

NEW ALGORITHMS IN COLOR VISUAL CRYPTOGRAPHY

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF DEGREE
OF

MASTER OF TECHNOLOGY
IN
SOFTWARE ENGINEERING

Submitted by:

RAJAT BHATNAGAR
(2K16/SWE/11)

Under the supervision of:

MR. MANOJ KUMAR



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi – 110042

MAY 2018

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi – 110042

CANDIDATE’S DECLARATION

I, RAJAT BHATNAGAR, 2K16/SWE/11 student of M .Tech (Software Engineering) hereby declare that the project Dissertation titled “New Algorithms in Color Visual Cryptography” which is submitted by me to the Department of Computer Science and Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associate-ship, Fellowship or other similar title or recognition.

Place: Delhi

RAJAT BHATNAGAR

Date:

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi – 110042

CERTIFICATE

I, hereby certify that the Project Dissertation titled “New Algorithms in Color Visual Cryptography” which is submitted by RAJAT BHATNAGAR, Roll number: 2K16/SWE/11, Department of Computer Science and Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology is a record of project work carried out by the student under my supervision. To the best of my knowledge, this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

MANOJ KUMAR

Date:

SUPERVISOR

ACKNOWLEDGEMENT

There is forever a sense of gratefulness one express to others for the obliging and needy service they deliver during all phases of life. I was able to build up this Project with the help of different people. I wish to convey my thanks towards each and every one of them.

I express my Sincere Gratitude to my guide Mr. Manoj Kumar (CSE Department) of Delhi Technological University, New Delhi, who, from his hectic schedule guided and supported me, which helped me in developing this project.

I would also like to thank my family for helping me in tough situation and guiding me whenever I needed their support.

Lastly, I would also like to express thanks to my friends and other teachers of the department.

RAJAT BHATNAGAR
M.TECH (SWE)
2K16/SWE/11

ABSTRACT

Visual cryptography framework is a cryptographic technique which permits visual data (E.g. composed content, manually written notes and pictures) to be encoded in such a way, that decoding can be performed by the person visual framework, without the help of PCs.

There are different measures, on which execution of visual cryptography plot depends, for example,

- pixel extension,
- contrast
- security
- Accuracy
- computational unpredictability
- share created is significant or negligible
- nature of secret pictures(whichever double or shading) and
- Number of secret images (whichever single or various) scrambled by the strategy.

Visual cryptography is a decent method for scrambling and unscrambling information on machines that have less figuring power since it doesn't depends on complex scientific squares and structures for encryption and decoding.

CONTENTS

CANDIDATE'S DECLARATION	ii
CERTIFICATE	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
CONTENTS	vi
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF ABBREVIATIONS	xi
CHAPTER 1 INTRODUCTION	10
1.1 Cryptography	10
1.2 Cryptography Types and Algorithms	12
1.3 Visual Cryptography	15
1.4 Visual Cryptography Types	17
1.5 Organisation of the Thesis	19
CHAPTER 2 LITERATURE REVIEW	20
2.1 Literature Review of Visual Cryptography	20
CHAPTER 3 PROPOSED METHODOLOGY	32
3.1 Secure and Efficient (2,2) Color Visual Cryptography	32
3.2 Two Secret (2,2) Color Visual Cryptography	38
3.3 Three Secret (2,2) Color Visual Cryptography	42
3.4 new k out of n Color Visual Cryptography	47
CHAPTER 4 EXPERIMENTAL SETUP AND RESULTS	50
4.1 Experimental Setup	50
4.2 Results of Secure and Efficient (2,2) Color Visual Cryptography	51
4.3 Results of Two Secret (2,2) Color Visual Cryptography	56

4.4 Results of Three Secret (2,2) Color Visual Cryptography	59
4.5 Results of new k out of n Color Visual Cryptography	61
CHAPTER 5 CONCLUSIONS AND FUTURE SCOPE	64
APPENDICES	65
A1. Code used for Interleaved Share Creation of 2 Secret (2,2) VCS	65
A2. Code used for Interleaved Share Creation of 3 Secret (2,2) VCS	66
REFERENCES	68
LIST OF PUBLICATIONS	73

LIST OF TABLES

Table 2.1 Comparison between Properties of Various Methods	25
Table 2.2 Description of Various Methods	27
Table 4.1 Algorithm 3.1 Results for Penguin Image	53
Table 4.2 Algorithm 3.1 Results for Lena Image	54
Table 4.3 Algorithm 3.1 Results for Baboon Image	55
Table 4.4 Algorithm 3.2 Results for various images	57
Table 4.5 Algorithm 3.3 Results for various images	60
Table 4.6 Algorithm 3.4 Results for various images	62

LIST OF FIGURES

Figure 1.1 Types of Cryptography	12
Figure 1.2 Block Ciphers Examples	14
Figure 1.3 Stream Ciphers Examples	14
Figure 1.4 Asymmetric Key Ciphers	15
Figure 1.5 Types of Visual Cryptography	18
Figure 2.1 (2,2) VC Scheme	21
Figure 2.2 Results of (2,2) VC Scheme[2]	21
Figure 2.3 (2,2) Size invariant Visual Cryptography[2][3]	22
Figure 2.4 Extended Visual Cryptography[2][4]	22
Figure 2.5 Joint contrast visual cryptography (Dynamic Visual Cryptography)[2]	23
Figure 2.6 Color Visual Cryptography [2]	24
Figure 2.7 Progressive Visual Cryptography [6]	25
Figure 3.1 Original (2,2) VCS Scheme	32
Figure 3.2 Original (2,2) VCS Scheme Restoration	33
Figure 3.3 Proposed Efficient VCS Share Generation part a	34
Figure 3.4 Proposed Efficient VCS Share Generation part b	34
Figure 3.5 Proposed Efficient VCS Secret Restoration part a	36
Figure 3.6 Proposed Efficient VCS Secret Restoration part b	36
Figure 3.7 Proposed 2 Secret (2,2) VCS Share Generation part a	38
Figure 3.8 Proposed 2 Secret (2,2) VCS Share Generation part b	38
Figure 3.9 Proposed 2 Secret (2,2) VCS Secret Restoration part a	40
Figure 3.10 Proposed 2 Secret (2,2) VCS Secret Restoration part b	40
Figure 3.11 Proposed 3 Secret (2,2) VCS Share Generation part a	43
Figure 3.12 Proposed 3 Secret (2,2) VCS Share Generation part b	43
Figure 3.13 Proposed 3 Secret (2,2) VCS Secret Restoration part a	45
Figure 3.14 Proposed 3 Secret (2,2) VCS Secret Restoration part b	45
Figure 4.1 Project Home Screen 1	50
Figure 4.2 Project Home Screen 2	51
Figure 4.3 Efficient (2,2) VCS Share Generation	51
Figure 4.4 Encrypted base64 Image	52

Figure 4.5 Efficient (2,2) VCS Secret Restoration	52
Figure 4.6 2 Secret (2,2) VCS Implementation Part 1	56
Figure 4.7 2 Secret (2,2) VCS Implementation Part 2	57
Figure 4.8 3 Secret (2,2) VCS Implementation Part 1	59
Figure 4.9 3 Secret (2,2) VCS Implementation Part 2	59
Figure 4.10 (k,n) VCS Implementation Part 1	61
Figure 4.11 (k,n) VCS Implementation Part 2	62

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
AES	Advanced Encryption Standard
TEA	Tiny Encryption Algorithm
XTEA	Extended Tiny Encryption Algorithm
ECC	Elliptic Curve Cryptography
VC	Visual Cryptography
VCS	Visual Cryptography Scheme
RGB	Red Green Blue
MSVC	Multi Secret Visual Cryptography
RC2	Second Rivest Cipher
RC4	Fourth Rivest Cipher
RC5	Fifth Rivest Cipher
RC6	Sixth Rivest Cipher

CHAPTER 1 INRODUCTION

In this chapter, the centre idea and related terms of Cryptography are briefly discussed. It takes a vital part in secure transmission of data. Cryptography has been coined from the term information security. Visual cryptography derives its roots from cryptography, and includes cryptography over images and visual data.

1.1 Cryptography

With the improvement in the field of data and innovation over the timeframe, new potential outcomes for correspondence among us are extended. Internet business being quick and more dependable technique for giving administrations rose as a standout amongst the most effective method for cooperation between end clients like us and government offices, managing an account fields and different associations [36]. The stage is overseen electronically without the need of sending any paper exchanges. Other most astounding leaps forward incorporate web and computerized versatile systems. These administrations are utilized by billion of individuals all through the globe [36].

Aside from these points of interest which advanced frameworks offer, there are a lot of vulnerabilities close by [37]. The unsecured channels can be effectively hacked and unapproved information change can happen. This can prompt bargain of client's protection and security. Computerized frameworks are exceptionally mind boggling and are difficult to troubleshoot.

There exists a need to build up a framework that can shield itself from the phase of exchanging information through putting away information [37].

Some terms related to cryptography are discussed below:-

Cryptography: It is the process of converting plain data to some gibberish form of data and vice versa. Derived from two words crypto and graphy, crypto refers to secret and graphy refers to writing.

Cryptanalysis: The procedure to overcome and break the rules of cryptography used. It thinks about the possibilities of breaking encryption without knowing qualifications [38].

Cryptology: The science about information transmission in secure and mystery shape. It includes both cryptography and cryptanalysis. The term cryptology is gotten from the Greek kryptós ("covered up") and logos ("word").

Cipher: The combined suite of encryption and decryption algorithms is called cipher.

Plaintext: It is normal text that humans can read and interpret. This acts as the input for any encryption module so that it can be converted to cipher text or unreadable form of data.

Cipher text: It is the not understandable or gibberish form of data that is obtained as output from encryption module of any cipher when applied over some plaintext.

Key: It is a combination of letters, symbols, special characters and numbers used to encrypt plain-data or plaintext to cipher text and decrypt cipher text back to the original plaintext from it was created using the aid of some cipher.

Steganography: It is science of hiding data with the help of other mediums.

Below is the listing of goals of cryptography:-

Among a considerable lot of the advantages picked up by the utilization of cryptography in the field of information transmission over various channels, underneath is the rundown of most imperative ones, which are basics.

1. Confidentiality: It is the administration offered that gives the information protection. Authoritative access is kept up and any un-approved information to get is prohibited. Term is like protection in like manner setting [38].
2. Authentication: This is the procedure portrayed as Identification. Gatherings enjoyed the procedure of correspondence needs to check their characters preceding trade of data [39].
3. Integrity: All the information exchanged among the clients must keep up the integrity. As such, any sort of activity performed on information like expansion, cancellation or sort of control must be noticeable to every client. This confines the phony inclusions by gatecrashers [40].
4. Non-repudiation: For a debate situation when a gathering differs about the information it transferred, there must be a framework or administration that can resolve this issue. In this manner the precluding from securing activity must be checked and substantial move must be made against committer [38].

1.2 Cryptography Types and Algorithms

Cryptography is performed with the aid of ciphers or in other words, a suite of encryption and decryption algorithms. Encryption algorithms convert plain-data to garbage or unreadable form of data while decryption algorithms perform the opposite process of encryption algorithms.

Below, we see a figure that illustrates various types of cryptography:-

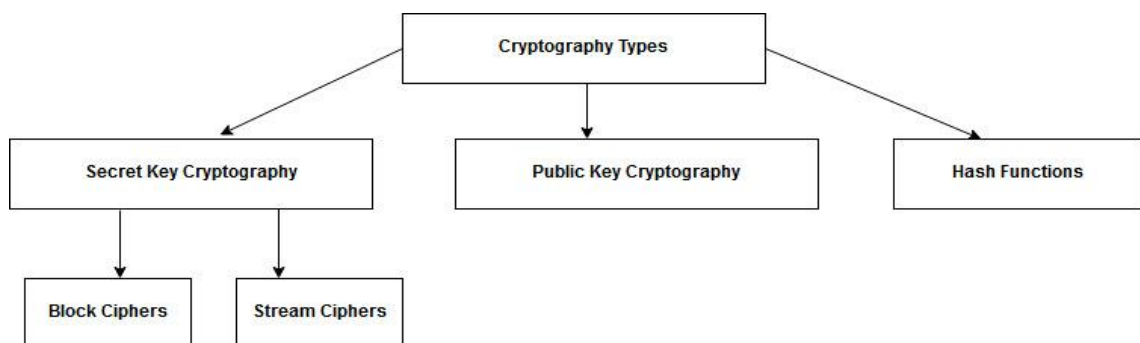


Figure 1.1 Types of Cryptography

We can see that mainly there are three types of cryptography:-

- 1.) Secret Key Cryptography
- 2.) Public Key Cryptography
- 3.) Hash Based Functions (or One Way Functions)

Secret Key Cryptography: This is also called as symmetric key or private key cryptography. Between two parties, that is sender and receiver, a common key is used for both encryption and decryption of messages. Suppose, we have a sender A and a receiver B that wants to communicate by encrypting their messages.

So, A sends a message to B by encrypting the message using the secret or private key shared between A and B. B receives the encrypted message and applied the shared key to that message for decryption. B gets the original text by decrypting the encrypted message it received from A. This is the way parties will communicate using shared or secret key cryptography. This type of cryptography technology is further divided as two techniques, namely: block ciphers and stream ciphers.

Public Key Cryptography: This scheme is also called as asymmetric key cryptography. Every entity in this scheme has a set of two keys. One key is called entity public key, and other key is called entity private key. Private Key of every entity is secret with them, while public key of each entity in the system will be shared by the entity them self for communication purposes.

This type of scheme is used for both encryption-decryption purposes as well as for digital signature and for verification purposes. Generally, public key is used for encryption, whereas the private key will hold good for decryption.

Hash Functions: Hash functions are otherwise also called message digests or one-way encryption [41]. These are the scheme which does not require any key for its processing. Consequently, a fixed length data known as hash is created relying on the message substituted. This hash is the mathematically computed impression for the message and assumes critical part in guaranteeing uprightness of the message.

The issue related with public key system for information confirmation is that the measurements of resultant message moves toward becoming around two times of the first. This issue can be tended to utilizing hash. Most critical part of this approach is that even a solitary piece information change can bring about totally unique hash data and consequently cheating can be distinguished.

The figures below describe the various cryptographic algorithms used in literature, along with their taxonomy.

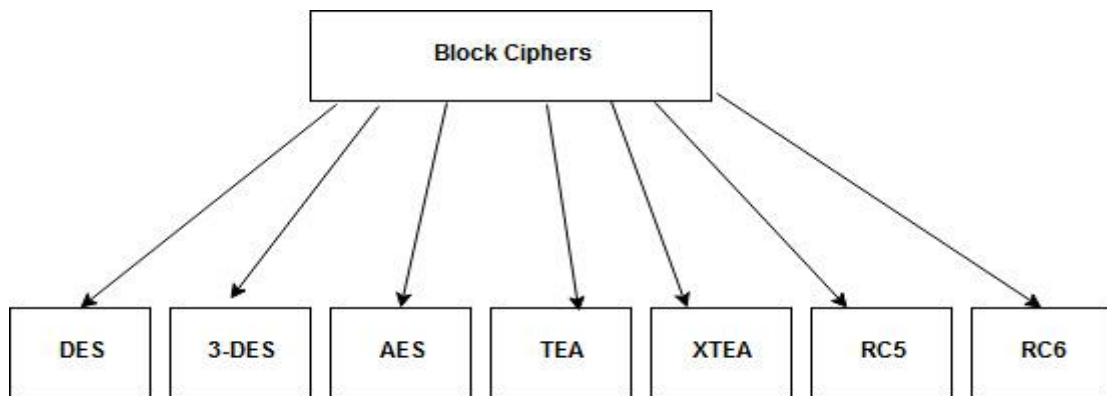


Figure 1.2 Block Ciphers Examples

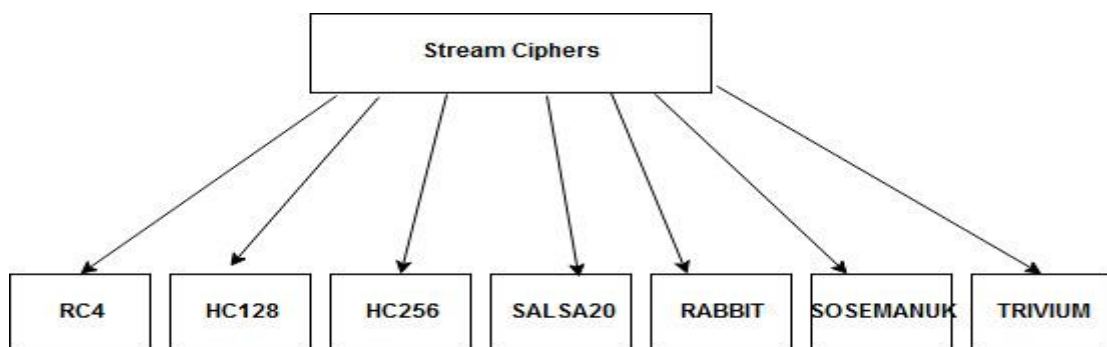


Figure 1.3 Stream Ciphers Examples

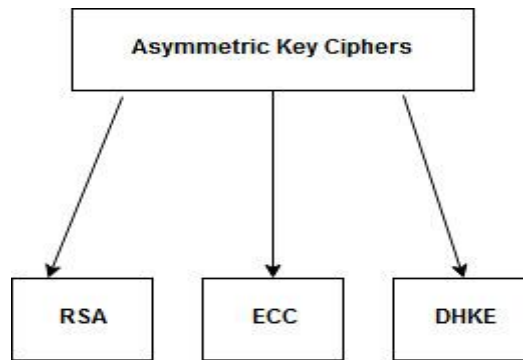


Figure 1.4 Asymmetric Key Ciphers

1.3 Visual Cryptography

Various techniques to protect the data have been proposed in the literature from time to time such as cryptography, Steganography and others.

Visual cryptography is one of the cryptographic methodology which permits visual information, for instance, text, images are encrypted in such means that decryption can be performed by the human eye, with no involvement of computers.

Visual cryptography technique was first developed by Noar and Shamir in 1994[1]. This technique worked for binary images.

It is noted that the trend has shifted from basic or grey scale visual cryptography to color visual cryptography.

The best algorithm for visual cryptography could be one in which we have the following parameters satisfied.

- a.) Meaningful Shares
- b.) Color Image as Secret
- c.) High Contrast Output Obtained
- d.) Possibility to include multiple secrets
- e.) Least Possibility to doubt that some secret is enclosed
- f.) Simple Stacking of Shares does not reveal secrets

Existing literature has provided many schemes for binary, greyscale and color images.

Focal points of Visual Cryptography

In this area points of interest and highlights of visual cryptography are talked about and these are as per the following:

- **Human Visual System:** The greatest favourable position of visual cryptography is that it requires no PCs or any machine to recoup the mystery covered up. Human eyes are much fit for doing this. Be that as it may, new plans are there which increment the determination and contrast at the cost of multifaceted nature and making it no longer workable for human vision framework to interpret it, yet these require small processing power when contrasted with any open or private key frameworks [18].
- **Perfectly Secure:** Visual cryptography is almost an impeccable sharing plan. It isn't conceivable to recover any valuable data from one single offer or the quantity of shares to be stacked are less than the alluring sum; there is no strategy to acquire mystery regardless of how much figuring power is available [19].
- **Robustness:** Any scaling, skewing, stretching, compacting or trimming activities does not give any data covered up in a mystery. The pixels that are dark will remain dark and comparatively white. Visual cryptography can withstand these specified assaults impeccably [22].

Restrictions of Visual Cryptography

No framework is impeccable, henceforth visual cryptography likewise has couple of constraints and these are scribbled down as takes after:

- **Contrast Loss:** This is the most noteworthy issue identified with visual cryptography. The contrast is separated among the quantity of shares. Since the lesser the contrast, lesser will be the human eye ability to recognize arbitrary pixels and

mystery pixels. Thus, contrast misfortune is straightforwardly connected to number of shares and increments with increment in share tally [21].

- Pixel Expansion: Single pixel is shared among different pictures. These makes bulky ways to deal with manage. Because of this, pixel estimate is expanded un-fundamentally [23].
- Larger Size Shares: Traditional visual cryptography plans make shares that are bigger than the measurements of genuine or mystery picture itself. These bigger shares themselves, difficult to deal with, as impeccable arrangement is intense in greater shares case [22].

Visual cryptography has been used in various applications from time to time. Various applications of visual cryptography are:-

- 1.) Secure Authentication System
- 2.) Secure E-Voting System
- 3.) Anti-Phishing
- 4.) Cheating Prevention
- 5.) User Identity Recognition

1.4 Visual Cryptography Types

Ideally, the first method for visual secret sharing or visual cryptography was proposed by Noar and Shamir in 1994[1]. Source image taken by them was a black and white image, i.e. pixels will be in the range of 0 and 1. They used a scheme through a master fixed coding handbook or coding table. By the aid of this table, the original source image was divided into individual transparencies or shares. The concept stated that to open a lock, we have k keys suppose, then we need at least n key ($n \leq k$) to open the lock. Similar technique was applied here.

Then the research progressed year by year and researchers and scholars started devising newer methods for visual cryptography. Some of them used black and white images, some used grayscale while some focused their work on color images.

Various types of visual cryptography techniques found in literature are pointed below (discussed in depth in chapter 2):-

- Black and white visual cryptography
- Color Visual Cryptography
- Grayscale Visual Cryptography
- Multi-secret Visual Cryptography
- Dynamic Visual Cryptography
- Progressive Visual Cryptography
- Size invariant Visual Cryptography

The figure below summarizes all types of visual cryptography existing in literature:-

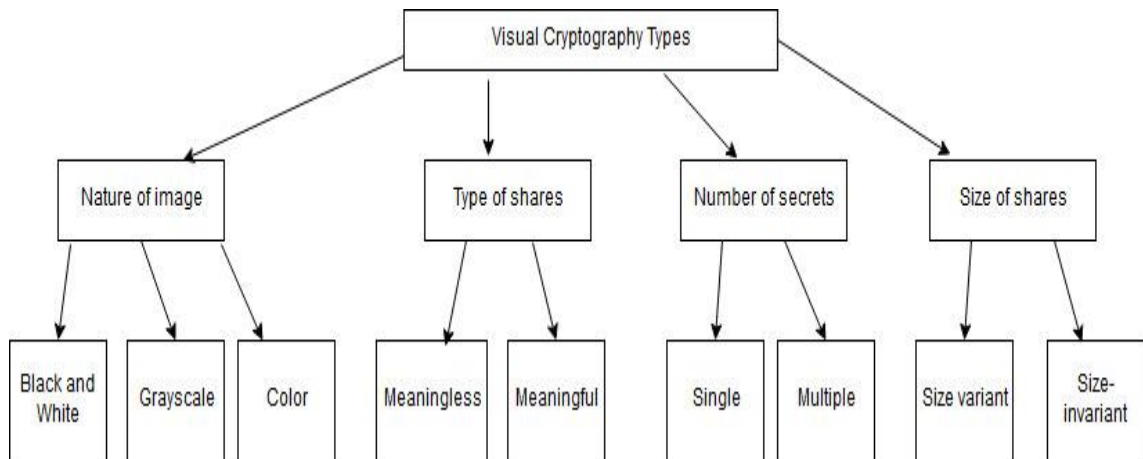


Figure 1.5 Types of Visual Cryptography

1.5 Organisation of the Thesis

The aim of this thesis was to contemplate different calculations given as of now in literature and after that to outline newer approaches. There are a set of proposed visual cryptography algorithms which forms the basis of thesis and is examined in detail in chapters 4 and 5. Following is the overall structure of this thesis and the primary contribution of every chapter:

- In Chapter 1, the fundamentals of both conventional and visual cryptography are talked about.
- In Chapter 2, work done by different scholars and researchers has been examined so as to propose and suggest newer methods. This segment specifies a portion of the applicable papers that aided in accomplishing the results.
- In Chapter 3, the proposed work is detailed. A total of four algorithms are suggested. First algorithm is a time and space comparison of a base method using various algorithms. Remaining proposed algorithms are modified versions of original algorithms to create newer approaches. Each subsection of this chapter explains the proposed theory in great depth.
- In Chapter 4, the results of the proposed algorithms are discussed along with the experimental setup used. The results are provided in proper tabular fashion along with figures and outputs.
- In Chapter 5, the last part demonstrates the concluding remarks of the proposed work and the extension for the future work is also examined.

CHAPTER 2 LITERATURE REVIEW

2.1 Literature Review of Visual Cryptography

This section provides an overall literature review of visual cryptography. Visual cryptography is one of the cryptographic methodology which permits visual information, for instance, text, images are encrypted in such means that decryption can be performed by the human eye, with no involvement of computers.

Visual cryptography technique was first developed by Noar and Shamir in 1994[1]. This technique worked for binary images.

This section presents a layout of the first visual cryptography method, along with the various methods developed and proposed from time to time.

This section also gives a survey of the applications that are based upon the concept of Visual Cryptography.

Visual Cryptography technique was originally invented by Moni Noar and Adi Shamir in 1994 at the Euro crypt Conference [1]. This implementation assumes that an image or message is a collection of black and white pixels. Shares or transparencies were created from the original message using a predetermined coding table.

Schemes were (k,n) or (n,n) . (k,n) scheme means that at least k shares out of given n shares are needed to decrypt the hidden secret. (n,n) scheme meant that all shares are needed to decrypt the hidden secret.

To decrypt the secret, shares were stacked and OR operation was performed. An example of such coding table is shown below in Fig.1 (a), along with results of the scheme in Fig.1 (b).









Secret message	Share 1	Share 2	Stacked share
0-bit 			
1-bit 			

Figure 2.1 (2,2) VC Scheme

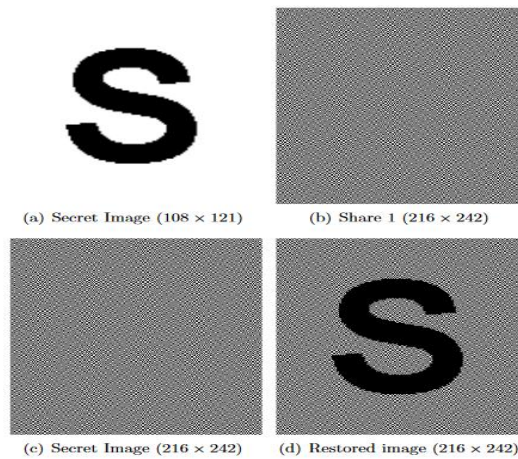


Figure 2.2 Results of (2,2) VC Scheme[2]

Traditional visual cryptography schemes use technique of pixel expansion. One pixel is divided into 4 sub pixels; hence the image shares size gets doubled as it can also be seen in figure 1(b). Ito et.al [3] proposed a VC technique in 1999 called the size invariant visual cryptography.

This technique was constructed over the original VC technique [1] but the share sizes were equal to the original image size. This technique was developed for both schemes of (k,n) as well as (n,n) schemes. Fig.2 shows a (2,2) scheme example of size invariant visual cryptography:-

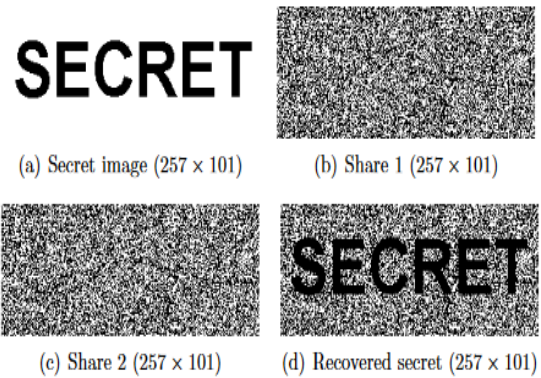


Figure 2.3 (2,2) Size invariant Visual Cryptography[2][3]

Extended VC takes the idea of visual cryptography further by creating shares which are meaningful to anyone who views them. This is used to alleviate suspicion about any encryption that has taken place and also presents visually pleasing shares which incorporate all the previously mentioned features of VC [2].

Fig.3 shows an example of Extended Visual Cryptography.

Two meaningful shares can be generated from two base images and the secret is hidden in between each of these shares. After stacking the shares, the secret is completely recovered and the meaningful information on the shares is completely disappeared.

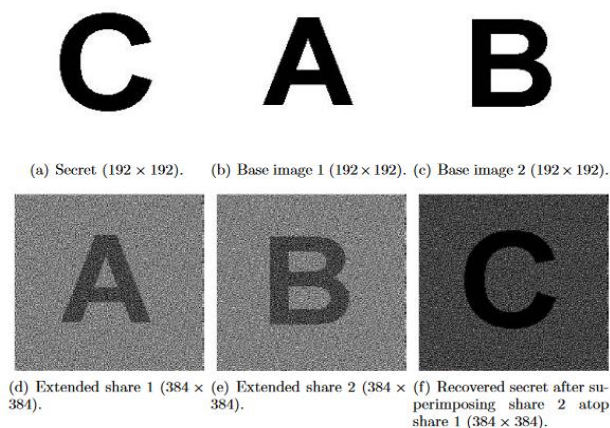


Figure 2.4 Extended Visual Cryptography[2][4]

It refers to the concept of hiding two or more secrets using two or more shares. The advantage of such scheme is that within the same size and number of shares as of

previous techniques, we can now hide much more secrets. Multiple-secret sharing issue was observed at first by Wu and Chen [5].

They embedded two secrets into two set of shares S_1 and S_2 . The secret is obtained by superimposing shares S_1 and S_2 . The second secret is obtained after share S_1 is rotated anti-clockwise 90 degrees and then superimposed on share S_2 . The degree of the angles used for obtaining the secrets is 90 or 180 or 270 and the scheme shares, at most, two secrets.

Because of this it becomes quite obvious that it was quite restricted for use. Other researchers have also proposed such schemes [2][5].

Fig.4 shows an example of dynamic visual cryptography.

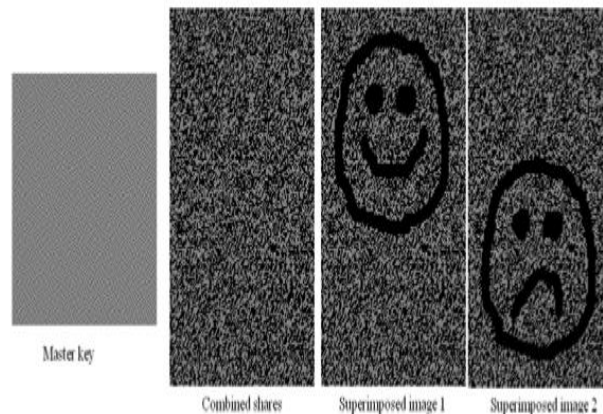


Figure 2.5 Joint contrast visual cryptography (Dynamic Visual Cryptography)[2]

Nowadays color or natural images are more common in existence than binary images. Color visual cryptography was developed so as to apply visual cryptography on such images.

Different researchers have used different approaches. Some of them have divided images into color spaces of C, M, Y or R, G, B and then processed them into shares or

some of them convert images to binary and then perform original Visual Cryptography scheme [1].

Even some convert original image to halftone image and then generate the shares and so on. An example of basic Color visual cryptography scheme is shown in the Fig.5 below:-

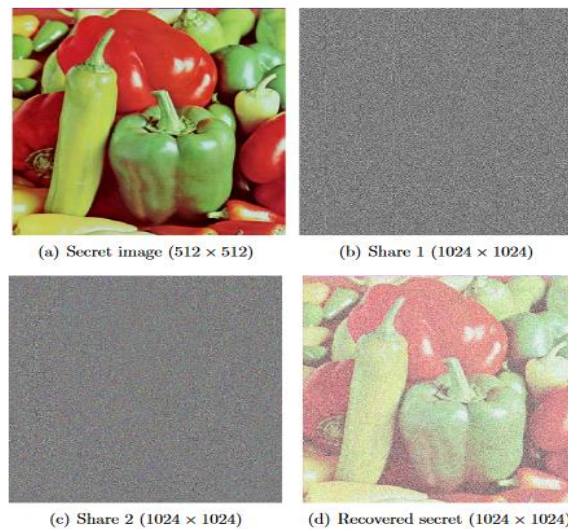


Figure 2.6 Color Visual Cryptography [2]

Progressive VC takes into the consideration the premise of perfect screen recovery and high quality secret reconstruction. Many schemes do require computational efforts to perfectly recover the secret.

The meaning of progressive refers to how the original image is built up. For example when downloading or viewing an image on web page, the image is loaded in stages.

The full dimension of the image is visible but it is very blurry. As more of the image is downloaded, the clearer the resulting image becomes until it is fully loaded. [2]. Fig.6 shows an example of this technique.

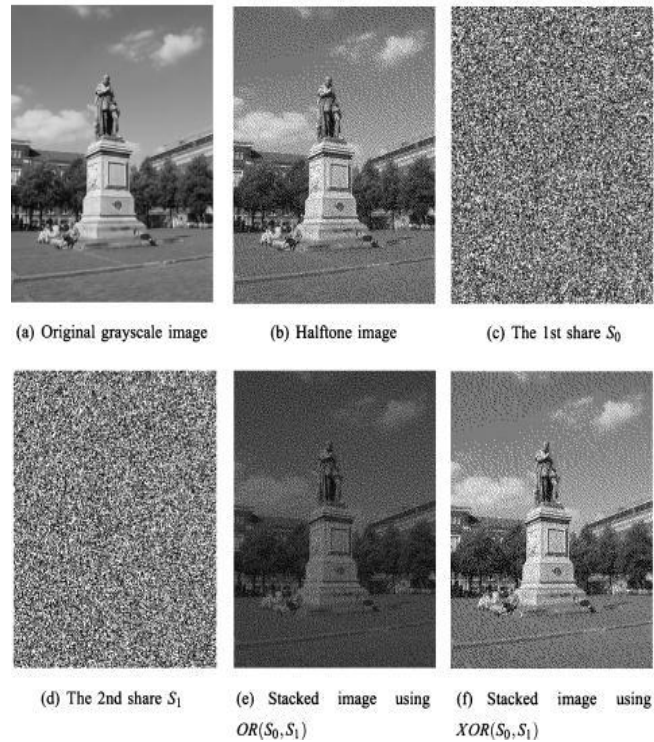


Figure 2.7 Progressive Visual Cryptography [6]

Various methods of visual cryptography are summarized in tabular form below. TABLE I gives a list of various methods. Each method is listed with various properties such as image format, number of secret images, etc and so on.

Table 2.1 Comparison between Properties of Various Methods

Year	Author(s)	Image Format	# of secret images	Type of the Share	Pixel Expansion
1994	Noar, Shamir	Binary	1	Meaningless	4
1997	VerheulTilborg	Color	1	Meaningless	$c*3$
1998	Wu , Chen	Binary	2	Meaningless	4
2000	Yang , Liah	Color	1	Meaningless	$c*2$
2000	Chang, Tsai	Color	1	Meaningless	529
2002	Chin Chen Chang et.al	Grayscale	1	Meaningful	9

2003	Young -Chang Hou	Color	1	Meaningless	4
2004	Hsu et al	Binary	2	Meaningless	4
2005	Lukac and Plataniotis	Grayscale	1	Meaningless	4
2005	Chin-Chen Chang et.al	Binary	1	Meaningful	4
2005	Wu and Chang	Binary	2	Meaningless	4
2006	S.J. Shyu	Color	1	Meaningless	$\log_2 c * m$
2006	R.Youmara n et.al	Color	1	Meaningful	9
2006	Liguo Fang et.al	Binary	1	Meaningless	2
2007	S.J. Shyu et.al	Binary	$n(n \geq 2)$	Meaningless	$2n$
2007	W.P. Fang	Binary	2	Meaningless	9
2008	Jen- BangFeng et.al	Binary	$n(n \geq 2)$	Meaningless	$3n$
2008	Mustafa Ulutas et.al	Binary	2	Meaningless	4
2008	Tzung Her- Chan et.al	Binary	2	Meaningless	1
2008	Tzung Her- Chan et.al	Binary/ Gray/C olor	$n(n \geq 2)$	Meaningless	4
2008	Mohsen Heidarinejei d et.al	Color	1	Meaningless	9/16
2008	F. Liu	Color	1	Meaningless	1

2008	HaiboZang et.al	Gray	1	Meaningless	1
2009	Jonathan Weir et.al	Binary	N	Meaningless	4
2009	Wei Qiao et. Al	Color	1	Meaningless	m
2009	Du-Shiau Tsai et.al	Color	1	Meaningful	9
2011	M. Arun Kumar , K. Jon Singh	Color	1	Meaningless	-
2013	Kaur, Khemchand ani	Color	1	Meaningless	4
2015	K.Shankar, P.Eswaran	Color	1	Meaningless	-
2016	K.Shankar, P.Eswaran	Color	1	Meaningless	-
2016	K.Shankar, P.Eswaran	Color	1	Meaningless	-

TABLE 2.2 provides a brief description of all the methods that were tabulated in table 2.1 above.

Table 2.2 Description of Various Methods

Year	Author(s)	Description of the method	Ref
1994	Noar, Shamir	Uses predetermined coding table to generate shares. Stack and OR shares to reconstruct secret.	[1]
1997	Verheul Tilborg	Arcs are used to construct shares. Single pixel is transformed into m-sub pixels,	[7]

		and all of these sub pixels are further separated into c-color regions. Every sub pixel has just one colored region, and remaining regions are black.	
1998	Wu , Chen	Angle restrictions to create secrets.	[5]
2000	Yang , Liah	Uses general access structure to construct (k,n) scheme.	[8]
2000	Chang,Tsai	Using a fixed Index Table for colours, the color image containing secret will be inserted inside two disguise pictures.	[9]
2002	Chin Chen Chang et.al	As we use fixed Size of these shares; and do not change at the point where the count of colours present in the secret image vary. No predefined Color Index Table is taken into this method.	[10]
2003	Young -Chang Hou	Create four shares C, M, Y, B. The secret won't be retrieved without the black one.	[11]
2004	Hsu et al	Arbitrary angle rotation is used to create the second secret.	[12]
2005	Lukac and Plataniotis	Decomposing the greyscale image into 8 bit planes. B-bit planes are used further to construct the shares.	[13]
2005	Chin-Chen Chang et.al	Random noise shares are generated and then these shares embedded into cover images using Steganography	[14]
2005	Wu and Chang	Using circular shares to restrict the angle restriction conditions of earlier methods.	[15]

2006	S.J. Shyu	A c-colored k-out-of-n V.S.S.S. by use of pixel expansion of $\log_2 c \times m$ which is more efficient than all other schemes.	[16]
2006	R.Youmaran et.al	Enhanced visual cryptographic technique for concealing a colored image into numerous colored cover images. Improves the SNR of the disguise images by creating images with a quality very much same as other quality of original secret.	[17]
2006	Liguo Fang et.al	Maintaining the performance between expansion of pixels and image contrast of original VC Scheme.	[18]
2007	S.J. Shyu et.al	Hides $n \geq 2$ secrets into two circular shares. These secrets can be revealed by stacking the first share and then rotating other share by various angles.	[19]
2007	W.P. Fang	Two secrets are embedded inside two shares; one of the secret is obtained simply through stacking both shares and the other secret is obtained through stacking two shares and then rotating one of them by 180 degrees..	[20]
2008	Jen-BangFeng et.al	Identifies the pixels of secret and related share blocks to derive a stacking relationship curve, where the nodes identify the blocks of share , and the arcs are the two blocks that have been stacked together on the required angle. Using the curve along with fixed set of visual patterns,	[21]

		two shares are created.	
2008	Mustafa Ulutas et.al	Shares are rectangular in nature and are developed in arbitrary way. Stacking two shares reveals the first secret. Rotating the 1st share by 90° counter clockwise and then stacking it with the 2nd share reveals the next secret.	[22]
2008	Tzung Her- Chan et.al	Numerous image encryption techniques using rotation of haphazard grids, without expansion of any pixel and code-book redesigning.	[23]
2008	Tzung Her- Chan et.al	Multiple-secrets visual cryptography scheme which is an extension to the conventional visual secret sharing scheme.	[24]
2008	Mohsen Heidarinejeid et.al	Ideal reconstruction which produces smaller size shares compared to the secret image using max. distance Separable approach. The scheme has lesser expansion of pixel.	[25]
2008	F. Liu	Color visual Cryptography method inspired from Noar and Shamir. Zero pixel expansion in this method proposed. The rise in the amount of colors of obtained secret image does not change the expansion of pixels.	[26]
2008	HaiboZang et.al	It employs a Multi -pixel encoding approach. Assigns uneven number of pixels for each iteration.	[27]
2009	Jonathan Weir et.al	Multiple-secrets embedding visual cryptography method. A Master key is produced for every secret; likewise,	[28]

		master key is used to share the secrets and multiple shares are reconstructed.	
2009	Wei Qiao et. al	Method for color image visual cryptography that is developed using halftone scheme.	[29]
2009	Du-Shiau Tsai et.al	Neural networks, blended with variant visual secret sharing, the class of the obtained secret image and disguise images are visually identical to the respective original images.	[30]
2011	M. Arun Kumar , K. Jon Singh	R, G, B components are first passed through error noise filter and then these are encrypted using AES.	[31]
2013	Kaur, Khemchandani	Color image divided into 2 shares based on original technique[1] and then encryption using RSA	[32]
2015	K.Shankar, P.Eswaran	R, G, B components are XORed with Random Key Matrix and then AES encryption is performed.	[33]
2016	K.Shankar, P.Eswaran	Extension of their previous method [33]. This time it is (k,n) scheme which was earlier (2,2).	[34]
2016	K.Shankar, P.Eswaran	R,G,B based share creation using Optimal Elliptic Curve Cryptography	[35]

CHAPTER 3 PROPOSED METHODOLOGY

3.1 Secure and Efficient (2,2) Color Visual Cryptography

This method uses an existing methodology proposed by K. Shankar in [34] as base. On top of this existing methodology, a new methodology is proposed. This method answers the problems that are found in the existing methodology. Secondly, algorithm is used with other security algorithms such as stream ciphers and lightweight algorithms. In research until now, researchers and scholars used visual cryptography with cryptographic algorithms such as AES, RSA, and Elliptic Curve Cryptography.

In this technique, the overall process is implemented by first developing a method to solve the problems found in existing technique, and then secondly, various cryptographic algorithms are used and evaluated with visual cryptography.

The images below illustrate the existing technique. After that, problems of this method are summarized. Next, the solution to these problems is explained using new method proposed. Also, use of stream ciphers and lightweight algorithms along with visual cryptography showed improved results as compared to the results seen until now.

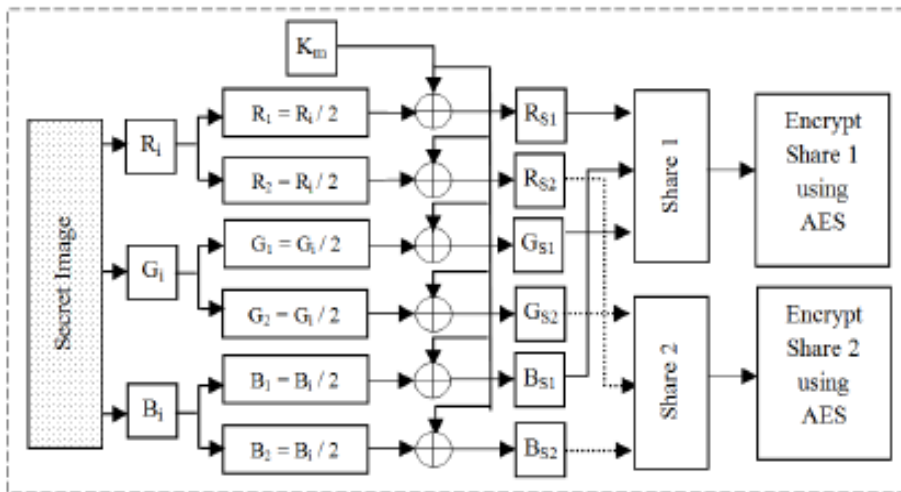


Figure 3.1 Original (2,2) VCS Scheme

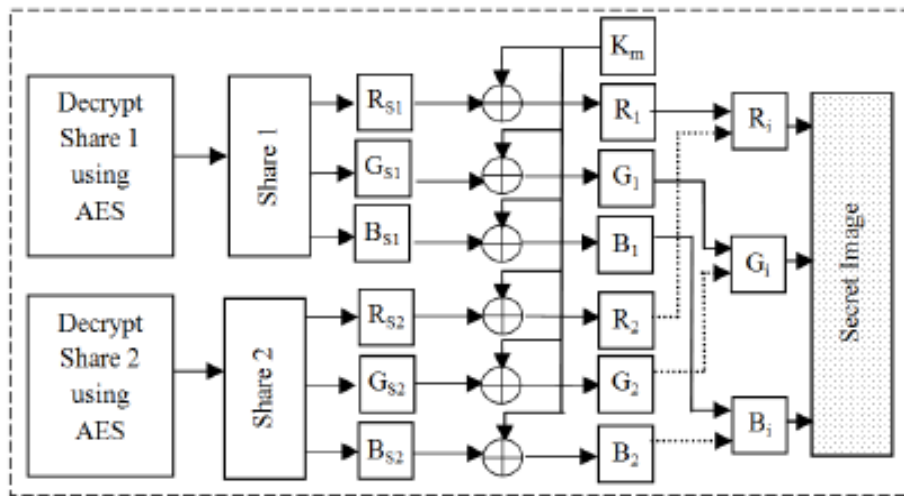


Figure 3.2 Original (2,2) VCS Scheme Restoration

The problems observed in the above method are:-

- i) Key creation and distribution used for the encryption algorithm are not discussed.
- ii) Sending of global key matrix (that is used to construct shares from the original secret images) is also not discussed. Global key matrix needs to be same for a communication between sender and receiver, so some method needs to be suggested to share the matrix.
- iii) Run time of the overall algorithm shown is very less; such time can only be expected when encryption is not performed.
- iv) Efficiency of existing encryption algorithms used alongside visual cryptography.
- v) The question still arises that is encryption still necessary and needed alongside visual cryptography

Now, below we see the flow diagram of proposed technique which answers the above problems.

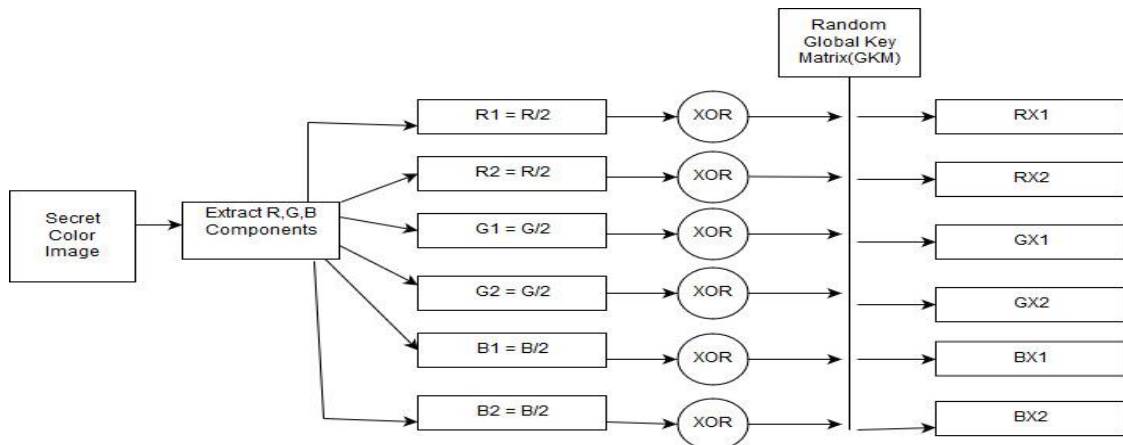


Figure 3.3 Proposed Efficient VCS Share Generation part a

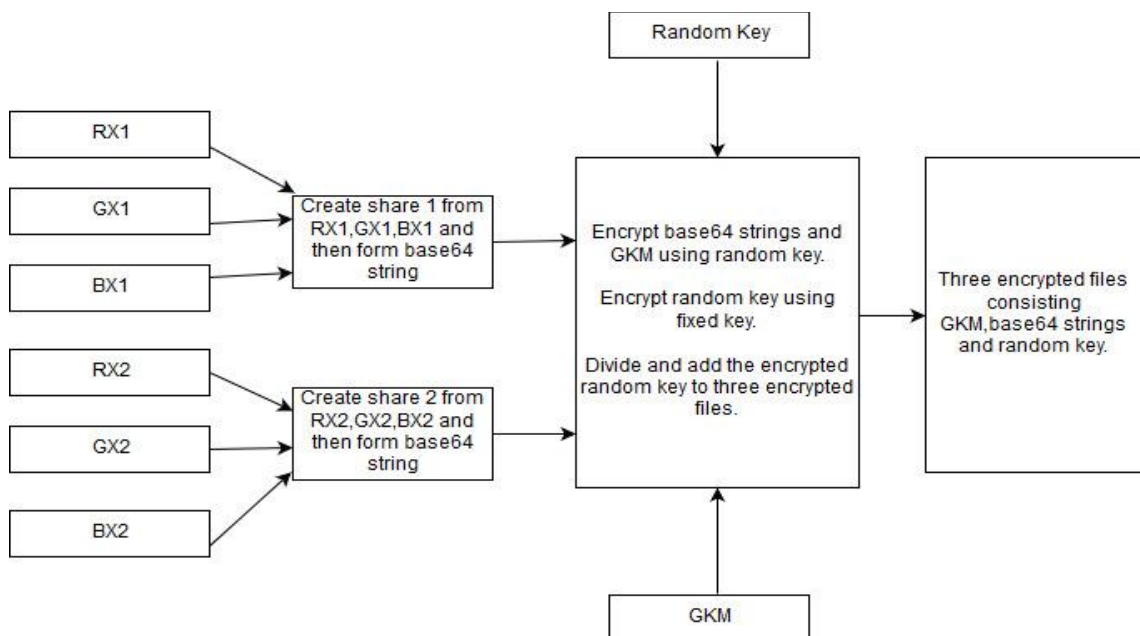


Figure 3.4 Proposed Efficient VCS Share Generation part b

The above two images show the share generation process workflow. This is explained in the steps discussed below:-

- i) R, G, B components are extracted from the input secret color image.
- ii) These components are divided into two equal parts, thereby making a total of 6 components.

iii) Global key matrix is generated using random numbers. Each random number gives a value between the ranges of 0 to 255, since we are using 8 bit images.

iv) These 6 components R1, R2, G1, G2, B1, and B2 are XORed with a global key matrix (generated in the previous step).

v) Share1 is created using components RX1, GX1 and BX1. Share 2 is created using components RX2, GX2, and BX2.

vi) Both the shares generated in the above step are converted into their equivalent base64 strings.

vii) Generate a random key consisting of small-case letters, upper-case letters, numbers, and special symbols.

viii) Both base64 strings and global key matrix are encrypted using the random key generated in the above step.

ix) The software has a master or fixed key. Encrypt the random key using this fixed key.

x) Divide the encrypted key formed in step (ix) above in three equal parts and mix it with data of three files consisting of base64 string1, base 64 strings 2 and global key matrix respectively.

The two figures below describe the secret reconstruction process from the two shares generated.

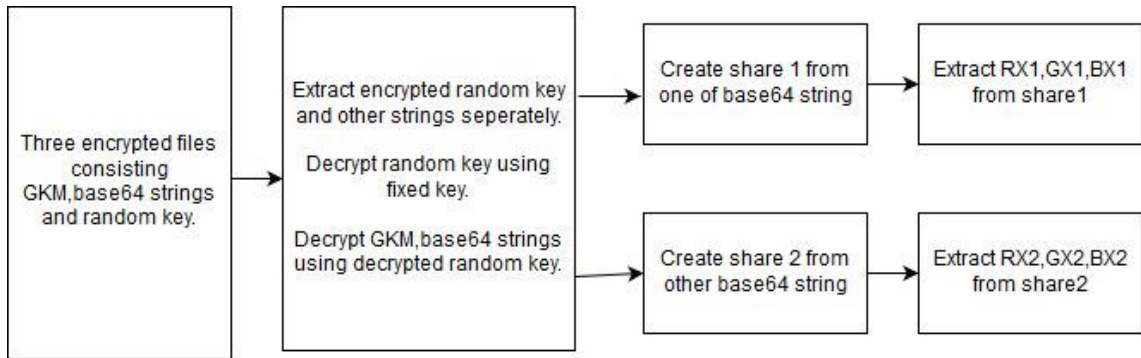


Figure 3.5 Proposed Efficient VCS Secret Restoration part a

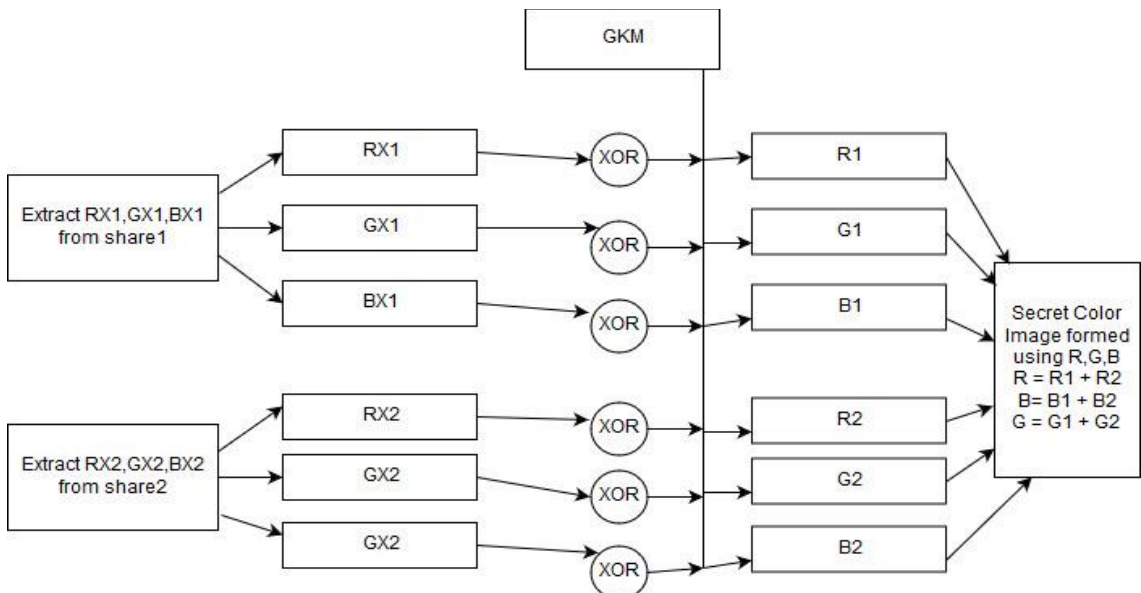


Figure 3.6 Proposed Efficient VCS Secret Restoration part b

The above two figures show the secret reconstruction process workflow. This is explained in the steps discussed below:-

- i. Data is separated from each of the three files into 2 parts respectively. One part is the encrypted data and other part is portion of encrypted random key.
- ii. Form the encrypted random key.
- iii. Decrypt the random key using fixed key.

- iv. Decrypt the base64 strings and global key matrix using the random key formed in step (iii) above.
- v. Share1 is created using base64 string1. Share2 is created using base64 string2
- vi. Extract the components RX1, GX1, BX1 from share1 and extract the components RX2, GX2, BX2 from share2.
- vii. After the above steps, we get 6 components R1, R2, G1, G2, B1, and B2.
- viii. Obtain R, G, B, by the following equations $R = R1+R2$, $G = G1 + G2$ AND $B = B1 + B2$.
- ix) Create the final image using components R, G and B.

The proposed method answers the above problem in the following manner:-

- i. Key creation and distribution is explained properly in the algorithm.
- ii. Global key matrix is also sent along the shares to the intended receiver for secret reconstruction or restoration. It must be encrypted first before sending.
- iii. Proper analysis and performance evaluation of various algorithms is done (see section 5.1).
- iv. Lightweight algorithms show much better performance than used in the existing literature.
- v. Visual cryptography was used as a method, so that no other method of encryption was to be used with it. But research stated that this technique can be hacked. So, researchers started adding encryption algorithms to visual cryptography. Proposed method tells that as such encryption is not needed along with visual cryptography. But if we want to use some key matrix or key in between then we should consider encryption for protection of key.

3.2 Two Secret (2,2) Color Visual Cryptography

This proposed algorithm is called as interleaved multi-secret visual cryptography with enlarged shares. This technique works as an extension from the standard method of (2,2) Color Visual Cryptography. The standard method hides one secret within 2 shares, and both shares are needed to re-obtain the original color image or original secret. This proposed methodology hides 2 secrets within 2 shares it by enlarging the shares to some extent.

The flow of the overall process of the proposed technique for share construction can be seen from the two figures below:-

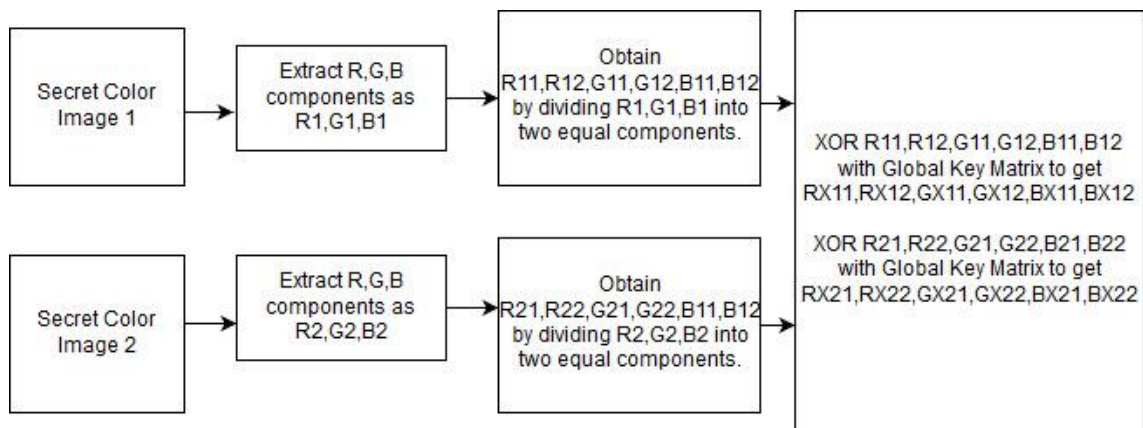


Figure 3.7 Proposed 2 Secret (2,2) VCS Share Generation part a

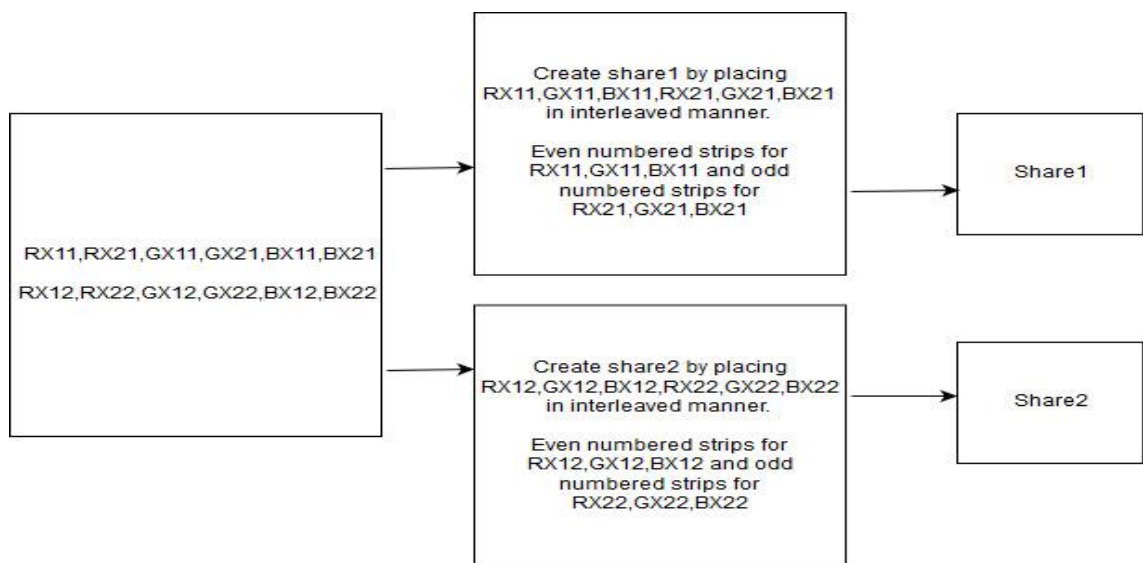


Figure 3.8 Proposed 2 Secret (2,2) VCS Share Generation part b

The above figures illustrate the process of concealing two secrets in two shares itself. The workflow can be explained in the steps discussed below:-

- i) Take two color images as input or secrets. Crop and adjust these two images in a size dimension of 400×400 (where width = 400 and height = 400).
- ii) Extract respective color components of both secrets separately. Color components of secret 1 are termed as R1, G1, B1, whereas color components of second secret are termed as R2, G2, and B2.
- iii) Next, we obtain a total of 12 components from these 6 components (obtained in the previous step). Each individual component is broken into two equal components.
- iv) Global key matrix is generated using random numbers. Each random number gives a value between the ranges of 0 to 255, since we are using 8 bit images.
- v) After obtaining the twelve different components, XOR each component with a Random Global Key Matrix, also called GKM. Construction of GKM is detailed in the previous step.
- vi) Now, generate two empty images as share1 and share2. Dimensions of both empty shares should be 800×400 (where width = 800 and height = 400).
- vii) Execute a loop (refer Appendix A1)
- viii) Execute a similar loop as seen in step (vii) for constructing share2 with components.
- ix) Two shares are constructed after step (viii). These two shares successfully embed two secrets inside them.

The proposed method uses the word interleaved because shares are formed by adding components of the secret color images in an interleaved style. Enlarged shares are called because if only one secret was hided using this method then dimension of share would have been equal to the dimensions of image.

The flow of the overall process of the proposed technique for secrets reconstruction from the constructed two shares can be seen from the two figures below:-

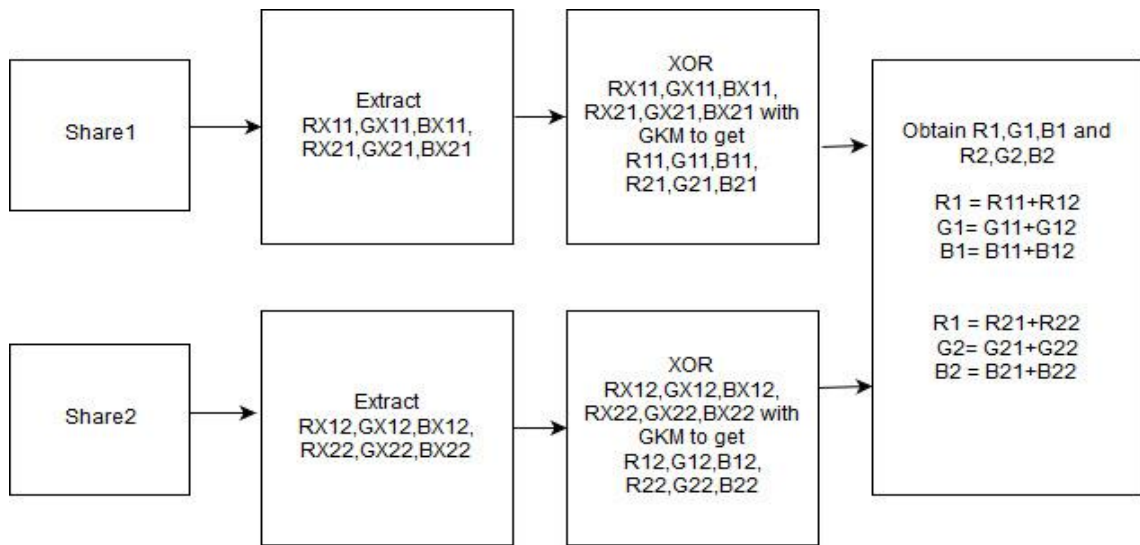


Figure 3.9 Proposed 2 Secret (2,2) VCS Secret Restoration part a

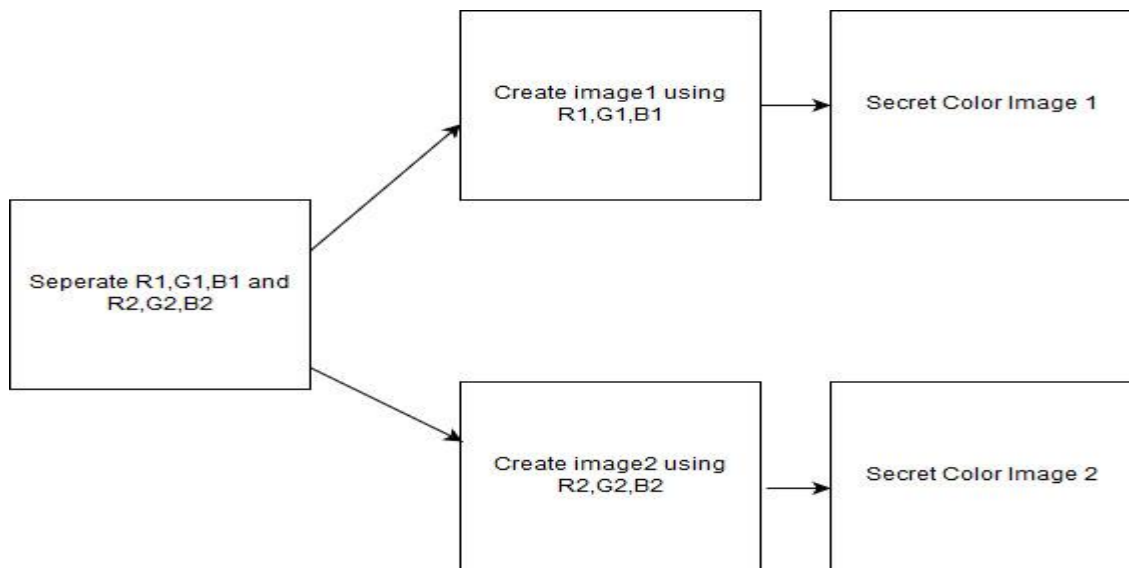


Figure 3.10 Proposed 2 Secret (2,2) VCS Secret Restoration part b

The above figures illustrate the process of reconstruction of two secrets back from earlier constructed two shares. The workflow can be explained in the steps discussed below:-

i) From each individual shares, extract components as RX11, GX11 ,BX11 ,RX21 , GX21,, BX21 from share1 and RX12,GX12,BX12,RX22,GX22 and BX22 from share2 respectively.

ii) Add components such as RX11 and RX12 to get a component called RX1.

iii) Apply step (ii) for other color components as well so as to get a total of 6 components in the last. These six components of color will be RX1, GX1, BX1, RX2, GX2, and BX2.

iv) XOR the six components obtained in the earlier step with global key matrix (GKM). Now, the components are called as R1, G1, B1, R2, G2 and B2.

v) Create secret1 from the components R1, G1 and B1.

v) Create secret2 from the components R2, G2 and B2.

This method is performed by enlarging the share horizontally (i.e. the width is made double to incorporate room for two secrets.) Alternate configuration for the proposed method is also possible (i.e. we can make the size dimensions of shares as 400*800, whereby we are enlarging the shares along their height and not their width).

If we were to use the alternate configuration as described above then loop to create the shares will be modified as following :-

```

for (int y = 0; y <400; y++)
{
for (int x = 0; x < 800; x++)
{
if(x is even)
{
int t = (x / 2);
Add components RX11, GX11, BX11 to share1 at location (y,x)
}
else
{
int t = (x - 1);
t = t / 2;
Add components RX21, GX21, BX21 to share1 at location (y,x)
}
}
}
}

```

3.3 Three Secret (2,2) Color Visual Cryptography

This proposed algorithm is also called as interleaved multi-secret visual cryptography with enlarged shares. This technique works as an extension from the standard method of (2,2) Color Visual Cryptography. The standard method hides one secret within 2 shares, and both shares are needed to re-obtain the original color image or original secret.

This proposed methodology hides 3 secrets within 2 shares it by enlarging the shares to some extent.

The flow of the overall process of the proposed technique for share construction can be seen from the two figures below:-

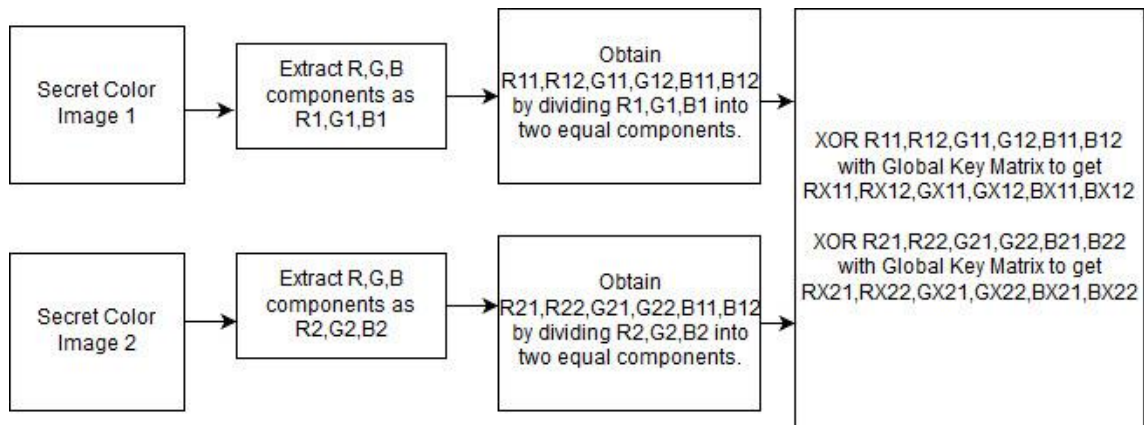


Figure 3.11 Proposed 3 Secret (2,2) VCS Share Generation part a

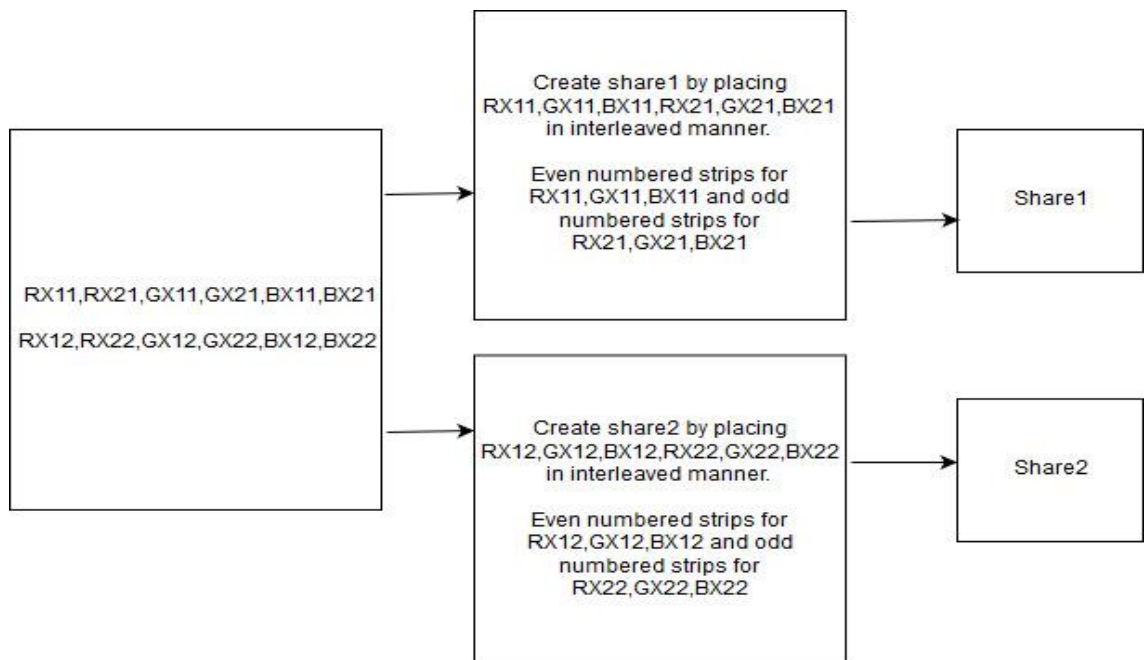


Figure 3.12 Proposed 3 Secret (2,2) VCS Share Generation part b

The above figure demonstrates the process of embedding three secrets in two shares itself. The workflow can be explained in the steps discussed below:-

- i) Take three color images as input or secrets. Crop and adjust these two images in a size dimension of 400*400(where width = 400 and height = 400).

- ii) Extract respective color components of these three secrets separately. Color components of secret 1 are termed as R1,G1,B1 , whereas color components of second secret are termed as R2,G2,B2 and , color components of second secret are termed as R3,G3,B3.
- iii) Next, we obtain a total of 18 components from these 9 components (obtained in the previous step). Each individual component is broken into two equal components.
- iv) Global key matrix is generated using random numbers. Each random number gives a value between the ranges of 0 to 255, since we are using 8 bit images.
- v) After obtaining the eighteen different components, XOR each component with a Random Global Key Matrix, also called GKM. Construction of GKM is detailed in the previous step.
- vi) Now, generate two empty images as share1 and share2. Dimesions of both empty shares should be 1200*400(where width = 1200 and height = 400).
- vii) Execute a loop as follows (for full loop, refer Appendices A2):-
- viii) Execute a similar loop as seen in step (vii) for constructing share2 with components.
- ix) Two shares are constructed after step (viii). These two shares successfully embed three secrets inside them.

The proposed method uses the word interleaved because shares are formed by adding components of the secret color images in an interleaved style. Enlarged shares are called because if only one secret was hided using this method then dimension of share would have been equal to the dimensions of image.

The flow of the overall process of the proposed technique for three secrets reconstruction from the constructed two shares can be seen from the two figures below:-

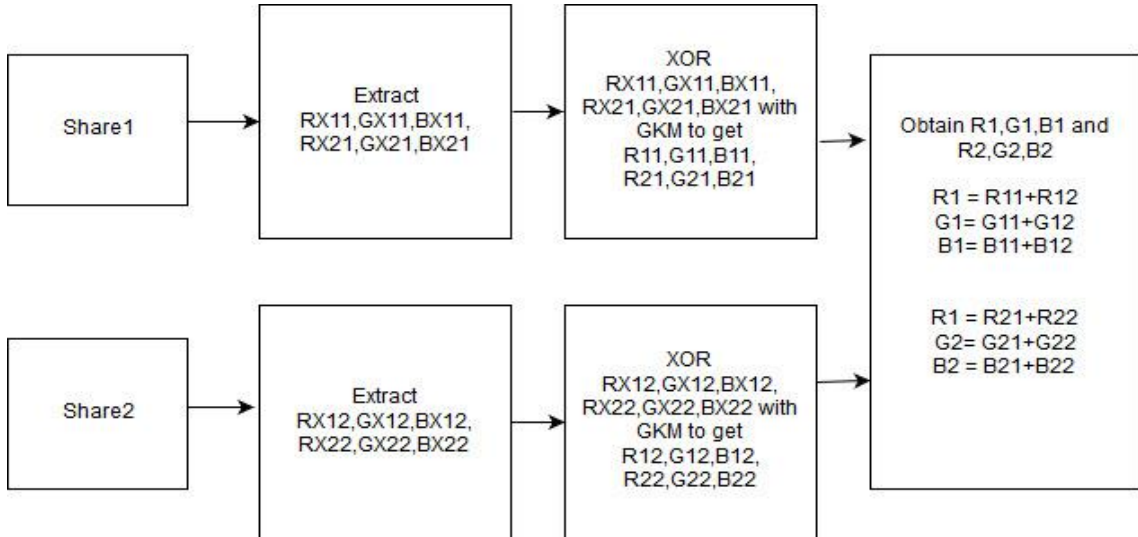


Figure 3.13 Proposed 3 Secret (2,2) VCS Secret Restoration part a

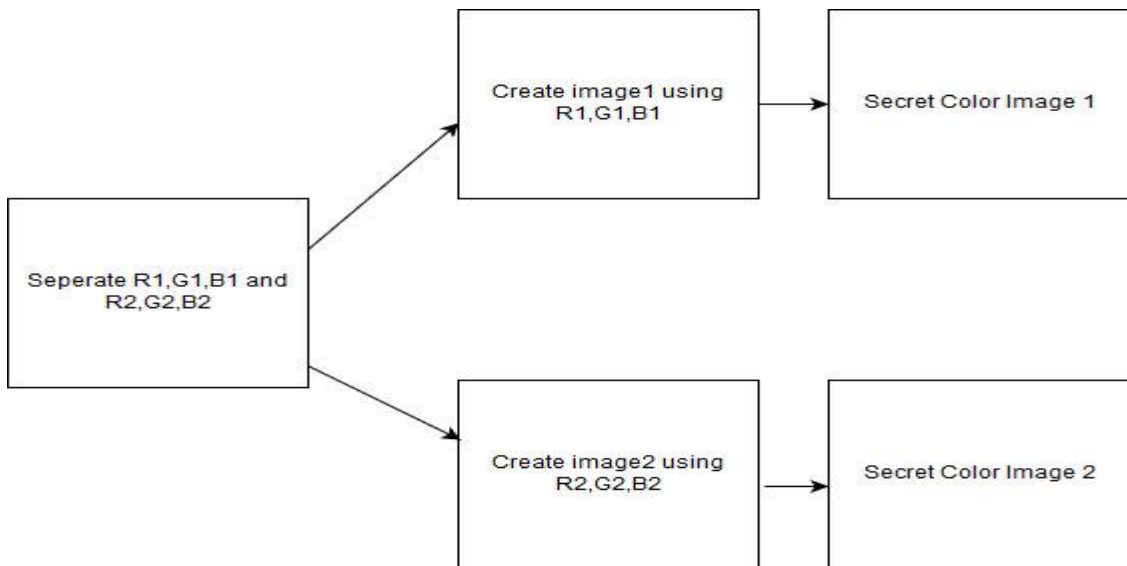


Figure 3.14 Proposed 3 Secret (2,2) VCS Secret Restoration part b

The above figures illustrate the process of reconstruction of three secrets back from earlier constructed two shares. The workflow can be explained in the steps discussed below:-

- i) From each individual shares, extract components as RX11, RX21,RX31 , GX11 ,GX21, GX31 , BX11, BX21, BX31 from share1 and extract components as RX12, RX22, RX32 , GX12 ,GX22, GX32 , BX12, BX22, BX32 from share2 respectively.
- ii) Add components such as RX11 and RX12 to get a component called RX1.
- iii) Apply step (ii) for other color components as well so as to get a total of 9 components in the last. These 9 components of color will be RX1, GX1, BX1, RX2, GX2, BX2, RX3, GX3 and BX3.
- iv) XOR the nine components obtained in the earlier step with global key matrix (GKM). Now, the components are called as R1, G1, B1, R2, G2, B2, R3, G3 and B3.
- v) Create secret1 from the components R1, G1 and B1.
- vi) Create secret2 from the components R2, G2 and B2.
- vii) Create secret3 from the components R3, G3 and B3.

This method is performed by enlarging the share horizontally (i.e. the width is made double to incorporate room for two secrets.) Alternate configuration for the proposed method is also possible (i.e. we can make the size dimensions of shares as 400*800, whereby we are enlarging the shares along their height and not their width).

If we were to use the alternate configuration as described above then loop to create the shares will be modified as following :-


```

for (int y = 0; y <400; y++)
{
for (int x = 0; x < 800; x++)
{
if (x is even)
{
int t = (x / 2);
Add components RX11, GX11, BX11 to share1 at location (y,x)
}
else
{
int t = (x - 1);
t = t / 2;
Add components RX21, GX21, BX21 to share1 at location (y,x)
}
}
}
}

```

3.4 new k out of n Color Visual Cryptography

This proposed algorithm is a modified scheme of (k,n) visual cryptography. This technique works as an extension from the standard method of (2,2) Color Visual Cryptography and uses concepts of (k,n) VCS. The scheme is implemented as (2,3) VSS where a single image is distributed as three transparencies. At least 2 out of these 3 are required to obtain the secret. All the three transparencies will reveal full secret.

The workflow for shares generation can be explained in the steps discussed below:-

- i) Take a color input image as secret image. Crop an image into a size of say 300*300.
- ii) Extract the components of image as R, G, and B.
- iii) Divide the components one by one as follows:-

- a.) Scan the image pixel by pixel.
- b.) For a color component value = V at some pixel location (y,x) , take a scale of values ranging from 0 to V .
- c.) Now divide this scale of values into equal portions such that we are able to extract exactly n values.
- d.) For example, suppose pixel color component red value = 150 at location $(20, 10)$ then the scale will be 0 to 150. Now, for $(2, 3)$ VSS, the scale will be further segregated into equal components so as to extract 3 values. So, our scale will be 0 to $25(V/6$ or $V/2k)$, 25 to $50(V/6$ or $V/2k$ to $V/3$ or $V/k)$, and then 50 to 150.
- e.) Call random function to obtain a random value from each of these segregated equal portions on the value scale.
- f.) Assign the random value computed to each share respectively.
- g.) Repeat the overall steps for creating all three color components R, G, B of each individual share.
- h.) Add R, G, B values for location pixel (y, x) and check the difference between computed sum and original sum of these components. If there is difference then adjust the component difference by adding or removing a factor unit of $\text{difference}/k$ from each share calculated component.
- iv) Once all shares are created. Compute a global key matrix of size equal to size of cropped secret image.
- v) Mathematically perform XOR between each color component of each share with GKM computed in previous step.
- vi.) Finally, the shares are obtained.

The above steps detailed the process used for constructing n shares from a secret color image that was provided as input by the user of the system.

Now the steps detailed below describe the process of workflow used to generate or restore the original secret back from these n shares created earlier.

The workflow for secret restoration is explained in the steps discussed below:-

- i) Take input in the form of two options: - a.) GKM along with any of k shares
b.) GKM with every n share.
- ii) Extract the components of share1 as R1,G1, and B1
- iii) Similarly extract the components of other shares as well.
- iv) Once all shares are created. Mathematically perform XOR between each color component of each share with GKM computed in previous step.
- v.) Now we have components as RX1, GX1, and BX1 for share1 and so on for others,
- vi) Add all same color components to get one final full color component. For example, all calculated RX1, RX2, and so on to get one RX component.
- vii) Divide the components by 255 to keep them in range of color values for 8 bit image.
- viii) Now, after all the processing as discussed in earlier steps, we have three final color components as RX, GX, and BX.
- ix) Obtain the final image by these components.
- x) The secret image is formed

CHAPTER 4 EXPERIMENTAL SETUP AND RESULTS

4.1 Experimental Setup

Algorithms proposed in Chapter 3 were implemented and tested successfully over different images. Algorithms were implemented using C# language in Microsoft Visual Studio 2012 .Out of 10 algorithms compared in section 4.2, 6 were implemented using Bouncy Castle C# Library which is inbuilt in .NET Framework 4.5.

The configuration of the system used is as follows:-

- i) Intel core i5-3rd generation
- ii) 4GB DDR3 RAM
- iii) Windows 7 Ultimate

Images used for the testing and analysis of the algorithms is shown below:-



Below we can view the home screen of the implemented project.

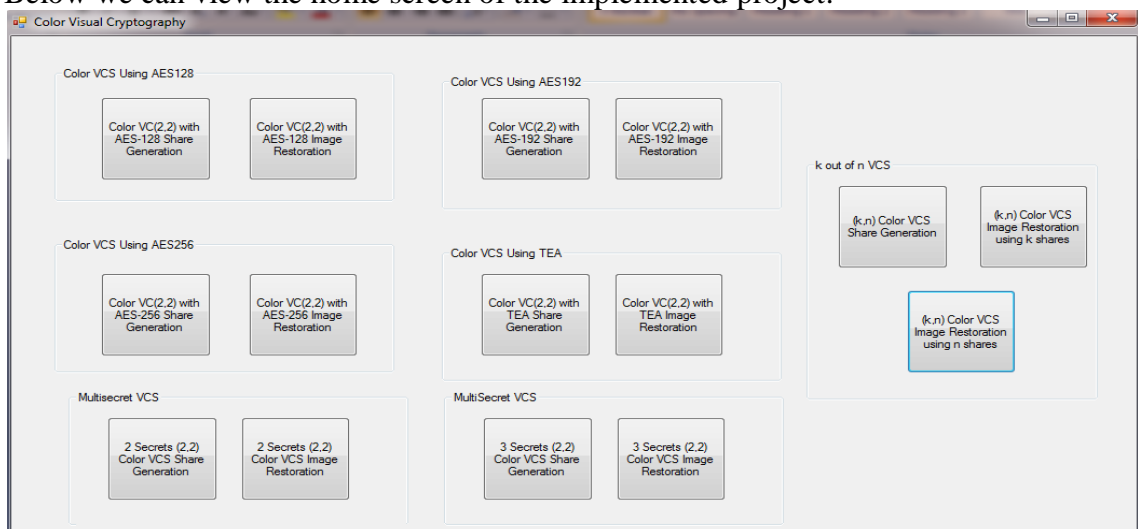


Figure 4.1 Project Home Screen 1

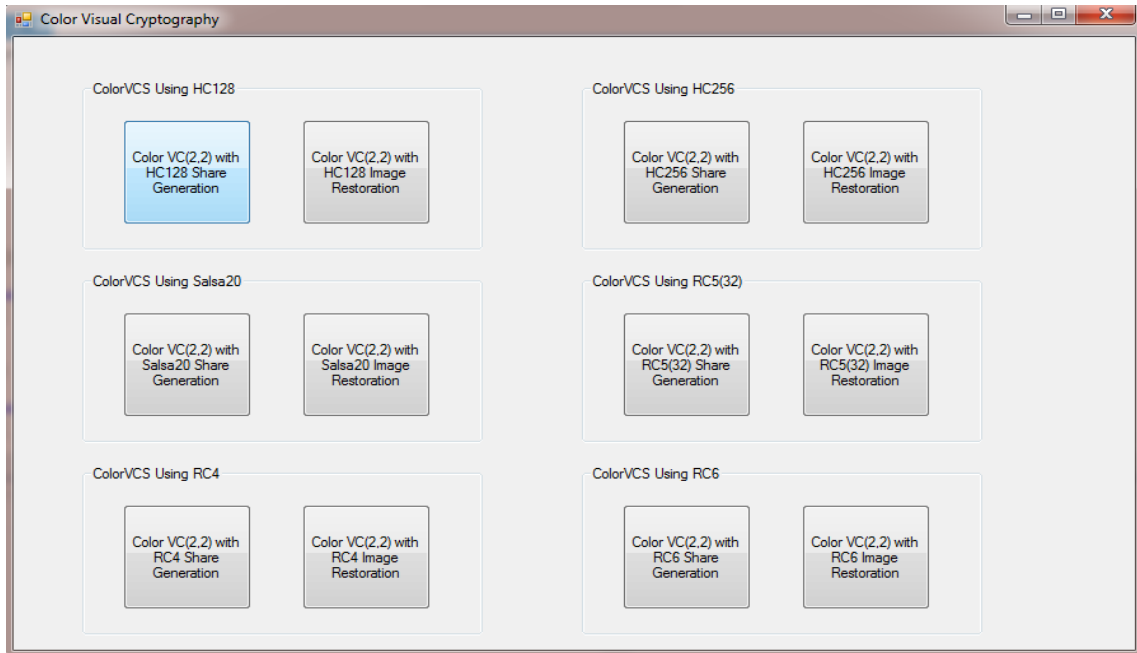


Figure 4.2 Project Home Screen 2

4.2 Results of Secure and Efficient (2,2) Color Visual Cryptography

Here, we can see the results of the methodology proposed in section 3.1 for various images. First three images below shows the overall workflow of the algorithm. Next, we observe the results of each image respectively.

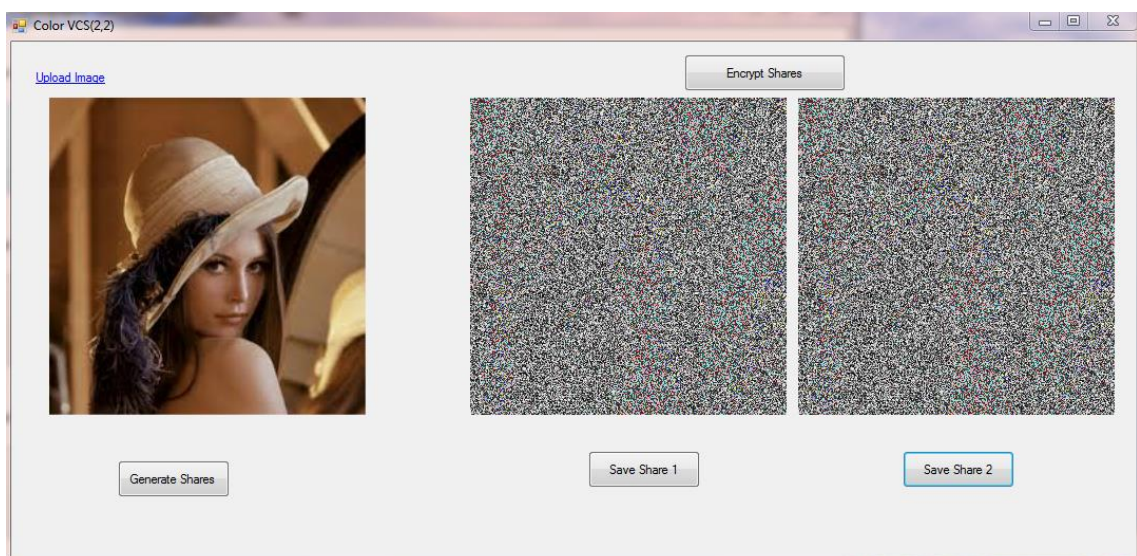


Figure 4.3 Efficient (2,2) VCS Share Generation

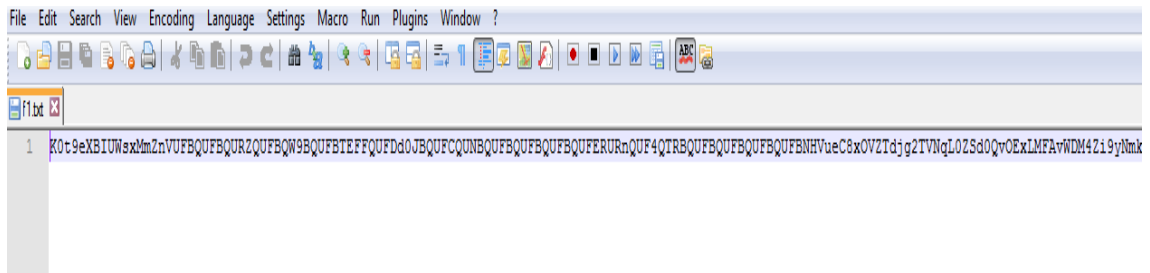


Figure 4.4 Encrypted base64 Image

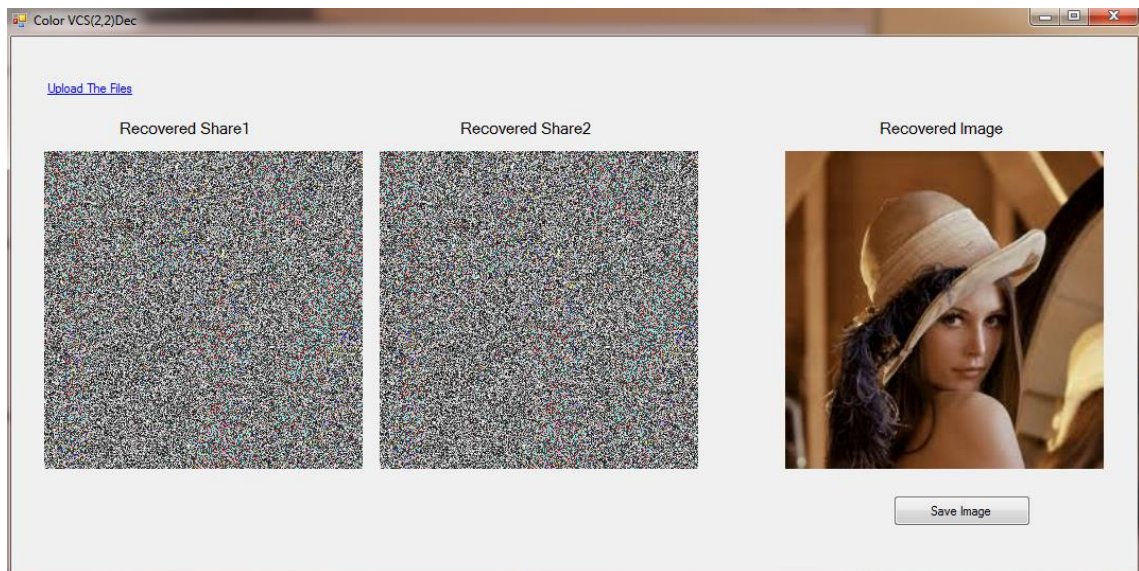


Figure 4.5 Efficient (2,2) VCS Secret Restoration

Below, the results are shown for each image respectively in a tabular manner. Total of 10 algorithms were evaluated for these images and the overall process.

6 algorithms used were Block Ciphers consisting of AES-128, AES-192, AES-256, RC5 (32), RC6, TEA.

4 algorithms used were Stream ciphers consisting of HC128, HC256, Salsa20 and RC4.

HC128, HC256, and Salsa20 are also called lightweight stream ciphers.

Penguin.jpg



Table 4.1 Algorithm 3.1 Results for Penguin Image

Algorithm Used	Share Generation Time	Secret Reconstruction Time	Total Output File Sizes
AES-128	0.435 seconds	0.426 seconds	3.25 MB
AES-192	0.424 seconds	0.424 seconds	3.26 MB
AES-256	0.465 seconds	0.445 seconds	3.26 MB
TEA	0.697 seconds	0.569 seconds	7.33 MB
RC5(32)	0.504 seconds	0.437 seconds	1.63 MB
RC6	0.464 seconds	0.376 seconds	1.66 MB
RC4	0.311 seconds	0.307 seconds	1.63 MB
HC128	0.364 seconds	0.325 seconds	1.63 MB
HC256	0.347 seconds	0.325 seconds	1.63 MB
Salsa20	0.384 seconds	0.347 seconds	1.63 MB

It can be clearly observed from the above tabular data that:-

- i) Lightweight stream ciphers performed the best in both terms: time and space used.
- ii) In stream ciphers, RC4 has performed the best, but its use has been discontinued in most of the places around the world due to its potential flaws.
- iii) Hence, as per above point, we will consider that HC256 performed as the best security algorithm for this image.
- iv) In block ciphers, AES-192 gives the best share generation time, and RC6 gives best share reconstruction time.

Lena.jpg



Table 4.2 Algorithm 3.1 Results for Lena Image

Algorithm Used	Share Generation Time	Secret Reconstruction Time	Total Output File Sizes
AES-128	0.414 seconds	0.435 seconds	3.26 MB
AES-192	0.457 seconds	0.444 seconds	3.26 MB
AES-256	0.470 seconds	0.449 seconds	3.26 MB
TEA	0.661 seconds	0.556 seconds	7.35 MB
RC5(32)	0.422 seconds	0.373 seconds	1.63 MB
RC6	0.454 seconds	0.382 seconds	1.66 MB
RC4	0.343 seconds	0.329 seconds	1.63 MB
HC128	0.364 seconds	0.313 seconds	1.63 MB
HC256	0.367 seconds	0.325 seconds	1.63 MB
Salsa20	0.341 seconds	0.323 seconds	1.63 MB

It can be clearly observed from the above tabular data that:-

- i) Lightweight stream ciphers performed the best in both terms: time and space used.
- ii) Salsa20 performed as the best security algorithm for this image.
- iii) In block ciphers, AES-128 gives the best share generation time, and RC5 gives best share reconstruction time.

Baboon.jpg



Table 4.3 Algorithm 3.1 Results for Baboon Image

Algorithm Used	Share Generation Time	Secret Reconstruction Time	Total Output File Sizes
AES-128	0.421 seconds	0.426 seconds	3.26 MB
AES-192	0.443 seconds	0.442 seconds	3.26 MB
AES-256	0.439 seconds	0.440 seconds	3.26 MB
TEA	0.624 seconds	0.533 seconds	7.35 MB
RC5(32)	0.422 seconds	0.373 seconds	1.63 MB
RC6	0.391 seconds	0.379 seconds	1.66 MB
RC4	0.331 seconds	0.308 seconds	1.63 MB
HC128	0.355 seconds	0.312 seconds	1.63 MB
HC256	0.334 seconds	0.328 seconds	1.63 MB
Salsa20	0.326 seconds	0.315 seconds	1.63 MB

It can be clearly observed from the above tabular data that:-

- i) Lightweight stream ciphers performed the best in both terms: time and space used.
- ii) Salsa20 performed as the best security algorithm for this image.
- iii) In block ciphers, RC6 performed the best.

Finally, we can make the following observations after performing several iterations of each algorithm over different images:-

- i) The method is highly secure and difficult to hack since two keys are used for encryption, one key is embedded inside the software and second key is encrypted and mixed with the image data. Separating encrypted key from image data is itself a very difficult process, then key needs to be decrypted using embedded key. Embedded key is random string which is difficult to crack using brute force or dictionary attacks.
- ii) Stream ciphers or lightweight stream ciphers performed as the best security algorithm for images.
- iii) In block ciphers, RC6 performed better than the most famous and highly used AES algorithm

4.3 Results of Two Secret (2,2) Color Visual Cryptography

This section first demonstrates the overall workflow of the algorithm. The first two images shown below display that how the algorithm executes. After these two images, we see the performance of the algorithm for various images.

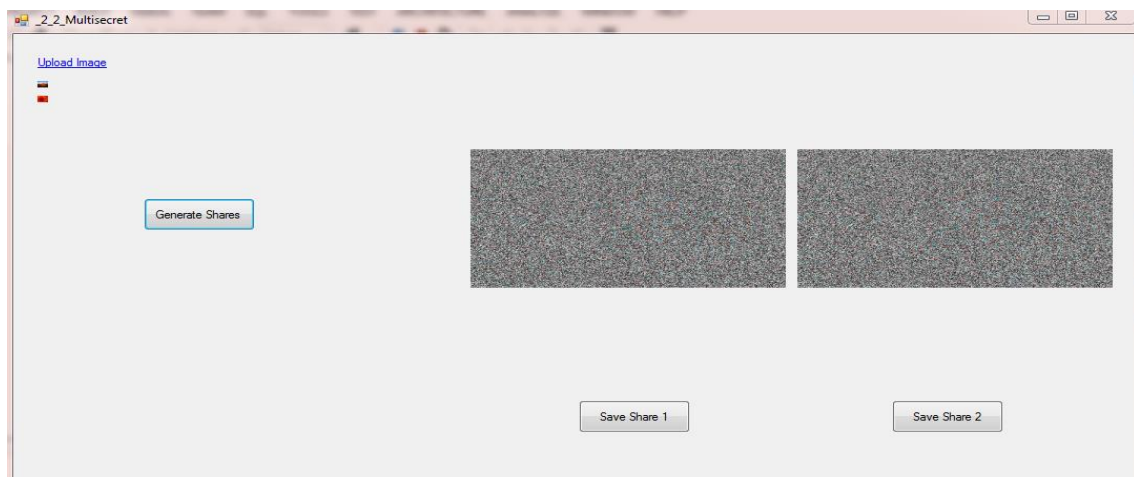


Figure 4.6 2 Secret (2,2) VCS Implementation Part 1

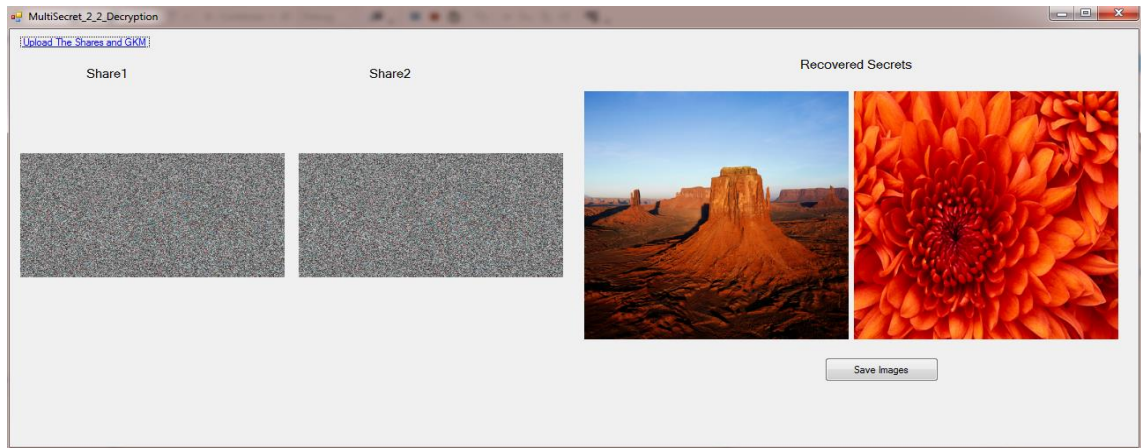






Figure 4.7 2 Secret (2,2) VCS Implementation Part 2

Now, we observe the results of the methodology proposed in section 3.2. Two secrets are hidden using 2 shares. Both shares are needed to reconstruct the original two secrets.

In the tabular data shown below, we see the execution results of the algorithm when tested with different images.

Table 4.4 Algorithm 3.2 Results for various images

Secret Images Used	Share Generation Time + Share Reconstruction Time	Input File Size + Output File Size
	0.758 seconds 0.676 seconds	4.02 MB 2.48 MB
	0.539 seconds 0.490 seconds	1.00 MB 2.48 MB

	<p>0.705 seconds 0.669 seconds</p>	<p>1.00 MB 2.48 MB</p>
	<p>0.713 seconds 0.666 seconds</p>	<p>760 KB 2.48 MB</p>

We can summarize from the above results the following observations:-

- i) Algorithm executes decently where share generation and share reconstruction speeds is less than 1 second
- ii) Output size of the algorithm is fixed irrespective of size and dimensions of the input images.
- iii) Share sizes vary in between 0.95MB to 1.05 MB whereas size of global key matrix remains fixed at 550 KB.
- iv) Share sizes may appear larger sized than individual secret images but one share is containing 2 images information, hence it is even not that larger.

4.4 Results of Three Secret (2,2) Color Visual Cryptography

This section first demonstrates the overall workflow of the algorithm. The first two images shown below display that how the algorithm executes. After these two images, we see the performance of the algorithm for various images.

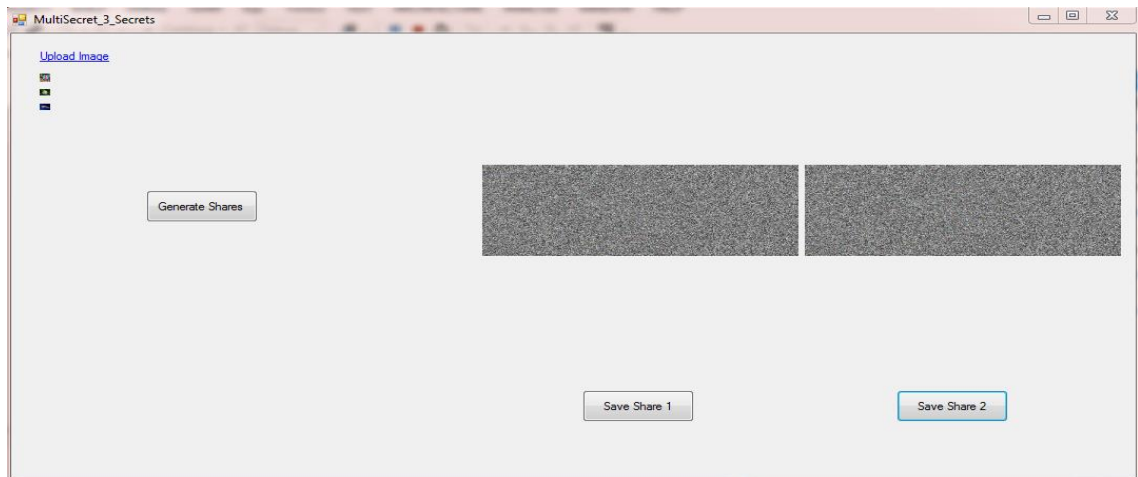


Figure 4.8 3 Secret (2,2) VCS Implementation Part 1

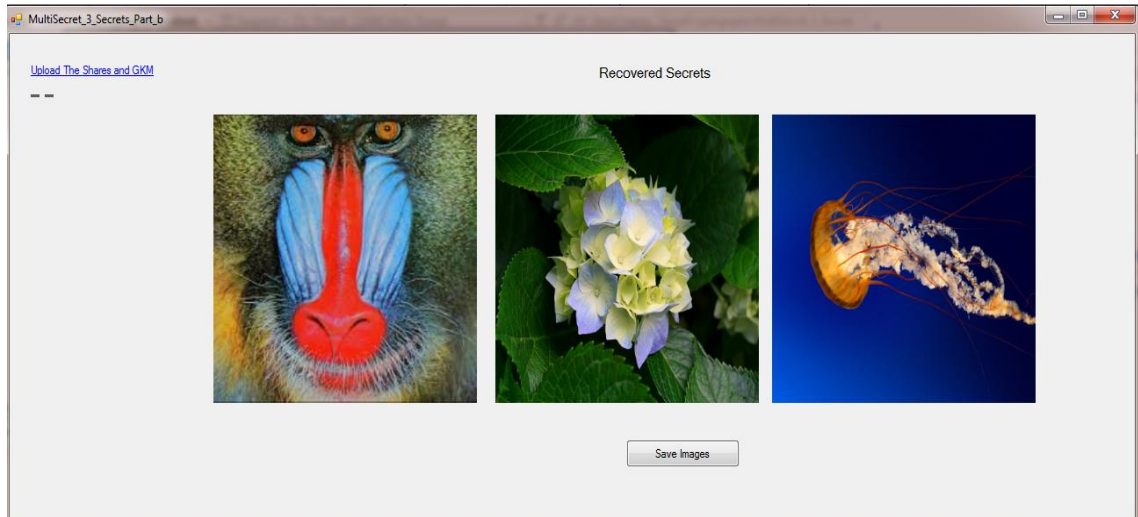

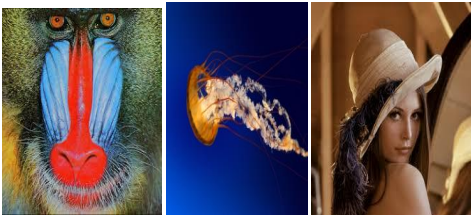




Figure 4.9 3 Secret (2,2) VCS Implementation Part 2

Now, we observe the results of the methodology proposed in section 3.3. Two secrets are hidden using 2 shares. Both shares are needed to reconstruct the original two secrets.

In the tabular data shown below, we see the execution results of the algorithm when tested with different images.

Table 4.5 Algorithm 3.3 Results for various images

Secret Images Used	Share Generation Time + Share Reconstruction Time	Input File Size + Output File Size
	0.921 seconds 0.748 seconds	4.01 MB 3.48 MB
	1.30 seconds 1.27 seconds	1.26 MB 3.48 MB
	1.18 seconds 0.805 seconds	1.76 MB 3.48 MB
	1.20 seconds 1.02 seconds	1.50 MB 3.48 MB

We can summarize from the above results the following observations:-

- i) Algorithm executes decently where share generation and share reconstruction speeds are less than 1.5 seconds

ii) Output size of the algorithm is fixed irrespective of size and dimensions of the input images.

iii) Share sizes vary in between 1.45 to 1.60 MB whereas size of global key matrix remains fixed at 550 KB.

iv) Share sizes may appear larger sized than individual secret images but one share is containing 3 images information, hence it is even not that larger.

4.5 Results of new k out of n Color Visual Cryptography

This section demonstrates the overall the results of the methodology proposed in section 3.4. Secret is hidden using n shares. A minimum of k shares are needed to reconstruct the original secret. In the tabular data shown below, we see the execution results of the algorithm when tested with different images.

The first two images below show the overall workflow and project screens for the implementation of algorithm proposed in section 3.4.

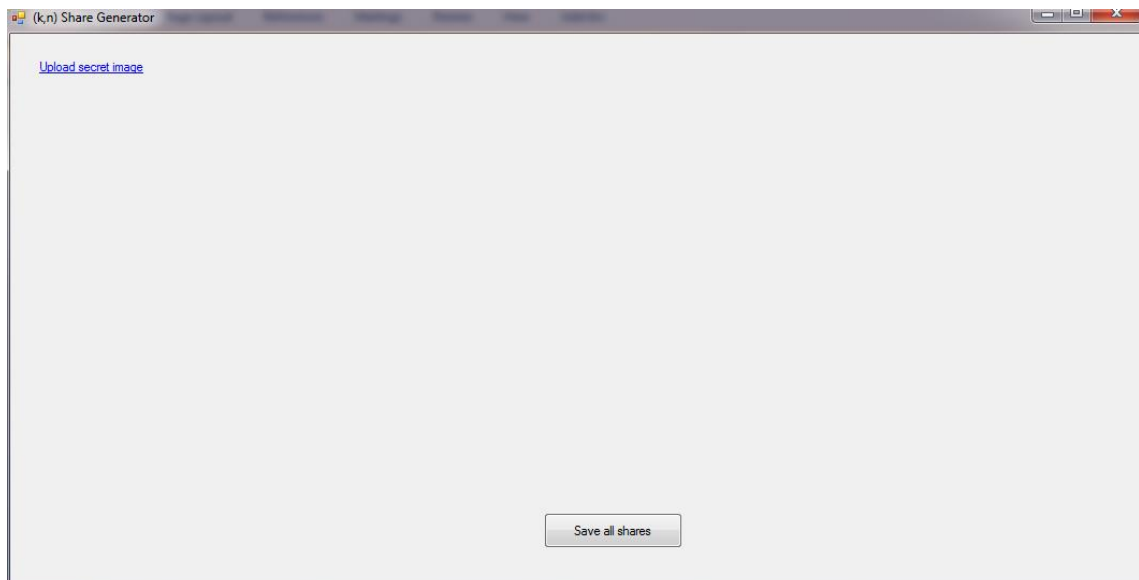


Figure 4.10 (k,n) VCS Implementation Part 1

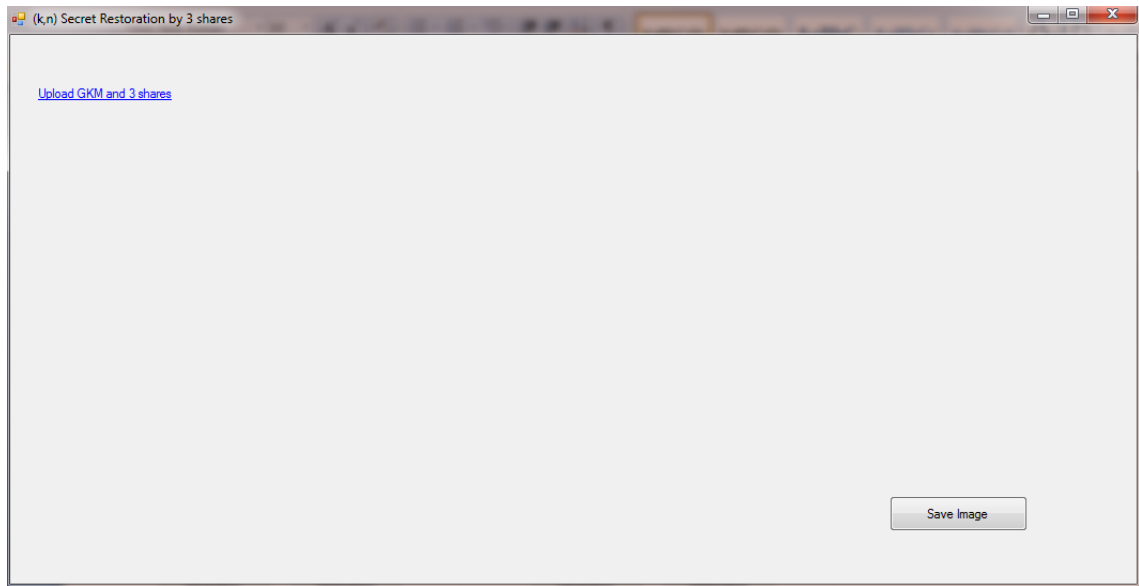

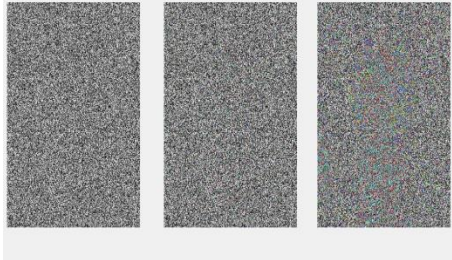
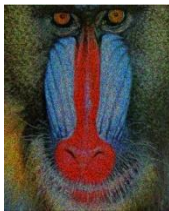
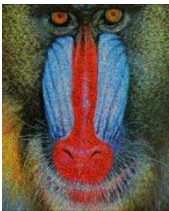

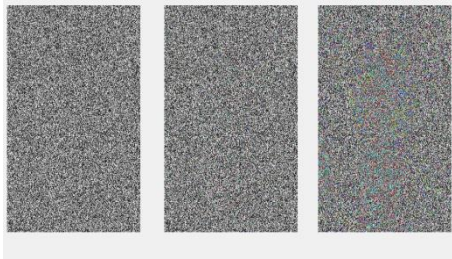


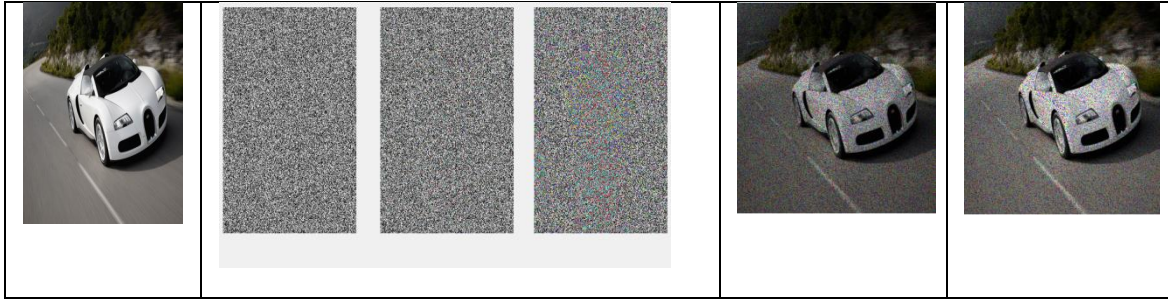


Figure 4.11 (k,n) VCS Implementation Part 2

Table 4.6 Algorithm 3.4 Results for various images

Secret Image	Generated shares	Recovery using k shares	Recovery using n shares
			
			



From the results, it is clear that whenever secret is obtained by k shares, then the quality of recovered secret is not up to the mark. But whenever we use all the n shares, we get the quality exactly the same as that of original image. Hence, proposed (k,n) visual cryptography scheme works correctly as also shown in the literature.

CHAPTER 5 CONCLUSIONS AND FUTURE SCOPE

From the results seen in Chapter 5, it is worth noting that (2,2) Color Visual Cryptography scheme performs better when used with the stream ciphers or lightweight cryptographic algorithms . There is an improvement in the algorithm performance considering, both the time as well as space requirements. Lightweight algorithms provide a 15 % improvement in speeds and 100 % improvement in storage required.

The secure and efficient method of (2,2) Color Visual cryptography with focus on especially the stream ciphers and lightweight cryptographic algorithms can be used with any other algorithms , but more importantly it demonstrated a new method of securing the shares. The method is also unaffected by any hacking attempt as, a combination of two random keys that are used within the approach. Also, these keys are mixed with the image data, as a result of which it becomes extremely complex to segregate the data and key.

We also saw from Chapter 5, new methods for (2,2) Color Visual Cryptography. These methods are designed to provide the capability to hide 2 and 3 secrets within 2 shares. Images or secrets are interleaved one by one and stacked into 1 share. The algorithm performed at fairly decent speeds. This method can even be extended to support the capability of the algorithm to hide secrets greater than or equal to 4 secrets.

Lastly, we saw a modified method for k out of n color visual cryptography scheme. The shares are generated based on random numbering in ascending order and then weights adjustments.

APPENDICES

A1. Code used for Interleaved Share Creation of 2 Secret (2,2) VCS

Outer loop for $y = 0$ to $y < 800$

```
{
    Inner loop for  $x = 0$  to  $x < 400$ 
    {
        Check if  $y$  is even
        {
             $\text{int } t = (y / 2);$ 
            Add components RX11, GX11, BX11 to share1 at location  $(y,x)$ 
        }
        Else check if  $y$  is odd
        {
             $\text{int } t = (y - 1);$ 
             $t = t / 2;$ 
            Add components RX21, GX21, BX21 to share1 at location  $(y,x)$ 
        }
    }
}
```

Outer loop for $y = 0$ to $y < 800$

```
{
    Inner loop for  $x = 0$  to  $x < 400$ 
    {
        Check if  $y$  is even
        {
             $\text{int } t = (y / 2);$ 
            Add components RX12, GX12, BX12 to share2 at location  $(y,x)$ 
        }
    }
}
```

```

Else check if y is odd
{
    int t = (y - 1);
    t = t / 2;
    Add components RX22, GX22, BX22 to share2 at location (y,x)
}
}
}

```

A2. Code used for Interleaved Share Creation of 3 Secret (2,2) VCS

Outer loop for y = 0 to y < 1200

```

{
    Inner loop for x = 0 to x < 400
    {
        Check if when y divided by 3 leaves 0 remainder
        {
            int t = (y / 3);
            Add components RX11, GX11, BX11 to share1 at location (y,x)
        }
        Else check if when y divided by 3 leaves 1 remainder
        {
            int t = (y - 1);
            t = t / 3;
            Add components RX21, GX21, BX21 to share1 at location (y,x)
        }
        Else check if when y divided by 3 leaves 2 as remainder
        {
            int t = (y - 2);
            t = t / 3;

```

```
        Add components RX31, GX31, BX31 to share1 at location (y,x)
    }

}

}
```

Outer loop for $y = 0$ to $y < 1200$

```
{
    Inner loop for  $x = 0$  to  $x < 400$ 
    {
        Check if when  $y$  divided by 3 leaves remainder 0
        {
            int t = (y / 3);
            Add components R12, GX12, BX12 to share2 at location (y,x)
        }

        Else check if when  $y$  divided by 3 leaves remainder 1
        {
            int t = (y - 1);
            t = t / 3;
            Add components RX22, GX22, BX22 to share2 at location (y,x)
        }

        Else check if when  $y$  divided by 3 leaves remainder 2
        {
            int t = (y - 2);
            t = t / 3;
            Add components RX32, GX32, BX32 to share2 at location (y,x)
        }
    }
}
```

REFERENCES

- [1] M. Noar and A. Shamir. ,”Visual cryptography.”, *Advances in Cryptology - Eurocrypt '94*,950:1–12, 1994.
- [2] Jonathan Weir and WeiQi Yan , “Visual Cryptography and Its Applications “,Ventus Publishing ApS , ISBN 978-87-403-0126-7
- [3] Ryo Ito, Hidenoir Kuwakado, and Hatsukazu Tanaka.” Image size invariant visual cryptography”. *IEICE Transactions*, E82-A(10):2172 – 2177, October 1999..
- [4] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. “Extended schemes for visual cryptography” *Theoretical Computer Science IEEE J. Quantum Electron.*, *submitted for publication.*
- [5] C.C. Wu and L.H. Chen. “A study on visual cryptography” Master's thesis, *Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C.*, 1998.
- [6] Duo Jin, Weiqi Yan, Mohan S. Kankanhalli , “Progressive color visual cryptography “, July 2005 *J. of Electronic Imaging*, 14(3), 033019 (2005).
- [7] E.R. Verheul and. van Tilborg, “Constructions and Properties of k out of n Visual Secret Sharing Schemes Designs”, *Codes and Cryptography*, Vol. 22(No. 2, pp. 179-196) 1997.
- [8] C. N. Yang and C. S. Laih, “New colored visual secret sharing schemes Designs”, *Codes and Cryptography*, Vol. 20, No. 3, pp. 325-335, 2000.
- [9] C.Chang, C. Tsai, and T. Chen. “A New Scheme For Sharing Secret Color Images In Computer Network”, *Proceedings of International Conference on Parallel and Distributed Systems*, pp. 21– 27,July 2000

- [10] Chin-Chen Chang, Tai-Xing Yu, “Sharing A Secret Gray Image In Multiple Images”, Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.
- [11] Young-Chang Hou ,”Visual cryptography for color images “,*Pattern Recognition*, Vol. 36, pp. 1619-1629, 2003.
- [12] Hwa-Chiug Hsu , Tung-Shou Chen, Yu-HsuanLin,The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing , in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004
- [13] R. Lukac, K.N. Plataniotis, “Bit-Level Based Secret Sharing For Image Encryption”, *Pattern Recognition* 38 (5), pp. 767–772, 2005.
- [14] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, “Sharing A Secret Two -Tone Image In Two Gray-Level Images” , *Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, 2005.
- [15] H.-C.Wu , C-C.Chang ,Sharing Visual Multi Secrets Using Circles Shares ,*Computer Stand Interfaces* 134 (28),pp 123–135,(2005).N. Kawasaki, “Parametric study of thermal and chemical non equilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.
- [16] S.J Shyu , “Efficient Visual Secret Sharing Scheme For Color Images “, *Pattern Recognition* , pp. 866–880, *2006IEEE Criteria for Class IE Electric Systems*
- [17] R.Youmaran, A. Adler, A.Miri, “An Improved Visual Cryptography Scheme For Secret Hiding”, 23rd Biennial Symposium on Communications, pp. 340-343, 2006.

- [18] LiguO Fang, Bin Yu, “Research On Pixel Expansion Of (2,n) Visual Threshold Scheme”, 1st International Symposium on Pervasive Computing and Applications, pp.856-860, IEEE.
- [19] S.J.Shyu, S.Y.Huanga, Y.K.Lee, R.Z.Wang, and K.Chen, “Sharing multiple secrets in visual cryptography”, *Pattern Recognition*, Vol.40, Issue 12, pp.3633-3651, 2007.
- [20] Wen-Pinn Fang, “Visual Cryptography In Reversible Style”, *IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IHMSP2007)*, Kaohsiung, Taiwan, R.O.C,2007.
- [21] Jen-Bang Feng, Hsien-ChuWu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, “Visual Secret Sharing For Multiple Secrets”, *Pattern Recognition* 41, pp.3572–3581, 2008.
- [22] Mustafa Ulutas, Rifat Yazıcı, VasifV. Nabiyev, Güzin Ulutas, (2,2)- “Secret Sharing Scheme With Improved Share Randomness”,978-1-4244-2881-6/08,*IEEE*,2008.
- [23] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multiple-Image Encryption By Rotating Random Grids”, *Eighth International Conference on Intelligent Systems Design and Applications*, pp. 252-256,2008.
- [24] Tzung-HerChen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multi-Secrets Visual Secret Sharing”, *Proceedings of APCC2008, IEICE*, 2008.
- [25] Mohsen Heidarinejad, Amirhossein AlamdarYazdi and Konstantinos N, Plataniotis “Algebraic Visual Cryptography Scheme For Color Images”,*ICASSP*, pp.1761-1764, 2008.
- [26] F. Liu, C.K. Wu X.J. Lin, “Colour Visual Cryptography Schemes”, *IET Information Security*, vol. 2,No. 4, pp 151-165, 2008.

- [27] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang, “Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size”, 2008.
- [28] Jonathan Weir, Wei Qi Yan, “Sharing Multiple Secrets Using Visual Cryptography”, 978-1- 4244-3828-0/09, *IEEE*, pp509-512, 2009.
- [29] Wei Qiao, Hongdong Yin, Huaqing Liang, “A kind Of Visual Cryptography Scheme For Color Images Based On Halftone Technique”, *International Conference on Measuring Technology and Mechatronics Automation* 978-0-7695-3583-8/09, pp. 393-395, 2009.
- [30] Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-TeHuang, “A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint”, *Information Sciences* 179 3247–3254 Elsevier, 2009.
- [31] M. Arun Kumar , K. Jhon Singh , “NOVEL SECURE TECHNIQUE USING VISUAL CRYPTOGRAPHY AND ADVANCE AES FOR IMAGES” , *International Journal of Knowledge Management & e-Learning* ,Volume 3 , pp.29-34, 2011.
- [32] Kulvinder Kaur, Vineeta Khemchandani , “Securing Visual Cryptographic Shares using Public- Key Encryption “ , *Advance Computing Conference (IACC, IEEE 3rd International)* 2013.
- [33] K. Shankar , P. Eswaran , “Sharing a Secret Image with Encapsulated Shares in Visual Cryptography”, *Procedia Computer Science*, Volume 70, 2015, Pages 462-468
- [34] K, Shankar, P. Eswaran, “A new k out of n secret image sharing scheme in visual cryptography”, *10th International Conference on Intelligent Systems and Control (ISCO)* , 2016.

- [35] K. Shankar and P. Eswaran, "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique", *J CIRCUIT SYST COMP* 25, 1650138 (2016).
- [36] S. Haykin, "Digital Communications" , 2nd ed. *John Wiley and Sons*,1998
- [37] S. Benedetto and E. Biglieri, "Principles of Digital Transmission: With Wireless Applications", 2nd ed. *Springer International Publishing*, 2008.
- [38] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography". 3rd ed. CRC Press, 1997.
- [39] D. Kahn, "The Code breakers: The story of secret writing." 2nd ed. *Scribners* 1996.
- [40] O. Goldreich, "Foundations of Cryptography: Basic Techniques", 1st ed. *Cambridge University Press*, 2004.
- [41] FIPS-180-4, "Secure Hash Standard," *National Institute of Standards and Technology*, Mar.2012.

LIST OF PUBLICATIONS

- 1.) Rajat Bhatnagar, Manoj Kumar, “Visual Cryptography: A Literature Survey”, 2nd International Conference on Communications and Aerospace Engineering (ICECA), IEEE ICECA 2018