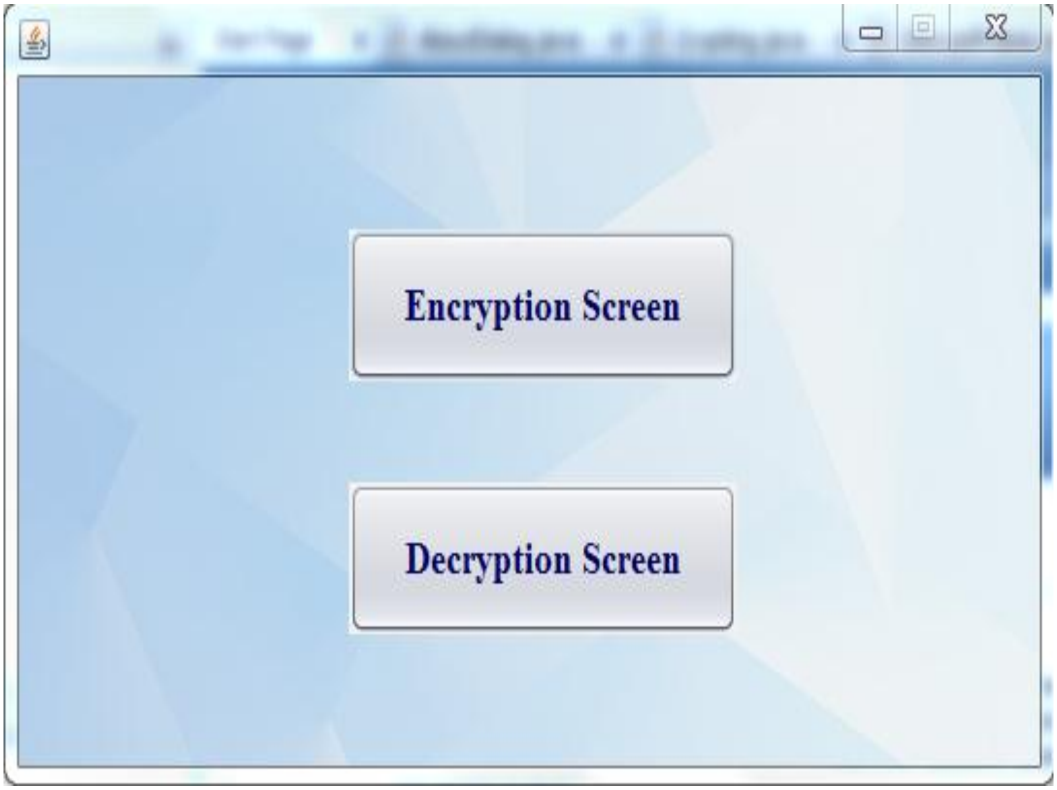


Figure 4.1: System main screen

The Figure 4.2 illustrates the graphical user interface of executing the application to encrypt such images. buttons (Select Image) which loads the image that the user selected,and three buttons (Encrypt) the first button[step1] to extract share1(R) and share2(G) and share3(B) and the tow button [step2] to Arnold Transform And three button (step 3) which complete encryption process after input primer number .

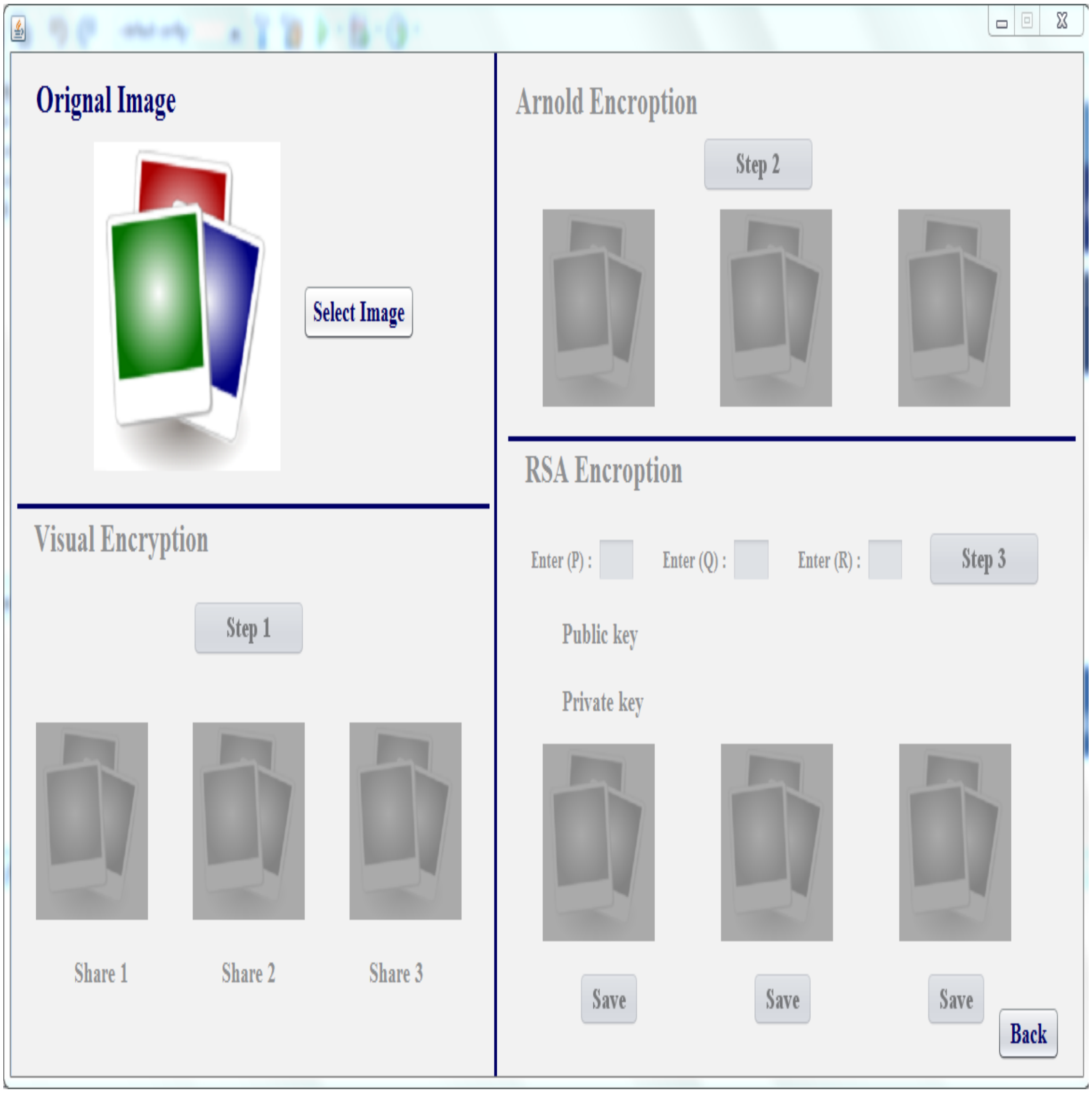


Figure 4.2 : Graphical user interface for encryption process

The Figure 4.3 illustrates the graphical user interface of executing the application to encrypt such images.select image from disk and click buttons [step1] the first button to extract share1(R) and share2(G) and share3(B).

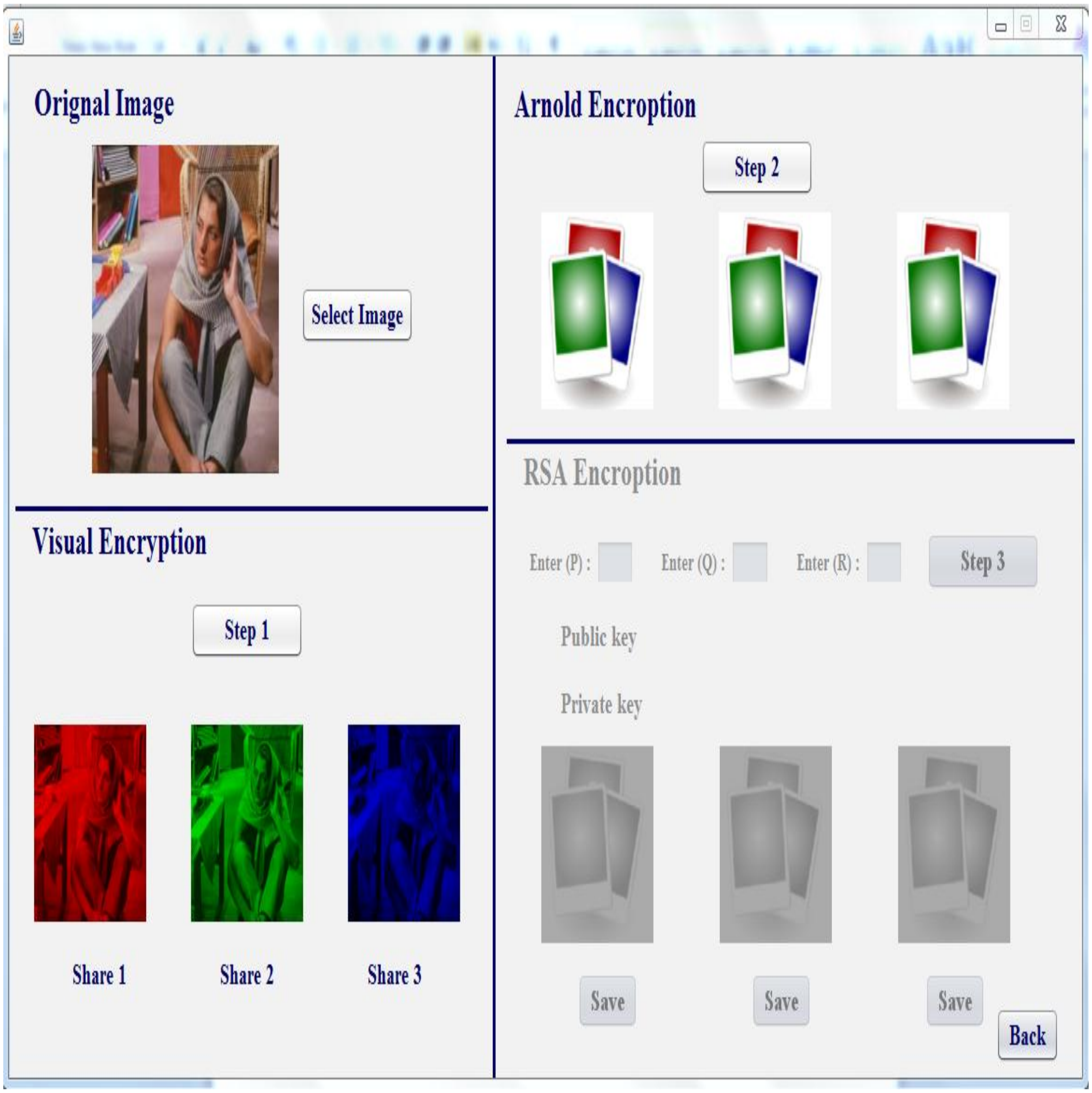


Figure 4.3: first- Encryption process

The Figure 4.4 illustrates the graphical user interface of executing the application to encrypt such images. calculated of Arnold map and show share1(R) and share2(G) and share3(B) after encryption process

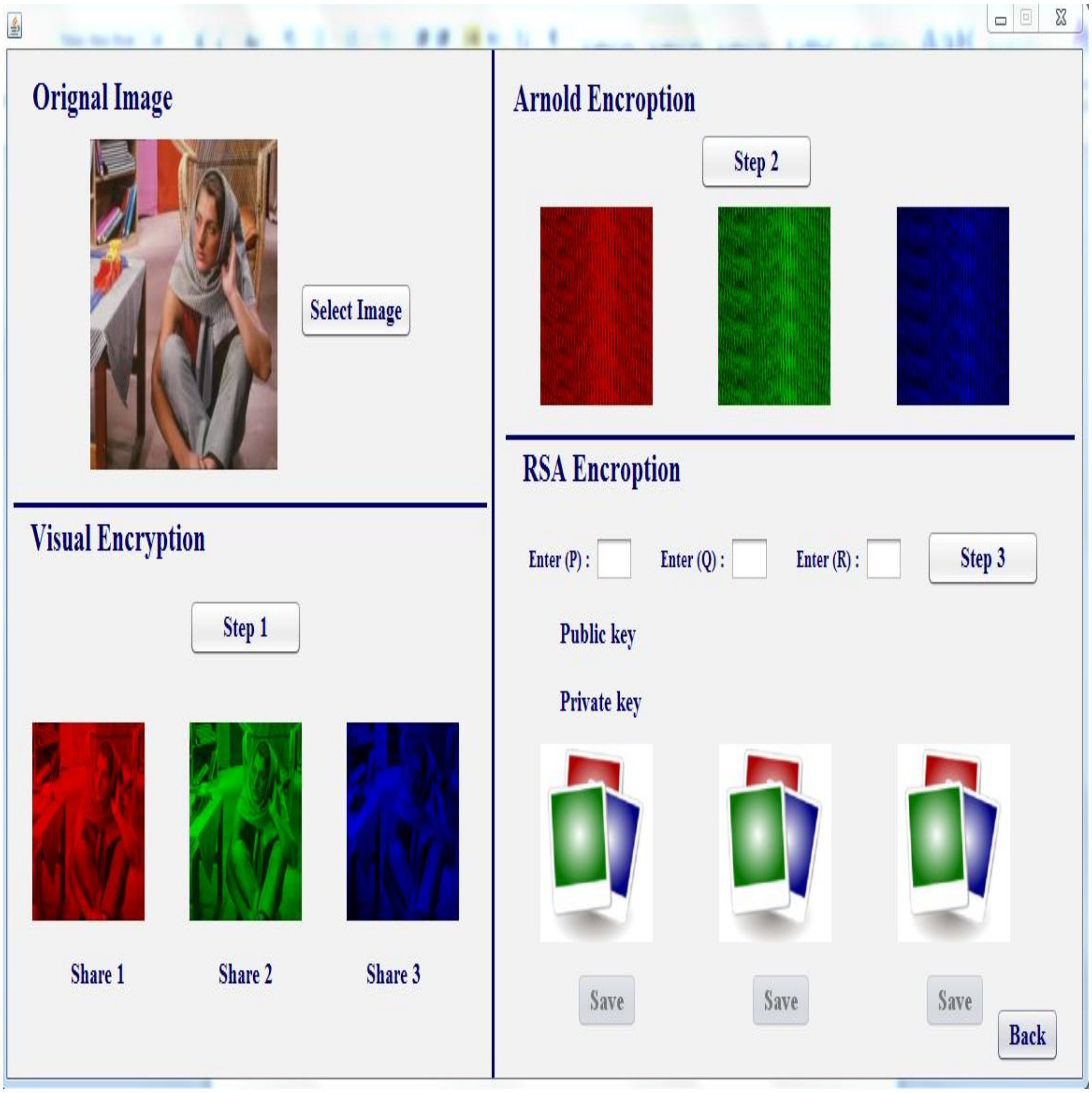
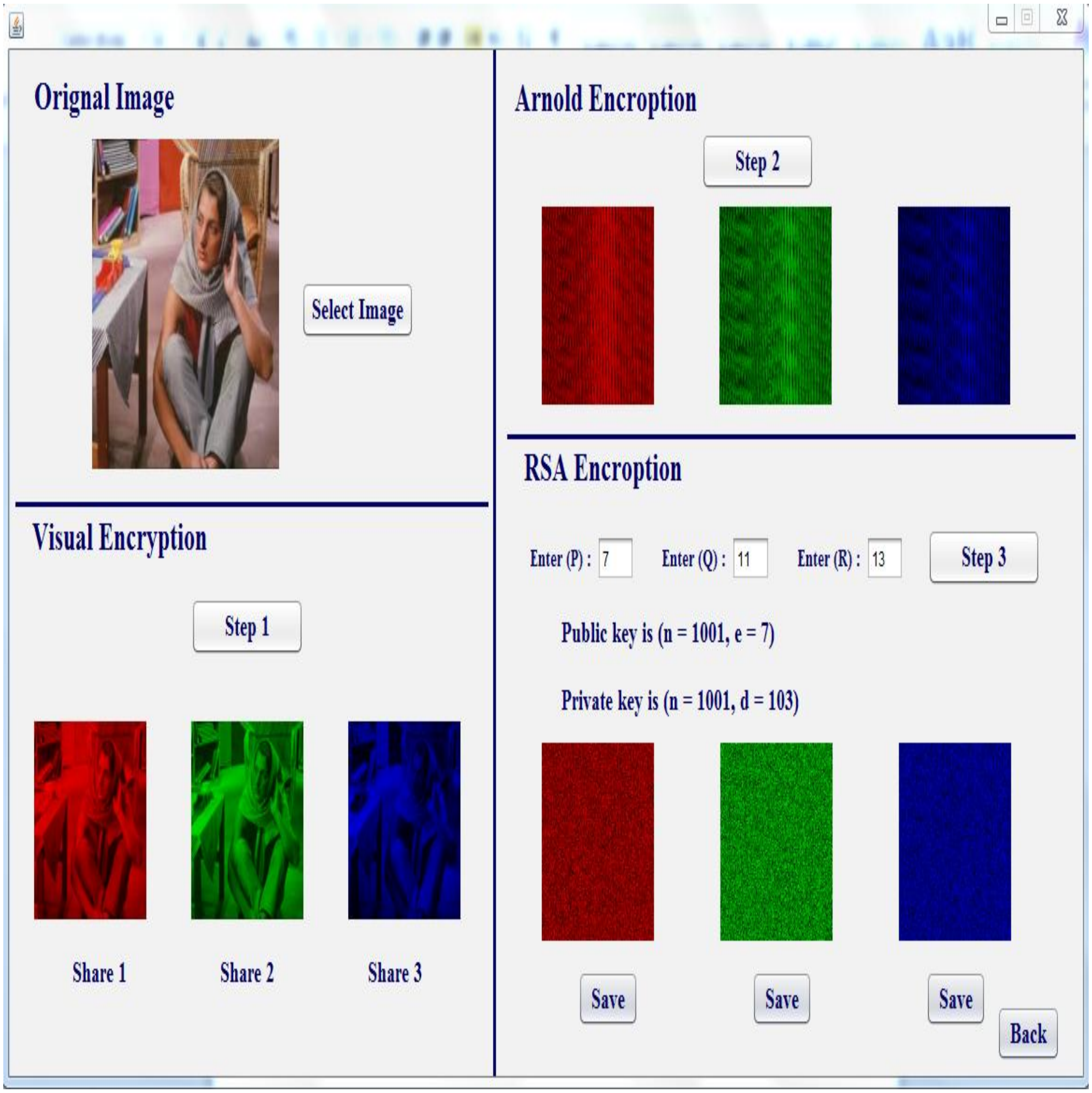


Figure 4.4 : The second- Encryption process for shares

The Figure 4.5 illustrates the graphical user interface of executing the application to encrypt such images. Text filed for In put primer Key. and calculated of RSA Public Key and show share1(R) and share2(G) and share3(B)after encryption process and save all shares.



Enter (P) : 7 Enter (Q) : 11 Enter (R) : 13

Public key is (n = 1001, e = 7)

Private key is (n = 1001, d = 103)

Figure 4.5 : Encryption proces

The Figure 4.6 illustrates the graphical user interface of executing the application to decrypt such images. Text filed for Input of RSA privet Key and three buttons (Select Images shares) which loads the image that the user selected, and (Decrypt) which complete decryption process after click it.

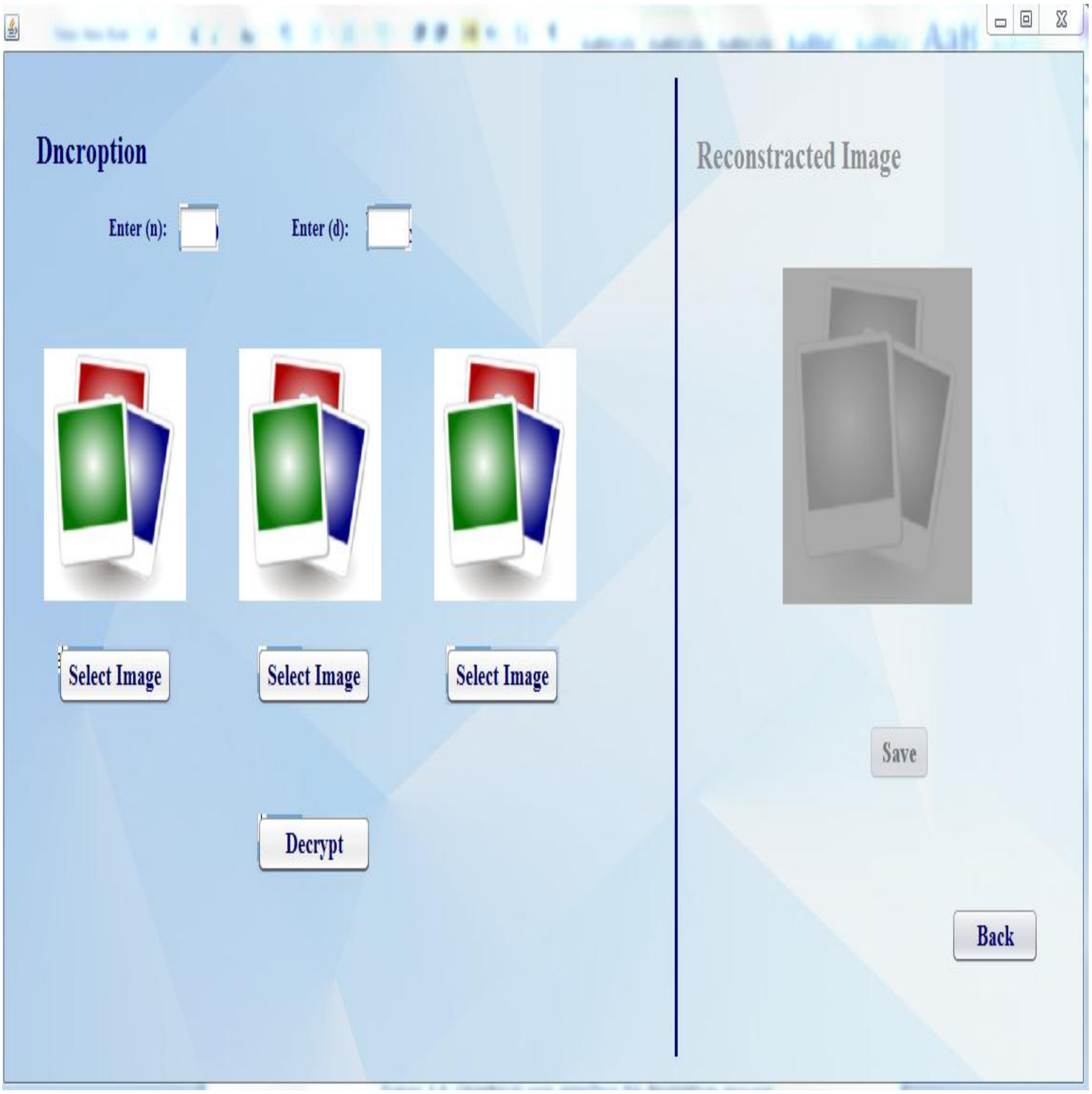
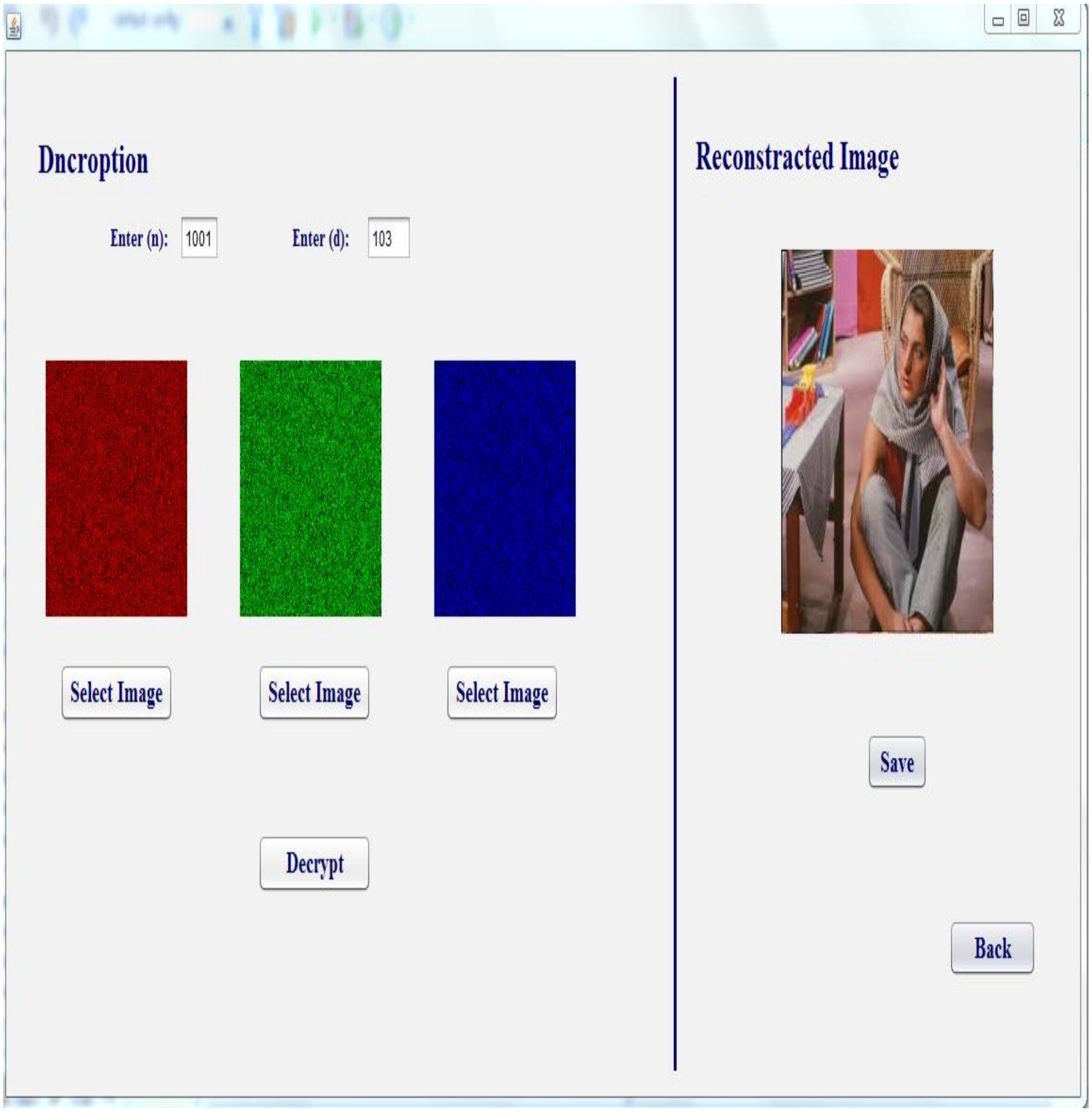


Figure 4.6 : Graphical user interface for decryption process

The Figure 4.5 illustrates the graphical user interface of executing the application to decrypt such images. enter RSA privet Key and (Select Images shares) click button (Decrypt) to complete decryption process and show image that the user selected and save.



Enter (n): 1001

Enter (d): 103

Figure 4.7 : Decryption process complete

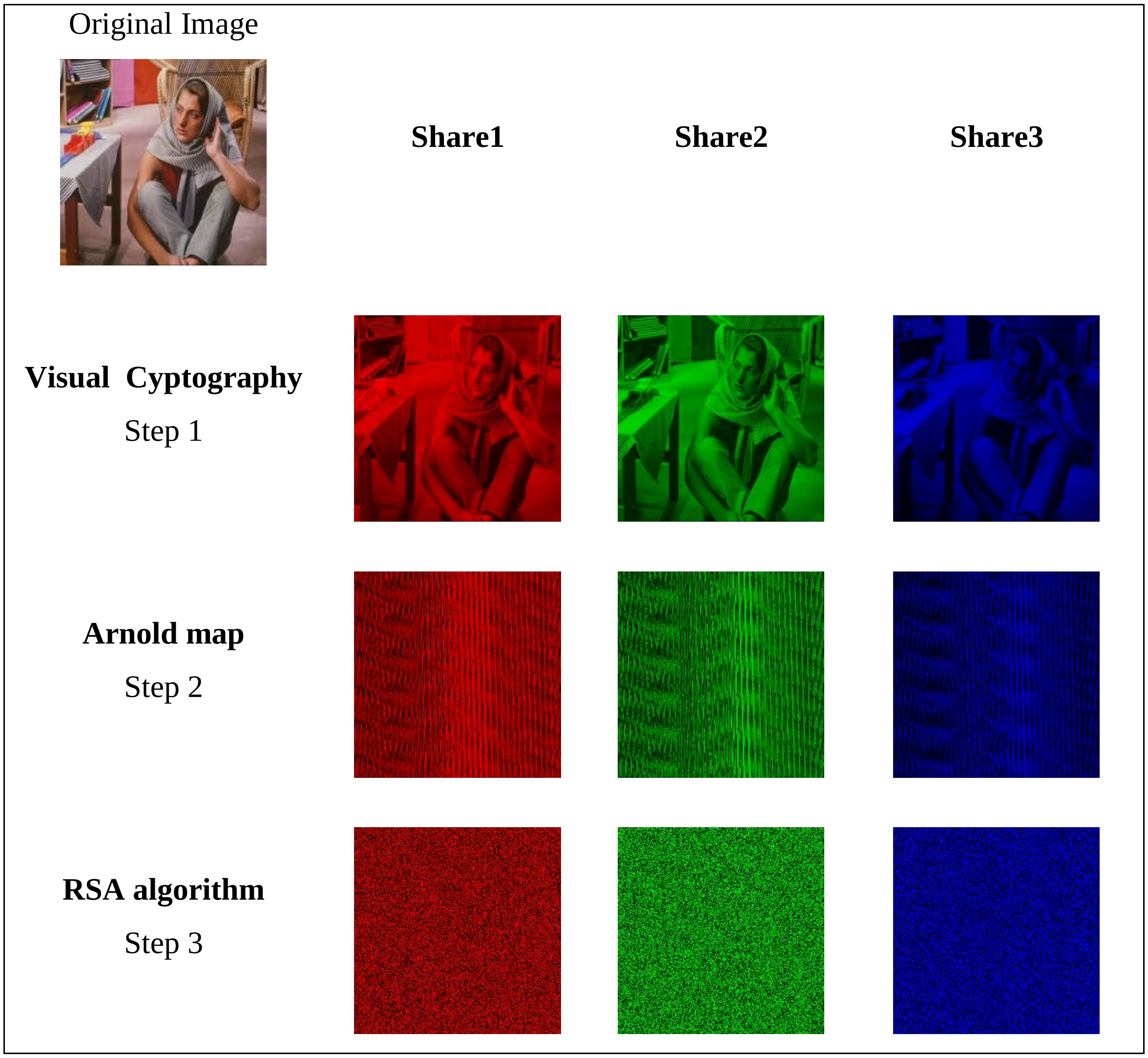


Figure 4.8: Comparison between results of algorithms from the proposed scheme

In the above Figure 4.8, represents the various steps of encrypting the input image by using visual Cryptography and Arnold's algorithm and RSA algorithm .

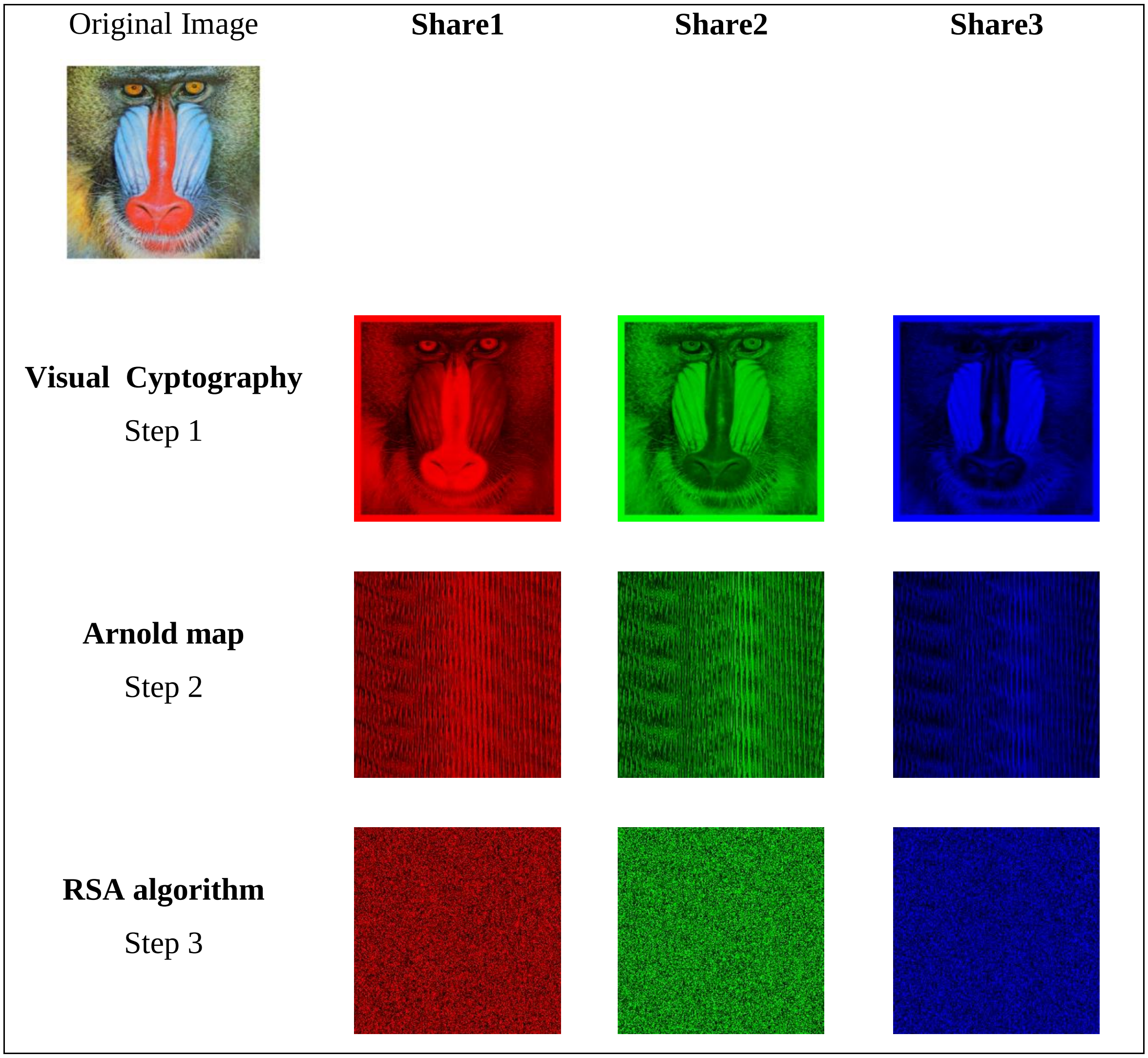


Figure 4.9: Comparison between results of algorithms from the proposed scheme

In the above Figure 4.9, represents the various steps of encrypting the input image by using visual Cryptography and Arnold's algorithm and RSA algorithm.

4.3 Visual Diffusion Test

More experimentation has been conducted to visually judge the diffusion in the resulted images using similar key values. The popular Peak signal-to-noise ratio (PSNR) metric was employed as a similarity measure. PSNR can be computed using the following formula:

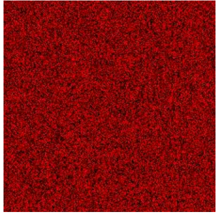
$$PSNR = 10 \times \log(\frac{(\max f(x,y))^2}{MSE}) \qquad (1)$$

$$MSE = \frac{1}{X \times Y} \sum_{x,y} (f(x,y) - p(x,y))^2 \qquad (2)$$

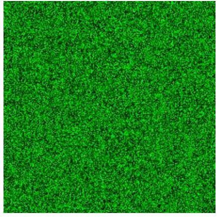
Where *f(x, y)* and *p(x, y)* are the compared images of size $X \times Y$ and MSE denotes the Mean Square Error. PSNR values are often expressed in decibels (dB) where the values will run to infinity if the two examined images are identical. Table 4.1: show PSNR, MSE values for share original images, cipher share images and reconstructed share image, and Table 4.2 compares the PSNR values showing further information on the diffusion aspect using different algorithms

4.4 Performance Analysis of Cryptosystem

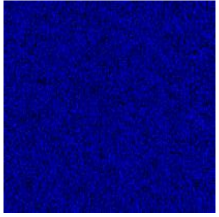
Table 4.1: PSNR, MSE values for share original images, cipher share images and reconstructed share image.

	Share1 	Encrypted 	Reconstructed

	MSE = 0.0
	PSNR = Inf dB
		MSE = +2325.15184
		PSNR = +14.50029 dB
			MSE = 0.0
			PSNR = Inf dB

	Share2 	Encrypted 	Reconstructed

	MSE = 0.0
	PSNR = Inf dB
		MSE = +2420.50500
		PSNR = +14.32574 dB
			MSE = 0.0
			PSNR = Inf dB

	Share3 	Encrypted 	Reconstructed

	MSE = 0.0
	PSNR = Inf dB
		MSE = +2833.65782
		PSNR = +13.64133 dB
			MSE = 0.0
			PSNR = Inf dB

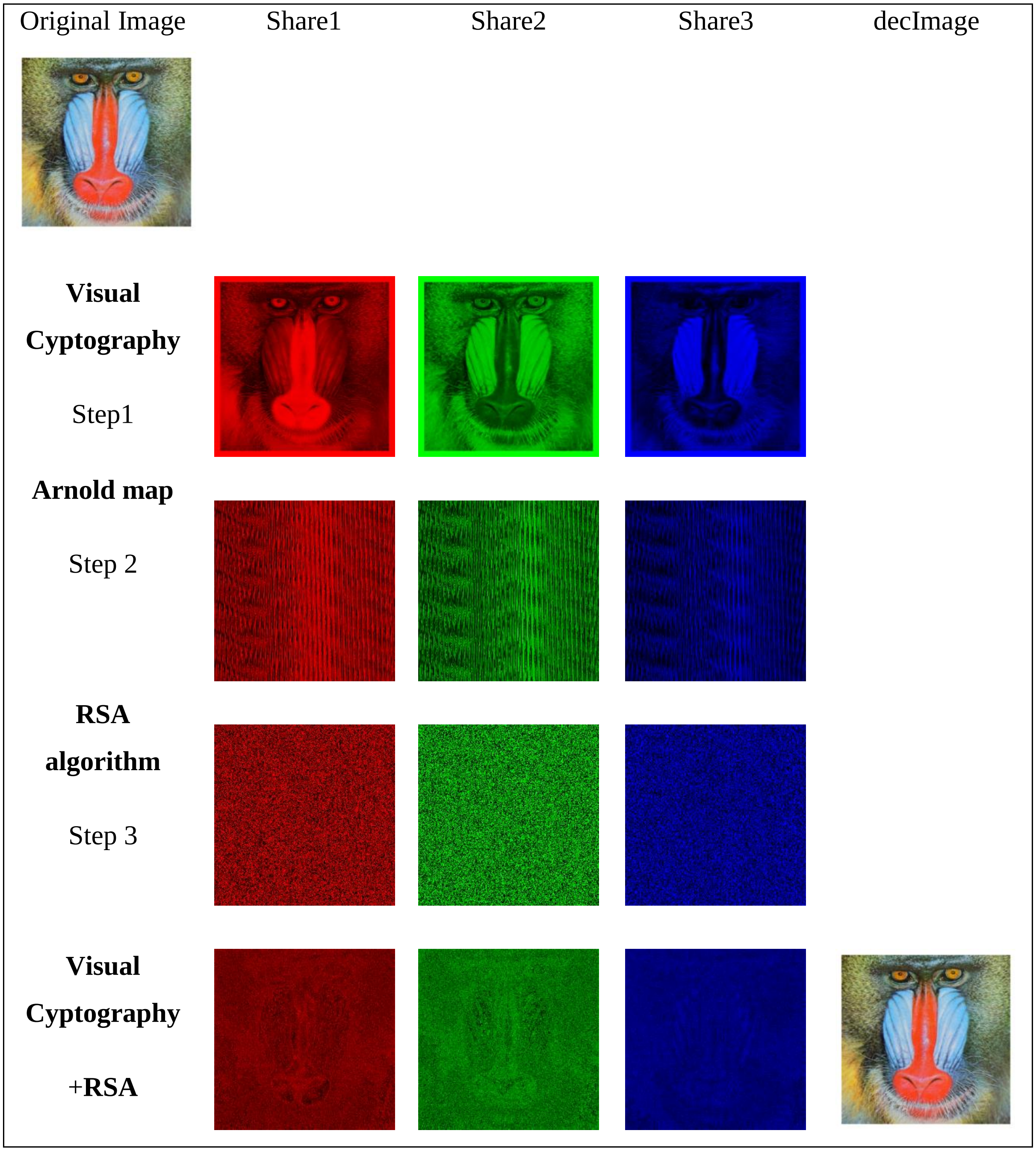
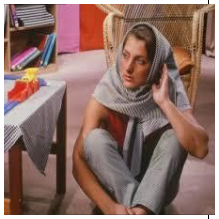
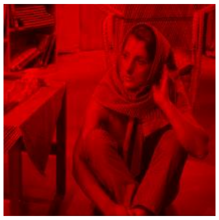
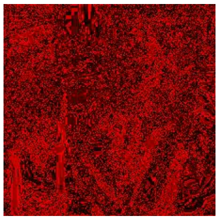
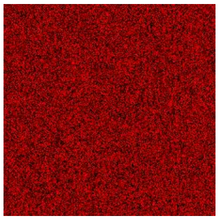
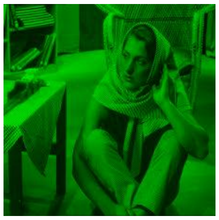
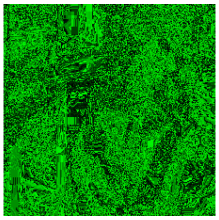
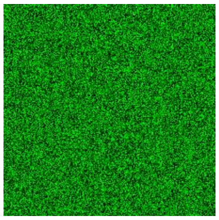


Figure 4.10: Comparison between results of algorithms from the proposed scheme and without Arnold map

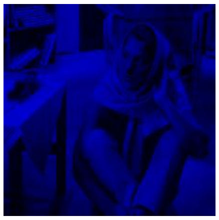
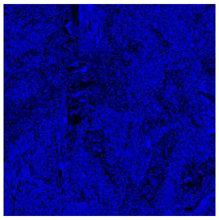
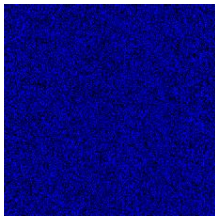
Table 4.2: Barbra shares after vc compere with the same share aftern using RSA only and using Arnold with RSA

Original Image	image VC	Vc+RSA	Vc+Arnold+RSA Proposed Algorithm
			

	Share (R)	MSE = +2584.21222
		PSNR = +14.04152 dB
			MSE = +2620.67310
			PSNR = +13.98067 dB

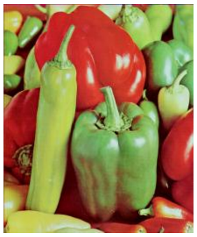
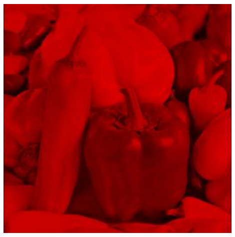
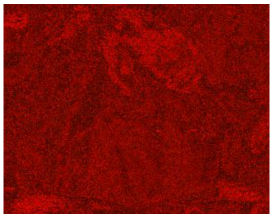
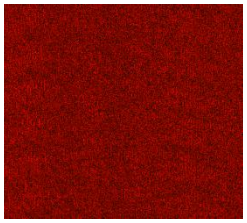
			

	Share (G)	MSE = +2320.78445
		PSNR = +14.50845 dB
			MSE = +2386.70503
			PSNR = +14.38681 dB

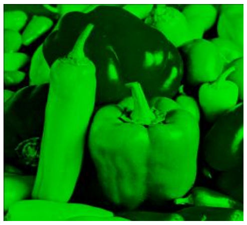
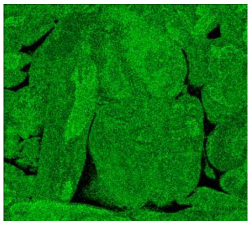
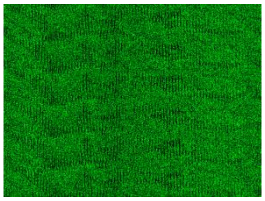
			

	Share (B)	MSE = +2781.27060
		PSNR = +13.72237 dB
			MSE = +2842.28274
			PSNR = +13.62813 dB

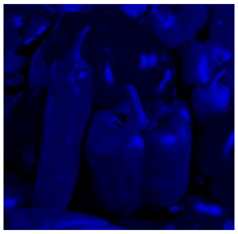
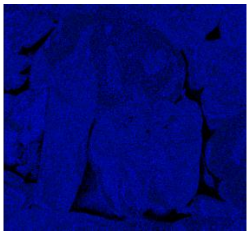
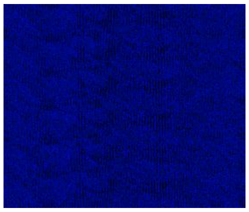
Table 4.2: pepperss shares after vc compere with the same share aftern using RSA only and using Arnold with RSA

Original Image	image VC	Vc+RSA	Vc+Arnold+RSA
			

	Share (R)	MSE = +2325.15184
		PSNR = +14.50029 dB
			MSE = +3560.71667
			PSNR = +12.64943 dB

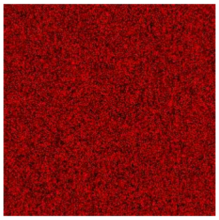
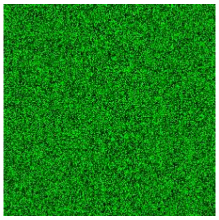
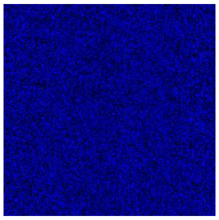
			

	Share(G)	MSE = +2420.50500
		PSNR = +14.32574 dB
			MSE = +3644.06218
			PSNR = +12.54894 dB

	Share (B)	MSE = +2833.65782
		PSNR = +13.64133 dB
			MSE = +4005.40879
			PSNR = +12.13833 dB

Table 4.2: PSNR, MSE values for original Images and various cipher share

Orgnal image	encrypted Share (1)	encrypted Share(2)	encrypted Share(3)
			

	MSE = +10159.84653
	PSNR = +8.09593 dB
		MSE = +12977.64415
		PSNR = +7.03284 dB
			MSE = +13800.72371
			PSNR = +6.76578 dB

Table 4.2 Show The proposed scheme with their PSNR is employed for sample test image. As per (PSNR) understanding with original image and decrypted image, the value should be higher. It shows the better for its superiority.

When the PSNR value is compared for the original image with encrypted image, the PSNR is low which yields better encryption quality. It is clear that the PSNR values are 8.09 and 7.03 and 6.76, which shows low PSNR value, it represents better encryption quality with high security of the secret image.

Table 4.3: PSNR, MSE values for original Image and Reconstructed image

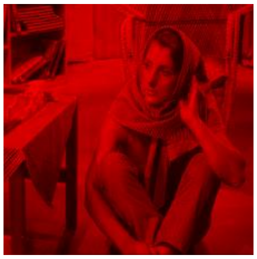
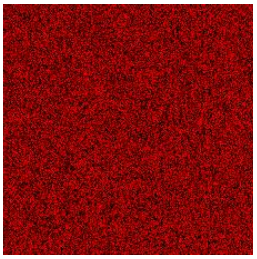
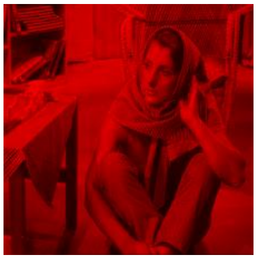
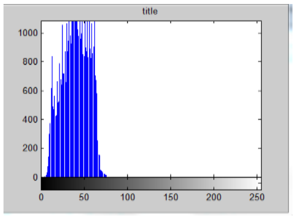
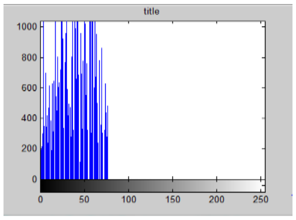
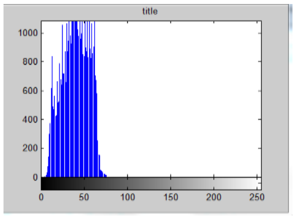
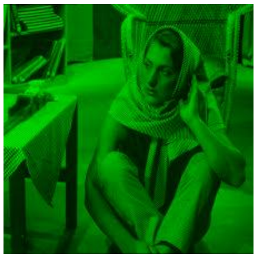
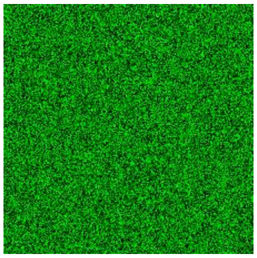
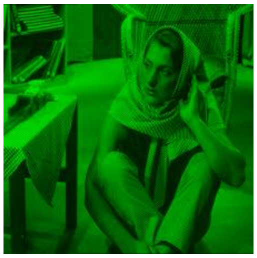
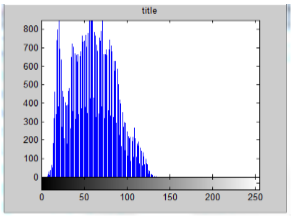
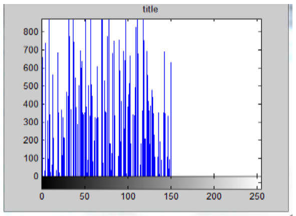
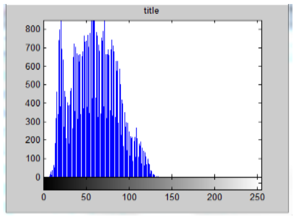
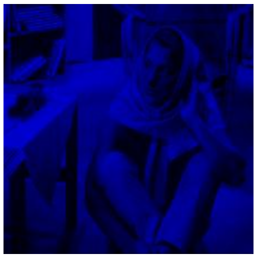
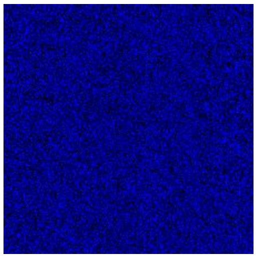
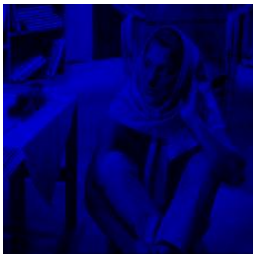
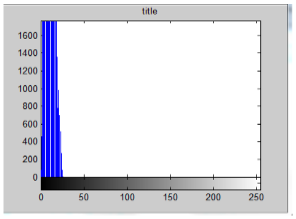
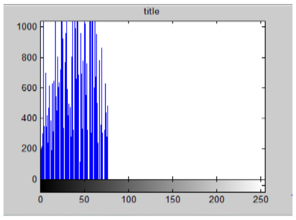
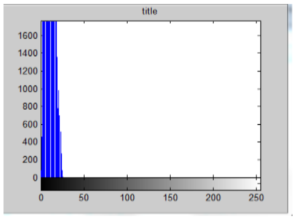
Original image	Original	Reconstructed

	MSE = +0.00000
	PSNR = + Inf dB
		MSE = +0.00000
		PSNR = + Inf dB

4.3 Histogram analysis

Histogram of an image depicts the frequency of each pixels. A good encrypted image has auniform frequency distribution of the pixel values. The statistical analysis of the original image and the encrypted image, Table 2 show the color histograms of the original image and the encrypted image, respectively for the proposed method. (Figure: 5.6) shows that the histogram results of the proposed scheme generated encrypted images are differ from that the original image that shows the goodness of the encrypted image generated.

Table 4.4: Original shares image and cipher shares image histograms

Share1 	Encrypted 	Reconstructed 
Histogram Share1 	Histogram Share1 	Histogram Reconstructed 
Share2 	Encrypted 	Reconstructed 
Histogram Share2 	Histogram Encrypted 	Histogram Reconstructed 
Share3 	Encrypted 	Reconstructed 
Histogram Share3 	Histogram Encrypted 	Histogram Reconstructed 

4.4 Results And Discussion

The proposed an enhanced encryption method which is a combination of Visual Cryptography System (VCS) and Arnold map to shuffles the position of pixel without changing the value of the pixel. In the scrambling process, the arrangement of the pixel values is changed from its original configuration to provide higher level of confusion and enhanced form of existing RSA algorithm by including third prime number in order to make the modulus n large . Both these systems have their own drawbacks but when used together our system more complex and provides more security .

The detailed evaluation of the proposed scheme is done with the help of histogram it is analysed that the histogram of the input image and final image is same but that of the encrypted image is different PSNR values and histogram comparisons between original image and encrypted images were also deployed to show the robustness of the proposed cipher.

Chapter Five

Conclusion and Recommendation

CHAPTER V

Conclusion and recommendation

5.1 Conclusion

Visual Cryptography is no longer safe for modern communication. A new methods must be introduced to overcome these limits. In this thesis anew proposed scheme using visual cryptography with RSA cipher introduced, the visual shares are encrypted using Image scrambling techniques, the pixels are scramble of share in such a manner that the image becomes chaotic and indistinguishable. This makes the scrambles images difficult to decode thus providing a high level of security to the shares compared to the previous scheme .and are again encrypted by Modified RSA algorithm by changing the value of n for providing the double security of secret image .

Using Arnold transformation provides high rate of diffusion rate, The experimental results showed the PSNR values between original image and encrypted images are low, it represents better encryption quality with high security of the secret image.

5.2 Future work

Visual Cryptography provides an effective and efficient way for providing security to a digital image. Using Visual Cryptography, the quality of an image can also be improved. The future scope of the work is to use 3D Images instead of 2D for creating shares and also improve the contrast of decoded secret image.

References

[1] Naor, Moni, and Adi Shamir. "Visual cryptography." Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994.

[2] ARAMĂ, Claudiu, and Eduard Eusebiu EMANDII. "CRYPTOLOGY AND INFORMATION SECURITY." (2017).

[3] Katz, Jonathan, et al. Handbook of applied cryptography. CRC press, 1996.

[4] Guru, Omkar, and Sanjay Majumdar. Implementation of cryptographic algorithms and protocols. Diss. 2007.

[5] AlSabti, Karrar Dheiaa Mohammed, and Hayder Raheem Hashim. "A New Approach for Image Encryption in the Modified RSA Cryptosystem Using MATLAB." Global Journal of Pure and Applied Mathematics 12.4 (2016).

[6] Naor, Moni, and Adi Shamir. "Visual cryptography." Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994.

[7] Ramya, J., and B. Parvathavarthini. "An extensive review on visual cryptography schemes." 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE, 2014.

[8] Abbas, Nidaa AbdulMohsin. "Image encryption based on independent component analysis and arnold's cat map." Egyptian informatics journal 17.1 (2016).

[9] Jesalkumari, Joshi, and R. R. Sedamka. "Modified visual cryptography scheme for colored secret image sharing." Int. J. Comput. Appl. Technol. Res 2.3 (2013).

[10] Karolin, M., and Dr T. Meyyapan. "RGB based secret sharing scheme in color visual cryptography." International Journal of Advanced Research in Computer and Communication Engineering 4.7 (2015).

[11] Bajaj, Surbhi, and Kamal Khajuri. "Enhancement of Security in Visual Cryptography using DES." International Journal of Engineering Science and Computing 6.7 (2016).

[12] Al-Khalid, Rola I., et al. "A secure visual cryptography scheme using private key with invariant share sizes." Journal of Software Engineering and Applications 10.01 (2017).

[13] Boroumand, Mehdi, and Jessica Fridrich. "Deep learning for detecting processing history of images." Electronic Imaging (2018)

[14] Jain, Hemant. Problem Solving in Data Structures & Algorithms Using Java. Independently published, 2018.

[15] Mikhailov, Eugeniy E. Programming with MATLAB for Scientists: A Beginner's Introduction. CRC Press, 2018.