

# CHAPTER 1

## **Chapter 1**

# **INTRODUCTION**

In today's fast developing era, security plays a very important role in the daily life. Today, more and more digital documents are transmitted and exchanged on internet. It has created an environment that the digital information is easy to distribute, duplicate and modify. Image security becomes a very important issue for image transmission over the internet or wireless network. Security has become the important features in communication and other text information, this is because of the presence of hackers who wait for a chance to gain an access to private data. Multimedia data (images, videos, audios and text) are of importance for use more widely. The most important point in that, the computer performed this cryptographic function, and from this point of view the process become a more secure and faster.

## **1.1 BIOMETRICS**

Biometrics is defined as the science of establishing the identity of an individual based on physical or behavioural characteristics to authenticate identity of person. There are various applications where personal identification is required such as computer login control, secure electronic banking, border crossing, airport, mobile phones etc. [1]. A biometric authentication system operates by acquiring raw biometric data from a subject, extracting a feature set from the data and comparing the feature set against the templates stored in a database in order to identify a person or to verify a claimed identity. Many biometric techniques are available such as fingerprint, face, iris, retina, palm print, hand vein, facial thermogram, keystroke, voice, hand geometry and signature etc. One of the main advantages of using biometrics as an entry mechanism is that it does not require memorizing complicated tokens or passwords. Fig. 1.1 refers to the biometric component in biometrics. Authentication in these systems refers to the automated recognition of individuals based on their behavioral and biological characteristics [3].

The template data in the database is generated during enrolment and is often stored along with the original raw data. In some instances, this data may have to be transmitted across a network. This has heightened the need to accord privacy to the subject by adequately protecting the contents of the database [3].

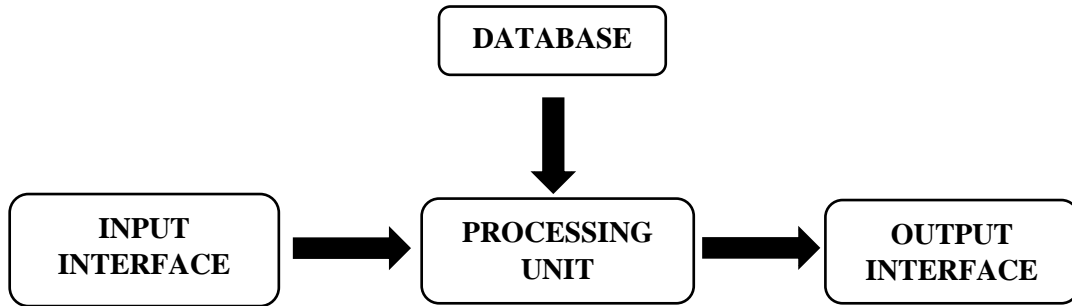


Fig. 1.1: Biometric Component

Fig. 1.2 refers to the eight types of attacks on biometrics system:

1. Involves presenting fake biometric.
2. Replay attack.
3. Feature extractor module is replaced with a Trojan horse program.
4. Genuine feature values are replaced with values selected by attacker.
5. The matcher is replaced with Trojan horse.
6. Template database attack.
7. Templates are replaced or altered in transition medium between template and database.
8. The matcher result can be overridden by attacker [1].

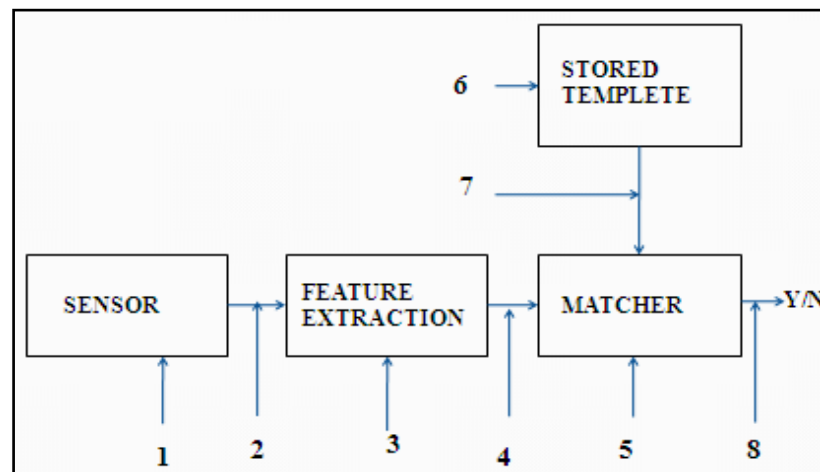


Fig. 1.2: Possible attack points in generic biometric system

One of the best techniques for the security of images or text is “Visual Cryptography” (VC). Visual cryptography will provide extra layer of authentication to the users. In Extended Visual Cryptography (EVC), the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating VC and biometric

security techniques. Initially, this technique was developed for black and white images but later on same was extended for colour images as well. The encrypted image is a noise image so that no one can obtain the secret image without knowing a decryption original image into another form that is difficult to understand [2].

## **1.2 APPLICATIONS OF BIOMETRIC SYSTEMS**

1. They are commonly used for automated attendance of employees and students. The most common traits used in these systems are faces and fingerprints.
2. Organizations like the Federal Bureau of Investigations (FBI) and Interpol have been using biometrics for forensic investigations to allow examiners to cross-check identities of suspects for possible matches with stored templates.
3. Biometric authentication is widely used around the world for home access control, mobile phone access, vehicle access authentication, etc.
4. Biometrics in banking has increased exponentially in recent years. Banks are implementing these technologies to increase security in transactions and reduce the chances of frauds. This would increase the convenience of customers [3].

## **1.3 CHALLENGES IN BIOMETRICS**

For biometric systems to be efficient, the similarity between various inputs from one individual must be high, and it should be low between inputs taken from different individuals. Most of the research in the field of biometrics is centered on two main problems:

- i. To find the best representation scheme for a particular trait. The feature extractor must be capable of minimizing intra-subject variations.
- ii. To design robust algorithms for feature extraction is another major challenge in biometric systems. Matching algorithms should be chosen based on the characteristics of various traits.

Some of the commonly used traits for biometric authentication are shown in Fig. 1.3. [3].

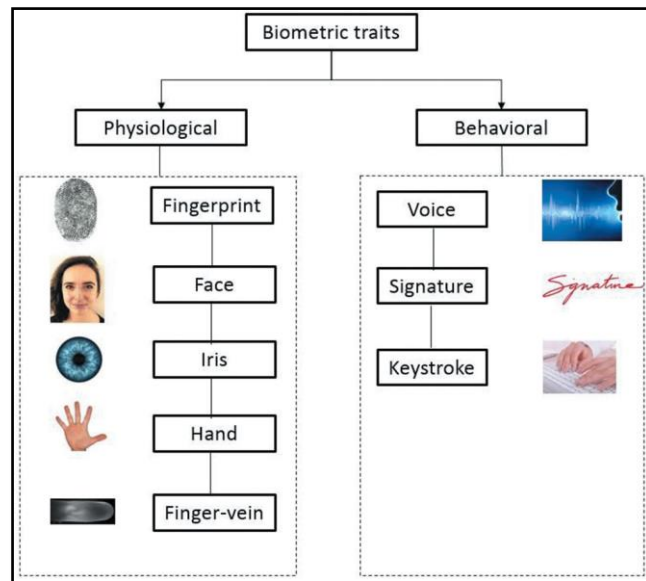


Fig. 1.3: Commonly used traits for biometric authentication

## 1.4 CRYPTOGRAPHIC TECHNIQUES

Encryption algorithms are classified in two broad categories- Symmetric key Cryptography and Asymmetric Key Cryptography.

### 1. Symmetric Key Cryptography

In symmetric Cryptography the key that is used for encryption is similar to the key used in decryption. So, the key distribution has to be made prior to the transmission of information.

### 2. Asymmetric Key Cryptography

In Asymmetric Cryptography, two different keys are used for encryption and decryption they are public and private. The public key is available to anyone on the network; those who want to encrypt the plaintext should know the Public Key of receiver. Only the authorized person can decrypt the cipher text through his/her own private key. Private Key is kept secret from the others. Symmetric Encryption Algorithm is faster as compared to Asymmetric key algorithms. The memory requirement of Symmetric algorithm is less than asymmetric [19].

### 1.4.1 KEYLESS ENCRYPTION

Image encryption can be carried out using:

- Image encryption using secret keys

Using encryption keys is a traditional method of image encryption can be carried out using DES, AES algorithms, digital signatures, vector quantisation, chaos theory etc. In some cases, secret key used for encryption is restricted and may have some limitations. It is inapt due bulk size of data. Also, it requires heavy computational cost. In contrast to this technique image encryption without using key provides more security as there is no need to maintain secret key, involves low encryption/decryption cost.

- **Keyless Image Encryption**

Encryption technique without using secret key includes generation of random shares; this technique is known as Visual Cryptography (VC). VC is a process where the secret image is encrypted into shares which refuse to provide information about the original secret image. The strength of this method is that the decryption of the secret image is through human visual system without computation. Thus, the proposed approach gives a secure novel technique for reversible data hiding using VC. With the scheme using secret keys have limitations regarding key management. In some cases, the available secret keys for encryption are limited and have some restricted space, also high computation involved in encryption. All these factors highlight the problem domain for using traditional encryption techniques in reversible data hiding. In converse to this approach is VC that involves no use of keys for encryption. Thus, the computations required are also less [30].

## **1.5 VISUAL CRYPTOGRAPHY**

One of the best-known techniques to protect data such as biometric templates is Cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver as shown in Fig. 1.4. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the Visual Cryptography Scheme (VCS) as a simple and secure way to allow the secret sharing of images, based on black and white or binary images without any cryptographic computations. We utilize this scheme in our approach [8].

In VC, an original image is encrypted into different images called as shares. VC is a paradigm in which a secret image is converted into two or more meaningless, non-identical shares, without using any encryption keys [4]. The hidden secret can be revealed only when the shares are stacked together. Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks [6]. If a

pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

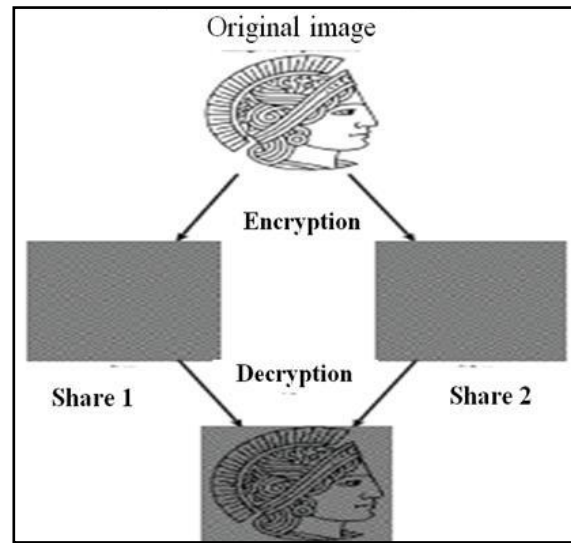


Fig. 1.4: Encryption & Decryption in VC

If a pixel in the secret image is white, then same pattern of sub-pixels is selected for both shares.

If a pixel in the secret image is black, then complementary pair of patterns of sub-pixels is selected for both shares [8] (Fig. 1.5).

Pixel	Probability	Shares #1 #2	Superposition of the two shares
<div style="border: 1px solid black; width: 30px; height: 30px; margin: 0 auto;"></div>	$p = 0.5$	<div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div>
	$p = 0.5$	<div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black;"></div>	
<div style="background-color: black; width: 30px; height: 30px; margin: 0 auto;"></div>	$p = 0.5$	<div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black;"></div>	<div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black;"></div>
	$p = 0.5$	<div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: black; border: 1px solid black; margin-right: 5px;"></div> <div style="display: inline-block; width: 15px; height: 15px; background-color: white; border: 1px solid black;"></div>	

Fig. 1.5: Pixel share illustration

VC takes in many formats such as for grayscale images, black and white images and for the color images. The proposed method is done for the color visual cryptography. In the Gray scale model, to ensure the transparencies the white pixels of black-and-white images as transparent. Typically, the black-and-white VC decomposes every pixel in a secret image into a  $2 \times 2$  block in the two transparencies according to the rules of the basic model. When a pixel is white, the method chooses one of the two combinations of white

pixels to form the content of the block in the two transparencies; when a pixel is black, it chooses one of the other two combinations. Therefore, when stacking two transparencies, the blocks corresponding to black pixels in the secret image are full black, and those corresponding to white pixels are half-black and half-white, which can be seen as 50% Gray pixels. The Gray-level images are transformed into halftone ones before printing, and the transformed Halftone images are black-and-white only; such an image format is very suitable for the traditional method to generate the shares of VC. For each black or white pixel in the halftone image, decompose it into a  $2 \times 2$  block of the two transparencies according to the rules. If the pixel is white, randomly select one combination from the former two rows as the content of the blocks in Shares 1 and 2. If the pixel is black, randomly select one combination from the latter two rows as the content of the blocks in the two transparencies. Repeat until every pixel in the halftone image is decomposed, hence resulting in two transparencies of VC to share the secret image [27].

VC is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. VC is a desirable scheme as it embodies both the scheme of perfect secrecy and a very simple mechanism for recovering the secret. VC provides robust security to the secret image. This makes VC suitable for highly sensitive applications like biometric authentication, secure electronic ballots, safe online banking, digital watermarking, security against attacks in authentication system etc [1].

### **1.5.1 VISUAL CRYPTOGRAPHY SCHEME MODEL**

VCS consists of Secret Image, Host Image, Pixel, Sheet, Target, Gray scaling. Whereas, Pixel is made up 4 components Alpha, Red, Blue and Green. VC can also be applied to color images by converting them into black and white binary images [5].

1. Secret image: The original image that has to be hidden.
2. Host Image: these are the face images used to encrypt the secret image using the EVCS.
3. Sheet: The secret image is encrypted into n sheet image which appear as random noise image or as a natural image.
4. Target: The image reconstructed by stacking or superimposing the sheets.
5. Pixel: It is the smallest element of an image. Each pixel corresponds to any one value. In an 8-bit grayscale image, the value of the pixel is between 0 to 255. The



value of a pixel at any point correspond to the intensity of the light photons striking at that point.

6. Gray Scaling: It is a process that uses gray shades to capture tone variation. This is usually applied to monochrome graphics and photos. It is a process of converting a continuous tone image to an image that a computer can manipulate [1].

### **1.5.2 TAXONOMY OF VISUAL CRYPTOGRAPHY**

1. Visual cryptography for binary image
2. Pixel-based visual cryptography
3. Extended visual cryptography.
4. Multiple image visual cryptography
5. Probabilistic visual cryptography
6. Bit-based/random grid-based visual cryptography
7. Visual cryptography for grayscale and color images:

For color images and Grayscale images, halftoning technique can be applied. Binary images can be encrypted into halftone images or shares in HVC. This method gives better visual quality (contrast) than other VCS.

8. Based on logical operation used during share recovery (OR- based and XOR-based):

The decryption process is very simple in VC. The shares are stacked or superimposed one on the other in order to reconstruct the secret from the share. Logical operations like 'OR' or 'XOR' operations can be utilized during recovery operation.

Based on this, the VC system is classified into OR-based VC and XOR-based VC.

OR - based VC:

The shares are superimposed to reconstruct the secret image again. This operation is equivalent to logical OR operation. The VCS using logical OR operation to recover the secret image are called OR-based VC.

XOR - based VC:

When numerous shares are superimposed, the reconstructed secret has a lower visual quality because the recovered image becomes darker. On the other hand, XOR-based VC is a significant branch of VC which can reconstruct the secret without darkening the background when more shares are utilized. XOR based VC system has good color, contrast and resolution properties compared to OR-based VC systems [8].

The VC techniques and taxonomy of VC is shown in Fig. 1.6 and 1.7 respectively.

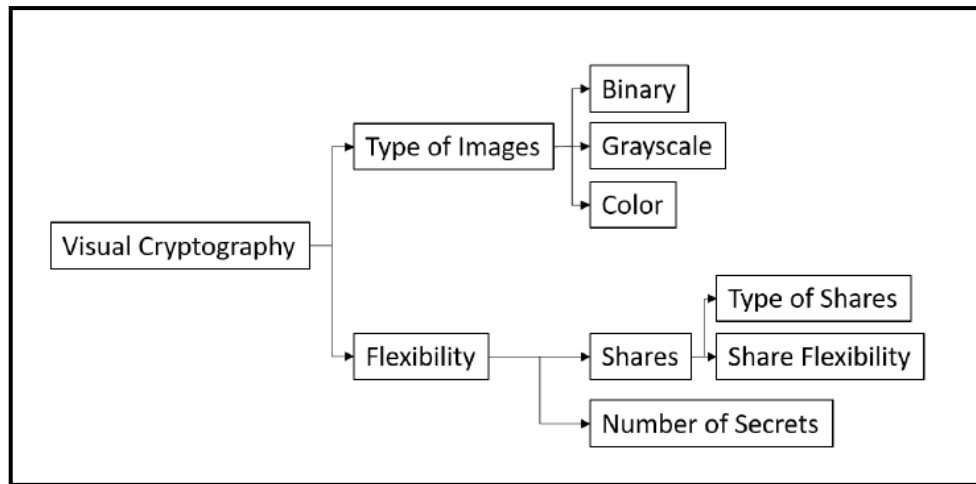


Fig. 1.6: VC techniques

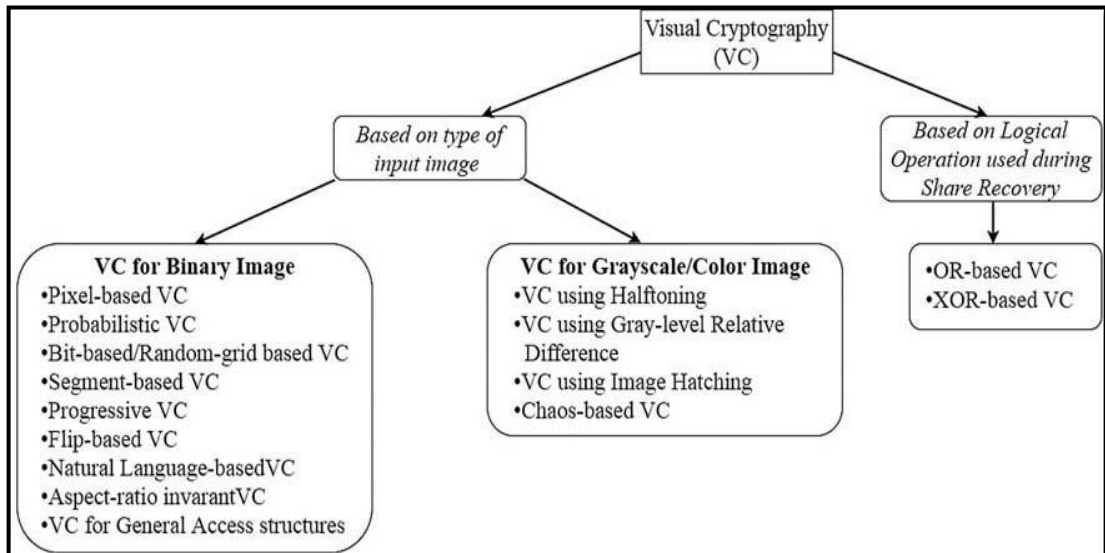


Fig. 1.7: Taxonomy of Visual Cryptography

### 1.5.2.1 XOR BASED VCS

In OR based  $(k, n)$ -VCS, the secret image can be recovered by stacking sufficient shares. Since the background of the reconstructed secret image becomes darkened when the shares are stacked together, the visual quality of the reconstructed image is less satisfactory. In order to obtain a better visual quality of the reconstructed image, XOR based VCS was proposed. It is important to notice that the secret image can be incompletely recovered by stacking  $k$  or more shares. Furthermore, if the secret is decoded by performing XOR operation, then the secret image can be reconstructed perfectly by  $n$  participants. In the following experiments, the binary secret images of size  $256 \times 256$  are used.

### **1.5.3 VISUAL CRYPTOGRAPHY METRICS**

These are some relevant metrics that are commonly used to evaluate or describe them.

1. **Pixel expansion:** It refers to number of sub-pixels  $m$  in generated shares that represent a single pixel in an original image. This parameter presents in loss of resolution from an original image to share image in VC procedure. When the shares are overlapped the recovered image will not be of the same quality of original image. The recovered image has less contrast and experiences a loss of resolution as compared to secret image. This parameter also reflects upon the size of the recovered image, which ideally should be as close as possible to the original secret.
2. **Contrast:** It is the relative difference between black and white pixels of a binary image or the difference in color tones in coloured images. It reflects upon the clarity or sharpness of a particular image. For VCS, the contrast of decrypted images is calculated as a measure of quality. In many cases, the VC encryption and decryption process leads to a loss in contrast.
3. **Security:** It refers to the amount of information about the secret image that can be extracted from share images. The recovered image should not be revealed with less than  $k-1$  shares in  $(k; n)$  schemes. The security parameter is generally satisfied when the strength of an encryption process prevents an intruder from extracting clues about the secret image.
4. **Complexity:** It can be divided into two types: computational and memory complexity. Computational complexity is concerned with the number of total operations (time) required to generate the set of shares  $n$ , and to reconstruct the secret image. Memory complexity refers to the amount of storage (memory) required for a VCS. Complex VC algorithms have higher computational and memory complexity, which then requires more powerful hardware to implement. This may render certain system unsuitable for fast-paced, real-time decisions. In theory, it is good to have a complex VC algorithm for optimal security but in practice, a complex algorithm may not be suitable for real-life applications that require minimal computational overhead.
5. **Accuracy:** The accuracy of a VC scheme measures the quality of a recovered image. Ideally, the recovered image should be an exact replica of the original secret image. The goal of any VCS is to maximize accuracy, which can be evaluated by PSNR, mean square error (MSE), and CC metrics.

Generally, an EVCS takes a secret image and original share images as input, and outputs shares that satisfy the following three conditions:

- 1) any qualified subset of shares can recover the secret image;
- 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image;
- 3) all the shares are meaningful images. [36]

#### **1.5.4 APPLICATIONS OF VISUAL CRYPTOGRAPHY**

1. Visual cryptography for Biometric Privacy
2. VC for security against DoS attacks in WiMAX authentication system
3. Safe online banking using VC
4. Secure electronic ballot using VC
5. Analysis in Frequency domain

#### **1.5.5 ADVANTAGES**

1. No Pixel Expansion The size of original image is as it is
2. High Level Security for biometric privacy
3. Prevent Attacks of biometric images
4. Secure Databases

### **1.6 HALFTONING PROCESS**

The color image owns three-channel (red channel, green channel and blue channel), and the range of every channel value is 0 to 255. It is A continuous tone image, and it cannot be shared by the proposed scheme directly. Therefore, the continuous tone image needs to be converted to the halftone image. The Floyd–Steinberg is used to convert the color image to the halftone image. The operation is that every channel of the continuous tone image is performed halftone by using Floyd–Steinberg. The continuous tone image is converted to the halftone image. This halftone image is the secret image H in this paper. H is a color image which is made up of eight colors R, G, B, C, M, Y, K, W. Halftone image can be decoded by HVS, and its information is the same as the continuous tone image from the perspective of HVS.

## 1.7 BLOWFISH ALGORITHM

Blowfish is a popular security algorithm that was planned in 1993 by Bruce Schneier and developed in the advent of the year 1994. He planned blowfish as a high-speed, free special to existing encryption algorithms. Blowfish is a symmetric encryption algorithm; it uses the same secret key to both encrypt and decrypt messages [6]. Blowfish is also a block cipher; it divides a message up into fixed length blocks during encryption and decryption. Blowfish is a cipher based on the Feistel rounds, and the plan of the function used amounts to an indication of the values used in DES to present the equal protection with better speed and efficiency in software. Blowfish is a 64-bit block cipher with a variable-length key and is possible as an alternate for the DES as shown in Fig. 1.8.

Blowfish became quite popular after its advent, the main reason for this was Bruce Schneier himself was one of the most famous cryptology experts and moreover his algorithm is non patented, open source freely and freely available for use and modifications. The Blowfish algorithm is secure next to illegal attacks and run quicker than the accepted presented algorithms [11].

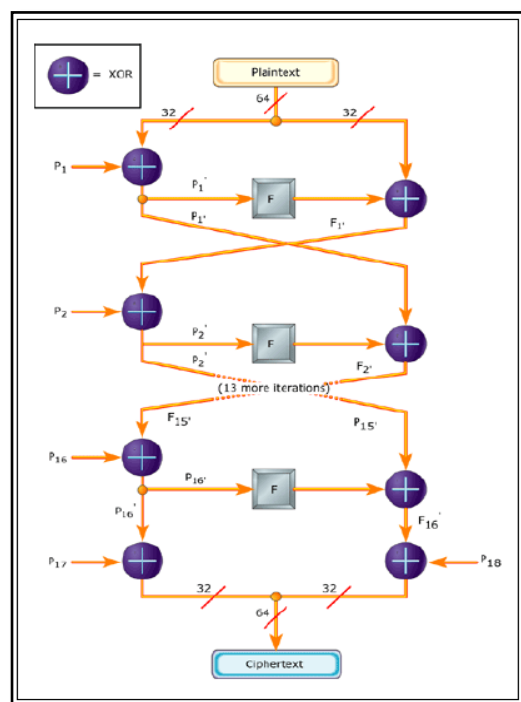


Fig. 1.8: Blowfish Algorithm

## 1.8 MULTIPLE IMAGE VISUAL CRYPTOGRAPHY

A multiple image visual cryptography is capable of hiding more than one secret within the shares. While recovering, the shares are superimposed on each other to reveal first secret. One of the shares is rotated to particular angle and then again superimposed

with another share to reveal the second secret. Another technique for securing multiple images is in order to increase the ease of rotation, the shares are circular in shape. Since these are extended versions of pixel-based visual cryptography, the pixel-expansion and contrast loss are still persistent in these techniques [28].

## 1.9 COLOR VISUAL CRYPTOGRAPHY

Nowadays, most people are used to color images to secure some type of image information [9]. Three methods for VC for Gray-scale and color images based on VC for binary image, the halftone techniques and the color decomposition method were proposed. These methods have similar advantages of VC for binary image. In the decryption phase, we can recover SI using HVS, and there is no need for computation.

Basic principles of color the additive (RGB model) and subtractive models (CMY model) are commonly used to describe the constitutions of colors as shown in Fig. 1.9. In color images, encryption and decryption is based on halftoning and inverse halftoning. In color images, image is divided into red, green, blue components and shares are generated by applying simple VCS on these components. Then at receiver side shares are superimposed to reveal secret image [36].

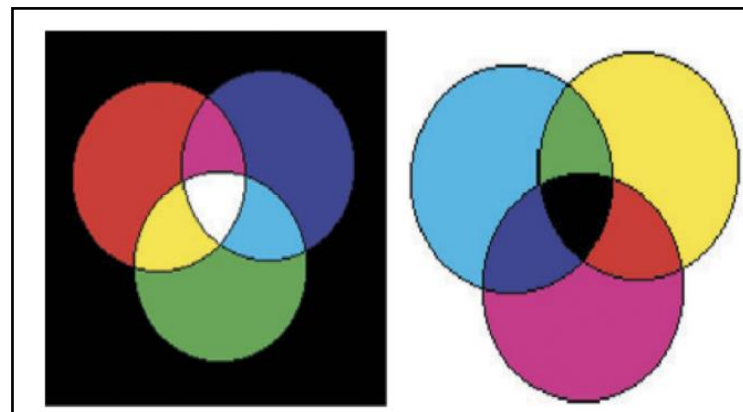


Fig.1.9: Additive Mode and Subtractive Model

There are three primary colors in the additive model. These are RGB. White color is obtained by mixing equal intensity of RGB components. The subtractive model is obtained by adding CMY components [28].

## 1.10 BALANCED BLOCK REPLACEMENT

Balanced Block Replacement (BBR) approach for pre-processing of halftone image refers to two black and two white pixels as candidate blocks. In this approach, they assign

some candidate block to white and others to black randomly, to balance black and white in the processed image. Thus, it improves contrast of the recovered SI. This approach keeps the local ratio of black to white pixels in the processed image close to the local ratio of black to white pixels in the original halftone image. Hence, the visual quality of the recovered SI is close to that of the original Gray-scale image [9].

## 1.11 FACE RECOGNITION

The face recognition algorithm is used in finding features that are uniquely described in the image. The facial image is already extracted, cropped, resized, and usually converted in the grayscale.

As we know a neural network takes an image of the face of the person as input and outputs a vector that represents the most important features of a face! In machine learning, this vector is nothing but called embedding and hence we call this vector face embedding. We have face embeddings for each face in our data saved in a file, the next step is to recognize a new image that is not in our data. Hence the first step is to compute the face embedding for the image using the same network we used earlier and then compare this embedding with the rest of the embeddings that we have. We recognize the face if the generated embedding is closer or similar to any other embedding as shown in Fig. 1.10 [31].

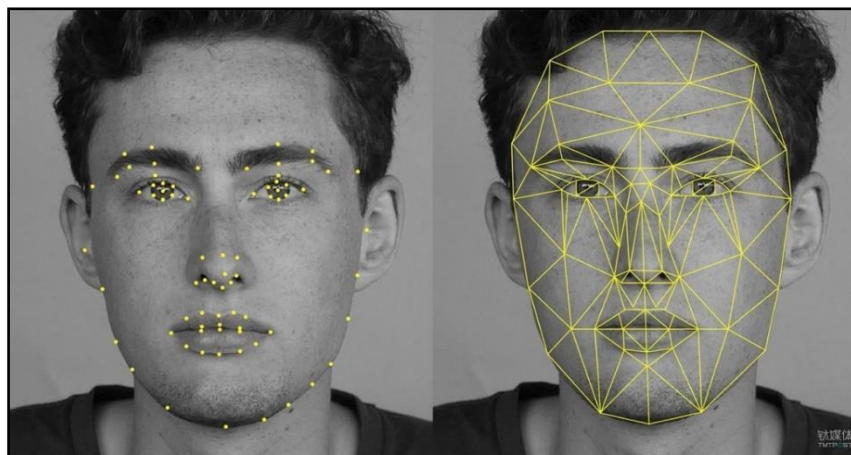


Fig. 1.10: Face Recognition

# **CHAPTER 2**



## **Chapter 2**

# **LITERATURE SURVEY**

A literature survey is that section which shows various analysis and research made in the field of our interest and results already published, taking into account of the various parameters and the extent of the project. It is the most important part of the report as it gives a direction in the area of research. It helps to set a goal for the analysis, thus giving the problem statement.

## **2.1 LITERATURE REVIEW**

Arun Ross, Asem Othman, “Visual Cryptography for Biometric Privacy”, IEEE Transactions on Information Forensics and Security, VOL.6 No.1, MARCH 2011 [1]. In the proposed scheme, a private face image is dithered into two host face images such that it can be revealed only when both host images are simultaneously available; at the same time, the individual host images do not reveal the identity of the original image.

Naor, M. and Shamir, A. (1995) “Visual Cryptography”, EUROCRYPT 1994, Lecture Notes in Computer Science, Vol. 950. Springer, Berlin, Heidelberg [2]. This conceived a new theory that lays as the groundwork for Visual Cryptography. The simplest version of this theory assumes that the message is a combination of 2 facets: Black pixels and White pixels, that message is distributed among  $n$  participants. The message is sliced up into  $n$  transparencies in such a way if  $k$  number of transparencies are stacked together, then the message becomes visible through HVS. But such a scheme is applicable on black and white images only and it also suffers from pixel expansion i.e., size of the recovered secret message is not same as of the original one.

Shefali Arora & M.P.S Bhatia, “Challenges and opportunities in biometric security: A survey”, Information Security Journal: A Global Perspective (2021) [3]. The main objective of this paper is to review the studies exploring the role of deep learning in the field of authentication using biometric systems, explore more such applications of deep learning, which hold a lot of potential in the field of biometrics to secure real-world applications. This paper summarizes these approaches and explore the challenges that continue to restrict the full potential of biometric systems.

Jeng-Shyang Pan, Tao Liu, Hong-Mei Yang, Bin Yan, Shu-Chuan Chu, Tongtong Zhu, “Visual cryptography scheme for secret colour images with colour QR codes”, Elsevier November 2021 [4]. This paper proposes two new schemes by using color XOR to solve problems of restoring the secret color image and generate meaningful shares. Visual cryptography scheme can divide the secret image into several shares. It can be used to enhance the secure transmission of the secret image on the Internet.

Yongkang Zhao, Fang-Wei Fu, “A contrast improved OR and XOR based  $(k, n)$  visual cryptography scheme without pixel expansion”, 20 December 2021, Published by Elsevier B.V [5]. This paper develops a novel contrast improved OR and XOR based  $(k, n)$ -VCS without pixel expansion. Significantly, it gives a general simplified calculation formula to compute the theoretical contrast of the proposed scheme. In addition, if there are no computing devices, then we can reconstruct the secret image by stacking the shares directly. Meanwhile, the recovering of the secret image perfectly by performing XOR operation when computing devices are available. Since the proposed scheme is based on the parity basis matrices, our scheme has no pixel expansion.

Jyoti Tripathi, Anu Saini, Kishan, Nikhil, Shazad, “Enhanced Visual Cryptography: An Augmented Model for Image Security”, (ICCIDS 2019), Published by Elsevier B.V [6]. This paper consists of the encryption techniques proposed in without pixel expansion and with a shared key concept. These methods require no overhead and less time for computation during the decryption process. The secret share is encrypted by dividing it two 3 shares depending on scheme imposed. Using 2-out-of-3 scheme for transmission will certainly reduce the time required to decrypt the image for recipient. The shares are generated using a key and are recovered using the same key. The results in this paper suggests fact that security of the scheme critically depends on a shared key and the sum of shares required for regeneration of the secret image.

M. Karolin and T. Meyyappan, “Secret Multiple Share Creation with Color Images using Visual Cryptography”, International Conference on Communication and Signal Processing, April 4-6, 2019, India, IEEE [7]. In this method RGB image, shares encrypted and decrypted to stacked image and then same as the original image. RGB color image is full for the information distribution. The testing results of the proposed system are compared to the share generation technique. Encryption and decryption are done by Blowfish Algorithm.

M. Karolin, T. Meyyappan, “Image Encryption and Decryption using RSA Algorithm with Share Creation Techniques”, ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019, IEEE [8]. In this paper, Visual cryptography secret share creation technique is used, original (RGB) color images and 2 shares are created and then those are encrypted and then decrypted. It is implemented with RSA algorithm and MATLAB coding. This results in better quality of RGB color images.

P. Punithavathi & S. Geetha (2017), “Visual cryptography: A brief survey”, Information Security Journal: A Global Perspective, 26:6, 305-317 [9]. In this paper, various visual cryptography techniques have been discussed. The metrics used to analyse the effectiveness of visual cryptography techniques have been briefed. The significant applications of visual cryptography have also been summarized in the survey. In this it suggests that during decryption phase, a user can perceive the recovered secret with their visual system, without the intervention of machines.

M. Karolin, Dr. T. Meyyappan, “RGB Based Secret Sharing Scheme in Color Visual Cryptography”, Vol. 4, Issue 7, July 2015 [10]. In this paper, the RGB color image is taken for the information sharing. The Floyd – Steinberg dithering algorithm is used to manipulate the 256-code image to low code image. The dithering algorithm is used instead of half toning the image.

Apurva A. Mohod, Prof. Komal B. Bijwe, “An Image Database Security Using Multilayer Multi Share Visual Cryptography: A Review”, ISSN 2319 -4847, Volume 3, Issue 10, October 2014 [11]. In this paper, we are using visual cryptography technique visual information is encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The visual secret sharing scheme divide the secret image into two or more images which are called shares. The secret image can be recovered in very simple way by stacking the shares together without any complex computation involved.

Neha Khatri Valmik, Prof. V. K Kshirsagar, “Blowfish Algorithm”, ISSN: 2278-8727, Volume 16, Issue 2, Ver. X (Mar-Apr. 2014) [12]. This paper suggests an algorithm i.e., blowfish Algorithm to encrypt the data file. This algorithm has been used because it requires less memory. Each round consists of XOR operation and a function. Each round consists of key expansion and data encryption. Blowfish can achieve efficient data

encryption. It is suitable for applications where the key doesn't change often, like a communications link.

Atul Sureshpant Akotkar, Chaitali Choudhary, "Secure of Face Authentication using Visual Cryptography", International Journal of Innovative Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-2, Issue-5, April 2014 [13]. In this paper, during encryption part actual image is decompose in to three shares this can be done for a greater number of share generation in future so that security will enhance. This paper implements VC for color images in a biometric application.

Shubhangi Rajanwar<sup>1</sup>, Shirish Kumbar<sup>2</sup>, Akshay Jadhav, "Visual Cryptography for Biometric Privacy", International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume 3 Issue 12, December 2014 [14]. This paper is to protect biometrics data from the various attacks by decomposing an input private image into two independent sheet images such that the private image can be reconstructed only when both sheets are simultaneously available. This selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. Increasing the pixel expansion factor can lead to an increase in the storage requirements for the sheets.

N. Askari, H.M. Heys, and C.R. Moloney, "An Extended Visual Cryptography Scheme Without Pixel Expansion for Halftone Images" [15]. In this paper, the proposed method for processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

Manika Sharma & Rekha Saraswat, (2013) "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2 [16]. This paper suggested a cryptography scheme to encrypt secret image by using the concept of RSA asymmetric key ciphering algorithm. The key generated will consist information about the number of shares and the information about the envelope images. Error diffusion using XOR technique is used for half toning. The quality of the original image depends on the quality of the channel images. The key has to be sent over the network in a secure manner so that it will not be accessible to the intruder.

Sozan Abdulla, “New Visual Cryptography Algorithm for Colored Image” Journal of Computing, 2010 [17]. In this paper, the visual cryptography scheme in which every single pixel of secret image is splitted into subpixels which can still be perceived as single pixel by HVS. Authors have used an input 24-bit bitmap color image which each 3-byte sequence in the bitmap array represents the relative intensities of red, green and blue respectively for image size 256x256 RGB pixel. Transparencies are generated by mixing the R, G and B component of an image with 3/4th pixel component of cover image through OR operation.

## **2.2 MOTIVATION**

Security of data has become a necessity in the present world. In present world, digital documents are transmitted and exchanged on internet. It has made digital information easy to distribute, duplicate and modify. Image security is a very important issue for image transmission over the internet or wireless network. The security is becoming more important as the volume of data being exchanged.

## **2.3 SCOPE OF THE PROJECT**

Security has become the important features in communication and other text information these is because of the presence of hackers who wait for a chance to gain an access to private data. Biometric template is stored in centralized database, due to security threats biometric template may be modified by attacker. Biometric templates are vulnerable to eavesdropping and attacks. If biometric template is altered by attacker, then authorized user will not be allowed to access the resource. So, VC technique has been applied on to the biometrics template to make it secure from attack in centralized database. VC will provide extra layer of authentication to the users.

## **2.4 EXISTING SYSTEM**

Cryptography is one of the most important techniques for protecting the data such as biometric templates. VCS is a cryptographic technique for the encryption of visual information such that the decryption process can be done by the human visual systems. Using this technique, the biometric data is captured from the authorized user. This original image is divided into the two cover images and, then each cover image is stored in two different databases geographically apart. When both the cover images are simultaneously available then only, we can access that original image.

### **2.4.1 DRAWBACKS OF THE EXISTING SYSTEM**

However, the investigations on the existing scheme with multiple decryptions are not sufficient. When we apply VC in the existing system, it requires more space for storing sheets due because of the pixel expansion. So, the size of the original image becomes larger instead of original size this is the disadvantage of the existing system and we are providing a solution for this, the pixel expansion occurs resulting in the increased size of original image. Pixel expansion refers to number of sub-pixels  $m$  in generated shares that represent a single pixel in an original image. This parameter presents in loss of resolution from an original image to share image in VC procedure.

## **2.5 PROBLEM STATEMENT**

When we transmit data (image) over the network, then any unauthenticated person can read it. So, in order to provide the security to data generally the sender will encrypt the data and then send it to the intended person and the receiver will decrypt that encrypted data and uses it. VC comes with the guarantee of the security by means of defining perfect secrecy. Mainly, retrieval of original information without losing the secret contents against the action of hackers in the network is a very challenging problem in today's world. The main objective of this study is to increase security in communication by encrypting the information using a key that is created through using an image.

# **CHAPTER 3**

## **Chapter 3**

# **DESIGN AND IMPLEMENTATION**

## **3.1 INTRODUCTION**

Biometrics can be used to determine a person's identity even without his knowledge or consent. There are two phases in a biometric system: registration (or enrolment) and recognition. The first step involves pre-processing and feature extraction. These features are stored as templates in the database. Hence, Visual Cryptography is used. VC is a secret sharing scheme that is used to share the secret image by dividing it into  $n$  noise-like secure shares which are meaningful, out of which any  $k$  shares are stacked together to recover the secret. Every image consists of Red, Blue & Green colours of 8 bit each. Each pixel is divided into three equivalent blocks R, G, B respectively.

## **3.2 METHODOLOGY**

This scheme divides true color image into R, G, B component. Two cover images are used to hide the bit planes using VCS. Using VCS on each bit level representation of cover images and secret images, meaningful shares are generated by combining corresponding share for each component.

Fig. 3.1 shown below gives a brief overview of the proposed system, where two cover images are used for the account access. Before that, the user needs to login with the username and password.

The proposed methodology has been divided into three phases, i.e., Image Encryption and Image Decryption and Face Matching.

There are many ways in which we can continue this process. VC can be divided on the basis of input images and logical operation during share recovery. Based on input images it can be divided as binary images and Gray-scale/color images and based on logical operation OR based and XOR based.

Here we use "Floyd Steinberg Dithering Algorithm" for Halftoning an input image and RANSAC algorithm for detecting the face edges.



The dithering algorithm is used instead of halftoning the image. By dithering for every share separate array is created and manipulated. For the secret image sharing and then stacking the decryption is involved. By using the proposed method, the intensity of the original image is maintained.

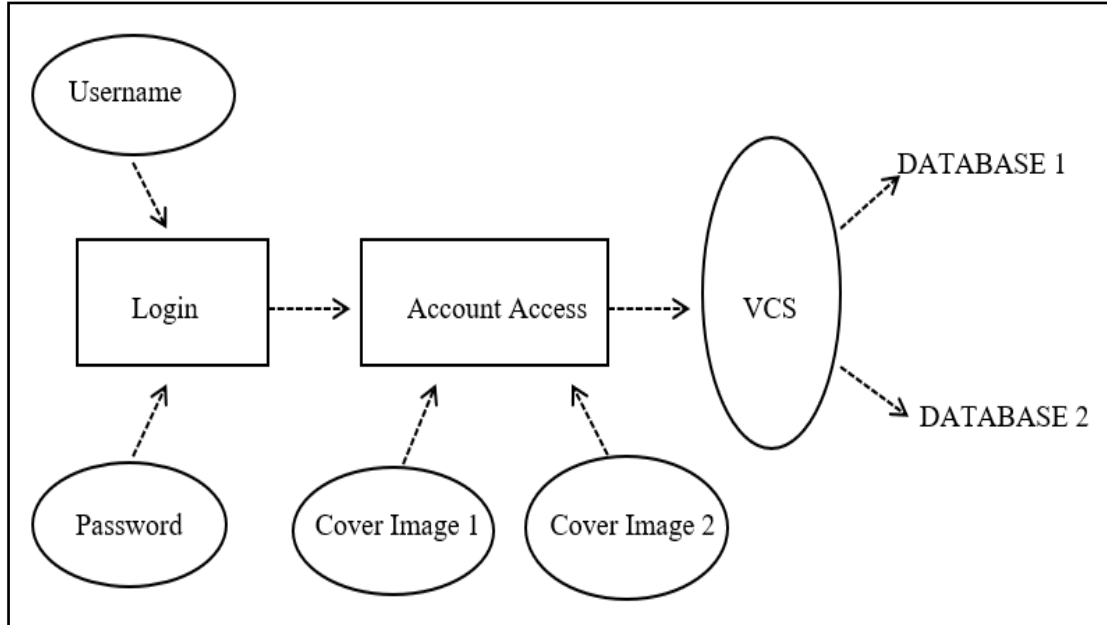


Fig. 3.1: Data Flow diagram for the Proposed System

Pixel consists of Alpha, Red, Green, Blue. This can be done by:

- a. Face Detection based on skin colour
  - b. RGB Share generation.
  - c. Share authentication
  - d. Image Retrieval from RGB Shares
- In this project, we use Visual Cryptography technique.
  - At first the image is added for the encryption process. Then it has four steps as shown in Fig. 3.4.

### 3.2.1 ENCRYPTION:

An encryption algorithm is the method used to transform data into ciphertext. An algorithm will use the encryption key in order to alter the data in a predictable way, so that even though the encrypted data will appear random, it can be turned back into plaintext by using the decryption key.

There are few encryption algorithms:

1. AES
  2. Triple DES
  3. Blowfish
  4. RSA
  5. Twofish
- Every image consists of three shares, RGB, hence each image is divided into three shares. This is known as Sieving. XOR- based VC method is used to generate shares.
  - These RGB shares are divided into two more shares each i.e., R1, R2, G1, G2, B1, B2 a total of six small shares. This is called Division.
  - Further these 6 shares are shuffled. This is Shuffling.
  - Then a random share is generated in order to form two different shares and saved, these are then shared to different people (users) or database. This is Combining.

The steps involved are shown in Fig. 3.2.

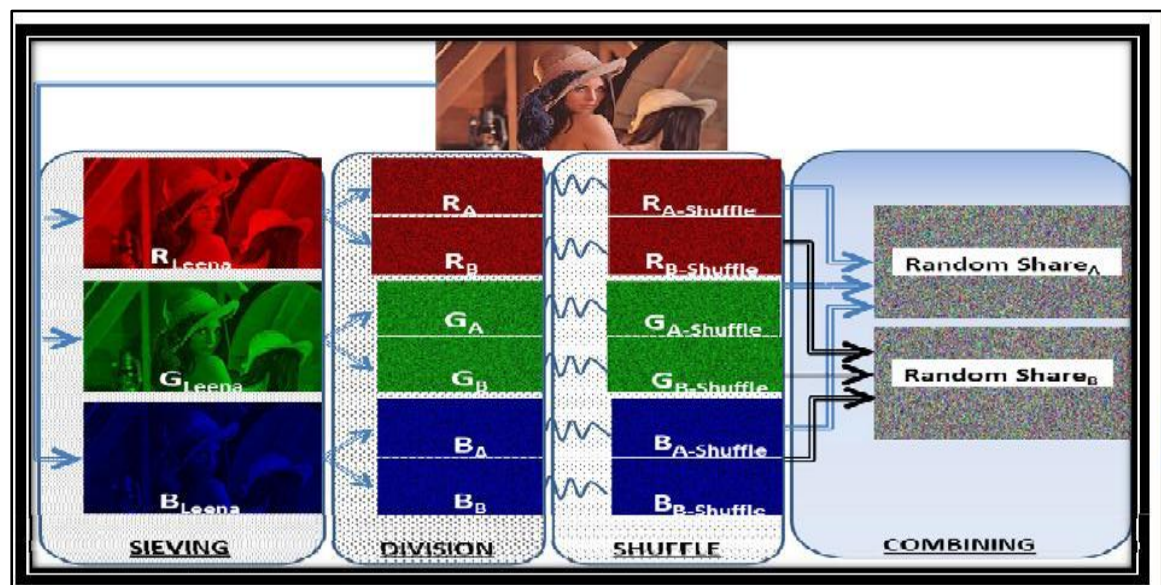


Fig. 3.2: Steps involved in generating 2 random shares

❖ XOR - based VCS:

In (2, 2)-VCS, a binary secret image is encrypted into two shares. The encryption rules are shown in Fig 3.3.











Secret Pixel	Probability	$S_1$	$S_2$	$S_1 \otimes S_2$
	$\frac{1}{2}$			
	$\frac{1}{2}$			
	$\frac{1}{2}$			
	$\frac{1}{2}$			

Fig. 3.3: Encryption rules

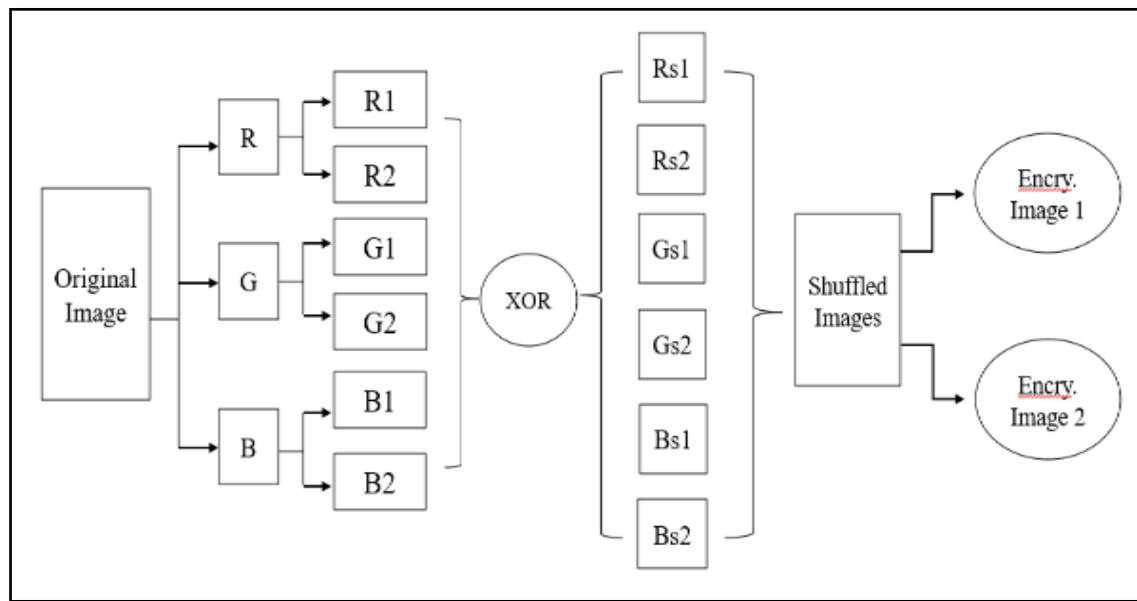


Fig. 3.4: Encryption Method

Each secret pixel  $S(i, j)$  in binary secret image  $S$  is encoded into a pair of black and white sub-pixel for two shares. The width of the reconstructed image is just twice as large as the original secret image, and the contrast loss can be noticed in the reconstructed image.

If the pixel of secret is white, we randomly select one of two encryption rules for white (resp. black) pixel. The secret pixel is encrypted into two sub-pixels with equal probability, such as black–white and white–black. After the reconstruction phase, the white pixel is decrypted to black–white or white–black with equal probability, and the black pixel is decrypted to black–black. Thus, we can reveal the secret image by stacking two shares together.

- After the encryption process is completed, these two generated shares are used for decryption process.

### 3.2.2 DECRYPTION:

Decryption is the process of converting unreadable ciphertext to readable information. Decryption operate by using the opposite conversion algorithm used to encode the information. The same key is needed to return the encrypted data to its initial state.

- The two randomly generated images are chosen to obtain the decrypted image i.e., the original image as shown is Fig. 3.5.

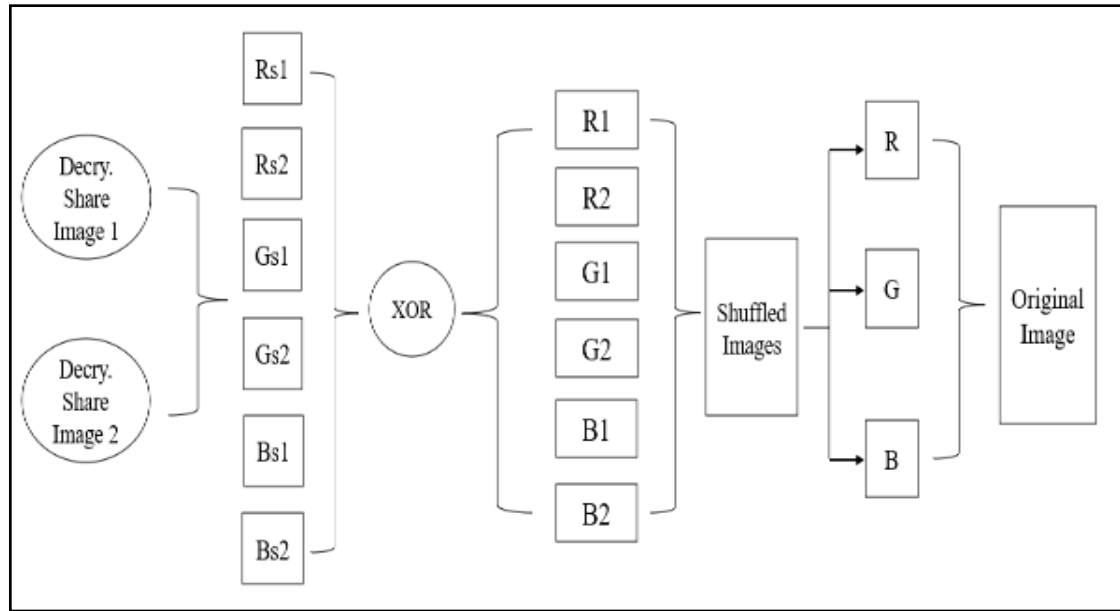


Fig. 3.5: Decryption Method

- Next process is face recognition, where it matches the original image with the decrypted image and checks for the similarity.

### 3.2.3 FACE MATCHING

- For this purpose, we use RANSAC method. It is used to detect the face edges which is helpful for the detection and face verification process.
- Using this method, the original and decrypted image is matched for accuracy.

## 3.3 IMPLEMENTATION

This part gives a brief of project requirements i.e., software and hardware requirements.

### 3.3.1 FULL – STACK DEVELOPMENT

Full stack refers to the development that makes up a website. It is composed of all the components necessary for the front-end and back-end of development as shown in Fig.

3.6. A full stack developer will have knowledge of the various roles that enable full stack web development. This would mean having a deep knowledge of client software and server software, including of course web frameworks that will ease the software development process.

For most software development projects, full stack development is a given. Front-end development would involve building a graphical user interface (UI).

This happens alongside back-end development which involves writing maintainable code, or the business logic, to make sure the application runs smoothly.

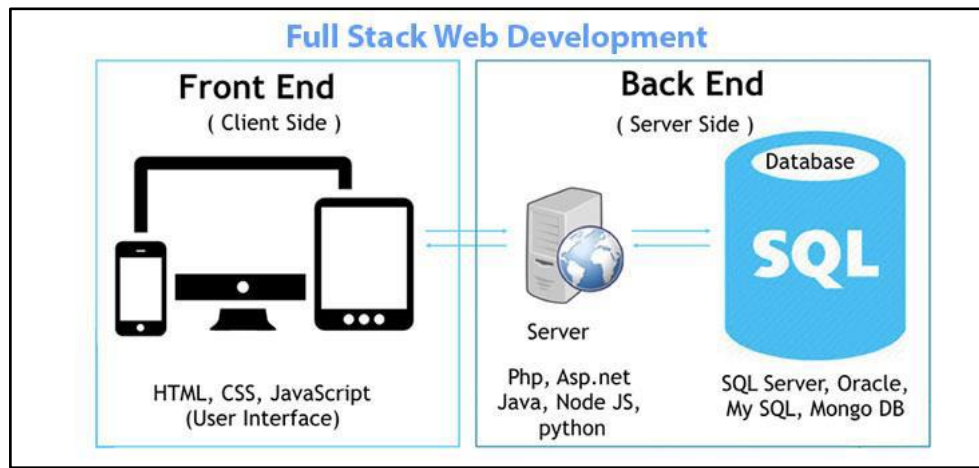


Fig. 3.6: Full-Stack Development

### 3.3.2 FRONT-END

Front-end mostly deals with managing what people interact with and see in a software application. Having web pages or mobile applications that are easily navigable and efficiently interactive is integral for users to continue to utilize your software. Those who work on the front-end have knowledge of client software like HTML, CSS, and JavaScript.

Hypertext Markup Language (HTML) and Cascading Style Sheets (CSS) are two of the core technologies for web pages. HTML determines the structure of a web page, and CSS influences the visual layout. JavaScript is a programming language making for dynamic web pages. The simple interactions that you take for granted like dragging and dropping or scrolling, are all the trademarks of JavaScript programming. Many JavaScript frameworks and libraries also exist to speed up and simplify the development process. Similarly, other technologies support HTML and CSS. It defines how a web page would look like so it can be considered the skeleton of any web application. CSS is a style sheet language which provides style and visual enhancements to the documents written in HTML. JavaScript

is the most advanced language among these technologies. It performs HTML DOM (Document Object Model) manipulation to provide a dynamic interface to users. Moreover, it provides an interactive interface to the users by creating pop-up messages, validating form inputs, and changing the layout based on events like user-input or mouse clicks. All these technologies are controlled by the browser to provide a front-end web interface.

### **3.3.3 BACK-END**

Back-end development handles everything that the user typically does not see. Whatever front-end technology is being built for users to see, back-end developers are peeking out from the curtain directing these features with their code. It refers to the server-side development of web application or website with a primary focus on how the website works. Server software would involve languages that perform well when it comes to servers and networking like Python or C++. Query languages for managing databases fall under the category of server software too.

Node.js, in particular, is a favourite among back-end developers. This is a JavaScript framework enabling back-end development, meaning developers can use JavaScript for front-end and back-end development, in other words, full stack development. A web application cannot run without both the front-end and back-end services. Back-end technologies usually consist of the programming languages such as PHP, Ruby, Python, Java, Node.js, and different frameworks.

### **3.3.4 DATABASES**

Many websites store data whose information is stored in a database server using SQL. A full stack developer uses a software package, like MySQL, to access database servers and retrieve queries. The SQL language is common, so a popular software alternative to MySQL is MongoDB and different database servers are available. Databases are much like groups of spreadsheets or tables, which link together using fields. Fields function is through IDs and keys to properly structure database tables.

### **3.4.3 LIBRARIES**

The libraries we will need:

1. OpenCV
2. dlib
3. Face\_recognition

OpenCV is a video and image processing library and it is used for image and video analysis, like facial detection, license plate reading, photo editing, advanced robotic vision, and many more.

The dlib library contains our implementation of ‘deep metric learning’ which is used to construct our face embeddings used for the actual recognition process.

The face\_recognition library is super easy to work with and we will be using this in our code. First, remember to install dlib library before you install face\_recognition.

#### **3.4.3.1 DLIB LIBRARY**

It’s an open-source software library written for Machine learning applications. One of the most important uses is face detection. This library uses a pre-trained model that identifies 68 data points on the user’s face depending upon the position of the eyes, nose and mouth. We are using this library to detect the eyes and mouth of the user and to apply appropriate try on. The Figure 4.4 illustrates the 68 landmarks numbering on the user’s face when using this library.

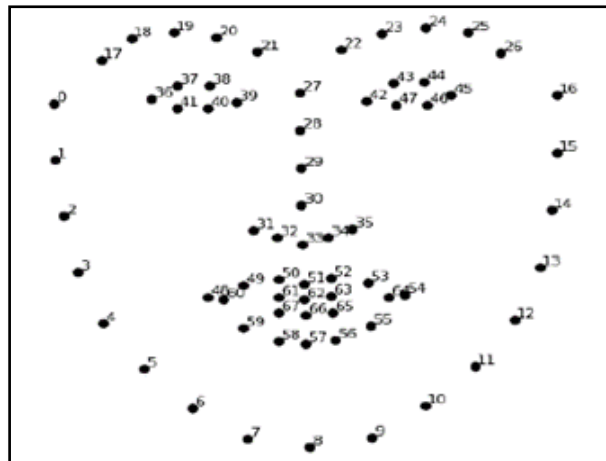


Fig. 3.7: Sample of 68 datapoints on the user’s face

### **3.3.5 PROJECT REQUIREMENTS**

#### **a. Software Requirements:**

- 1) Operating System - Windows
- 2) Front End – HTML, JAVA, CSS
- 3) Back End – Servlet
- 4) Scripts - JavaScript
- 5) Database – MySQL
- 6) OpenCV

**b. Hardware Requirements:**

Personal computers with required Configuration.

**c. Software's Used:**

- 1) Apache Tomcat Server
- 2) Eclipse IDE
- 3) MySQL

### **3.3.6 SOFTWARE'S USED**

- As we are using JAVA programming, Apache Tomcat Server is the best available server. It is an open-source application server for hosting JAVA based code, as it allows the users to run Servlet and JAVA Server Pages.
- Eclipse IDE is an open-source software, used for developing and editing the programs in JAVA.
- MySQL server, is the world's most popular open-source database for cost-effectively delivering reliable, high-performance and scalable e-commerce, online transaction processing, and embedded database applications. It provides a database management system with querying and connectivity capabilities, as well as the ability to have excellent data structure and integration with many different platforms. It can handle large databases reliably and quickly in high-demanding production environments. The MySQL server also provides rich function such as its connectivity, speed, and security that make it suitable for accessing databases.

For storing the data, we use MYSQL data server as a database.

- OpenCV: It is an open-source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in commercial products.
- HTML: HTML stands for Hypertext Markup Language. It is a standardized markup language used for creating a webpage. HTML is a markup language that combines hypertext with markup. The term "hypertext" refers to the link between web pages. The text document within the tag that defines the structure of web pages is defined using a markup language. These pages can include writing, links, pictures, sound and video.



HTML is used to denote these elements so that the web browser can display them correctly.

- CSS: It stands for Cascading Style Sheets. It is a style sheet language used for describing the presentation of a document written in a markup language such as HTML. It is used to create the stylistic parts of the website's user interface. As a full-stack developer, you'll use CSS to add stylistic elements and adjust the website for mobile and tablet devices. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple web pages to share formatting by specifying the relevant CSS in a separate.
- JavaScript: Developers use JavaScript to create the elements of a webpage that interacts with a user. As a full-stack developer, you'll use JavaScript to build the functional parts and draw together elements from the frontend and backend. For example, JavaScript when creating buttons for users to click. This means JavaScript functions can run after a webpage has loaded without communicating with the server.
- JAVA: Java is an object-oriented programming (OOP) language based around objects. It was first released in 1995, and 40.2% of software developers now use it. Eclipse is one among the IDEs for JAVA programming. Java is mainly used for server-side development, while JavaScript focuses more on client-side scripts.

# **CHAPTER 4**

## Chapter 4

# ALGORITHMS USED IN PROJECT DESIGN

The algorithms used in this project are Floyd–Steinberg dithering and RANSAC algorithm.

## 4.1 ALGORITHM FOR SHARES GENERATION

True color secret image of size is taken. In this scheme secret image is divided into R, G, B components. Each single value of pixel of  $R(i, j)$  ( $G(i, j)$  or  $B(i, j)$ ) red (green or blue) components is represented in binary form, 0 to represent transparent and 255 to represent red pixel (green or blue). Each component is represented into  $N$  1-bit planes. Colourful cover images are used to hide the  $N$  1-bit planes using EVCS for generation of meaningful shares. Cover images are also decomposed into three components (R, G, B) and  $N$  1-bit planes are generated. Then  $n$  bit planes of secret images are embedded into cover images for generating meaningful images. Then, every pixel of all the binary images generated from the bit plane is expanded into a  $2 \times 2$  block to which a black or white color is assigned according Fig. 1.5.

### Algorithm:

1. Transform the color image  $S$  into three channels: R, G, and B.
2. Each component is divided into  $N$  1-bit planes. Each bit plane is the binary image contacting level of information.
3. Apply EVCS to each bit planes of secret color image using corresponding bit planes of respective component (R, G or B) of  $n$  public color images.
4. Stack the corresponding binary shares in bit level to achieve  $n$  shares.
5. Generate the  $n$  color shares by combining the corresponding shares of R, G and B channels.

## 4.2 FLOYD STEINBERG DITHERING ALGORITHM

Floyd–Steinberg dithering is an image dithering algorithm, used by the image manipulation tools. It executes the dithering of image using error diffusion technique, which means it adds the residual quantization error of a pixel onto its neighbouring pixels. Dither is routinely used for processing both in audio as well as video data [13]. The diffusion coefficient pixels have the property, that if the original pixel values are exactly

halfway in between the nearest available colors, the dithered result is a checkerboard pattern. This property is applied in the share creation process of VC.

The working of the dithering algorithm is as follows:

- For each point in an image, we first find the closest color available.
- Then calculate the difference between the value in the image and the color in the image.
- Now we divide these error values and distribute them over the neighbouring pixels which have not visited yet. When get to these later pixels, just add the errors distributed from the earlier ones, clip the values to the allowed range if needed, and then continue.

The array structure thus formed without the noise level is used to construct the shares. The bit-depth transitions generated from the dithering algorithm increases the intensity of the image. The dithering is applied to the images with limited intensity resolutions [9].

### 4.3 RANSAC ALGORITHM

Random sample consensus, or RANSAC, is an iterative method for estimating a mathematical model from a data set that contains outliers. The RANSAC algorithm works by identifying the outliers in a data set and estimating the desired model using data that does not contain outliers. The RANSAC algorithm is a learning technique to estimate parameters of a model by random sampling of observed data. Given a dataset whose data elements contain both inliers and outliers, RANSAC uses the voting scheme to find the optimal fitting result. RANSAC is a resampling technique that generates candidate solutions by using the minimum number observations (data points) required to estimate the underlying model parameters [31].

### 4.4 XOR – BASED VCS

The detailed description of the  $(k, k)$ -VCS and  $(k, n)$ -VCS are illustrated as Algorithm 1 and Algorithm 2, respectively. The sharing procedure of Algorithm 4 for a secret pixel  $S$   $(i, j)$  in binary secret image.

Algorithm 1: OR and XOR based  $(k, k)$ -VCS

Input:

A binary secret image  $S$ , whose size is  $M \times N$ .

Output:

$k$  shares  $S_1, S_2, \dots, S_k$ .

Step 1: Construct the  $2k-1 \times k$  basis matrix *Beven* 0 by adding all  $k$ -dimensional binary vector that contains even numbers of 1s. Similarly, construct the  $2k-1 \times k$  basis matrix *B-odd* by adding all  $k$ -dimensional binary vector that contains odd numbers of 1s.

Step 2: For  $1 \leq i \leq M$ ,  $1 \leq j \leq N$ , repeat Steps 3-5.

Step 3: For each secret pixel  $S(i, j)$ ,

Step 3.1: If the secret pixel  $S(i, j)$  is white, then randomly select a row  $R = \{\bar{r}g\}$  from basis matrix *B-even*, where  $1 \leq g \leq k$ .

Step 3.2: If the secret pixel  $S(i, j)$  is black, then randomly select a row  $R = \{\bar{r}g\}$  from basis matrix *B-odd*, where  $1 \leq g \leq k$ .

Step 4: Distribute  $k$  grids  $\bar{r}1, \bar{r}2, \dots, \bar{r}k$  to  $r1, r2, \dots, rk$  randomly.

Step 5: Assign  $k$  grids  $r1, r2, \dots, rk$  to  $S1(i, j), S2(i, j), \dots, Sk(i, j)$ , respectively.

Step 6: Output the  $k$  shares  $S1, S2, \dots, Sk$ .

#### Algorithm 2: OR and XOR based $(k, n)$ -VCS

##### Input:

A binary secret image  $S$ , whose size is  $M \times N$ .

##### Output:

$n$  shares  $S1, S2, \dots, Sn$ .

Step 1: Construct the  $2k-1 \times k$  basis matrix *Beven* 0 by adding all  $k$ -dimensional binary vector that contains even numbers of 1s. Similarly, construct the  $2k-1 \times k$  basis matrix *B-odd* by adding all  $k$ -dimensional binary vector that contains odd numbers of 1s.

Step 2: For  $1 \leq i \leq M$ ,  $1 \leq j \leq N$ , repeat Steps 3–6.

Step 3: For the secret pixel  $S(i, j)$ ,

Step 3.1: If the secret pixel  $S(i, j)$  is white, then randomly select a row  $R = \{\bar{r}g\}$  from basis matrix *B-even*, where  $1 \leq g \leq k$ .

Step 3.2: If the secret pixel  $S(i, j)$  is black, then randomly select a row  $R = \{\bar{r}g\}$  from basis matrix *B-odd*, where  $1 \leq g \leq k$ .

Step 4: Let the rest of  $n - k$  grids:  $\bar{r}k+1 = \bar{r}k+2 = \dots = \bar{r}n = 0$ .

Step 5: Assign  $n$  grids  $\bar{r}1, \bar{r}2, \dots, \bar{r}k, \bar{r}k+1, \dots, \bar{r}n$  to  $r1, r2, \dots, rk, rk+1, \dots, rn$  randomly.

Step 6: Distribute  $r1, r2, \dots, rn$  to  $S1(i, j), S2(i, j), \dots, Sn(i, j)$ , respectively.

Step 7: Output  $n$  shares  $S1, S2, \dots, Sn$ .

# **CHAPTER 5**

## Chapter 5

# RESULTS AND DISCUSSION

This chapter briefs about the results obtained and the comparison related to other existing algorithms.

## 5.1 SNAPSHOTS OF THE PROJECT WEBSITE

- Login Page: The Fig. 5.1 below shows the user interface login page in which user can login using his/her login id and password.

The screenshot shows a web page titled "Visual Cryptography for biometric privacy". Below the title is a "User Login" section. It contains two input fields: "USERNAME" with the value "admin" and "PASSWORD" with masked characters "\*\*\*\*\*". Below these fields is a "Login" button.

Fig 5.1: Visual of our Login Page

- Profile details: Fig. 5.2 below shows the profile details on the webpage that is stored in the database.

The screenshot shows a web page titled "Visual Cryptography for biometric privacy". Below the title is a navigation bar with links: Home, Profile, Image, Encryption, Decryption, Logout. Below the navigation bar are two buttons: "Edit Profile" and "Change Password". Below these buttons is a "User Profile Details" section. It contains a table with the following data:

Your ID No	:	3
Your Name	:	Rahul
Your User ID	:	Rahul
Your Department	:	All
Your Designation	:	All
Your Mail ID	:	Admin@gmail.Com
Your Cell NO	:	9916876542
Your Address	:	Mangalore

Fig. 5.2: Admin Details

- Image page: Fig. 5.3 shows the webpage where we can add, edit or delete image for encryption.

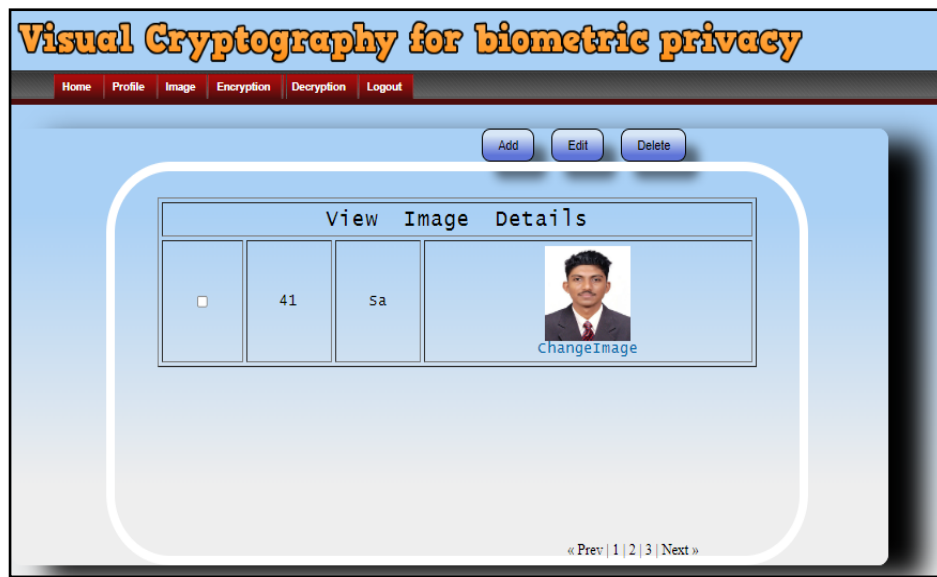


Fig. 5.3: Image addition, editing and deletion page

- Data Storage in MySQL: Fig. 5.4 depicts the data stored in the database.

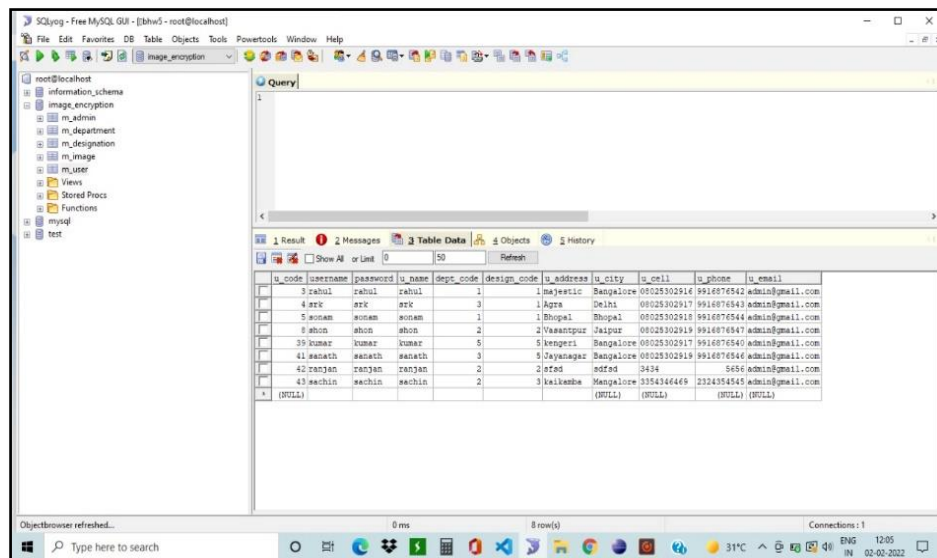


Fig. 5.4: Database (Back-End)

Once the user has logged in to his/her account with the username and password of theirs. In the profile page, the user details where all the details related to user like his department, mail id, cell number, user id etc. will be displayed. The user can add, edit or delete any image his wishes to. This page will further help in encryption since the image needed for encryption will be added here.



## 5.2 RESULTS

At the end of the project, we can,

- a. hide a private face image in two unrelated host face images.
- b. successfully match of face images that are reconstructed by superimposing the host images.
- c. the inability of the host images, known as sheets, to reveal the identity of the secret face image.
- d. use different pairs of host images to encrypt different samples of the same private face.

### 1. Encryption:

- There are 4 steps in the Encryption Process:

- a) Sieving
- b) Division
- c) Shuffling
- d) Combining

- Sieving: Sieving of the images is shown in Fig. 5.5.

Every image consists of RGB share; hence the original image is first divide into this RGB share. This is called as Sieving.

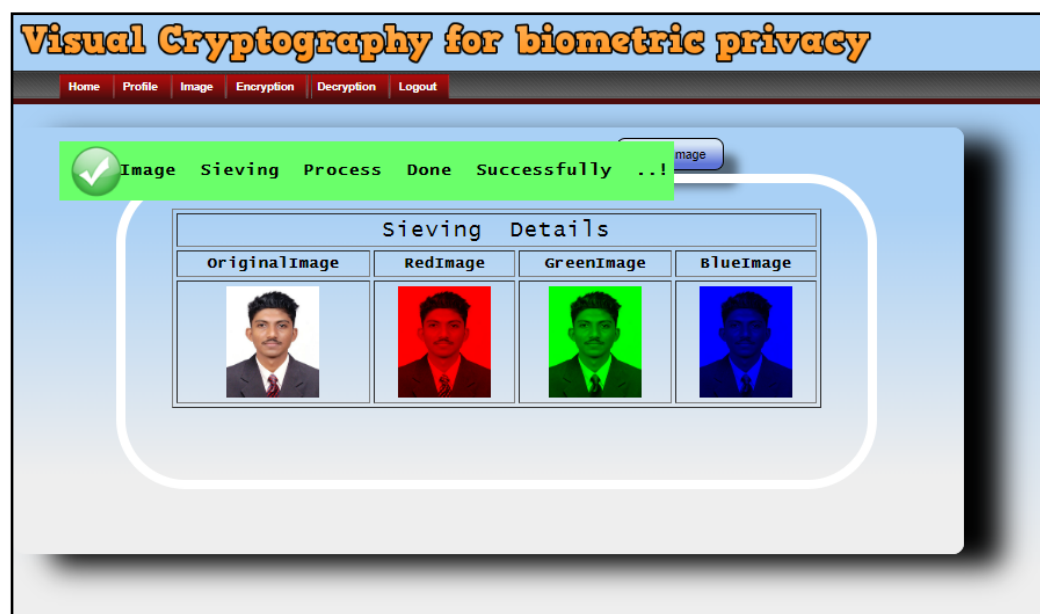


Fig 5.5: Sieving of the images

- Division: Image Division is shown in Fig. 5.6.  
After the Sieving process is completed, the division process takes place. Here, the original RGB share is further divided into two more shares.

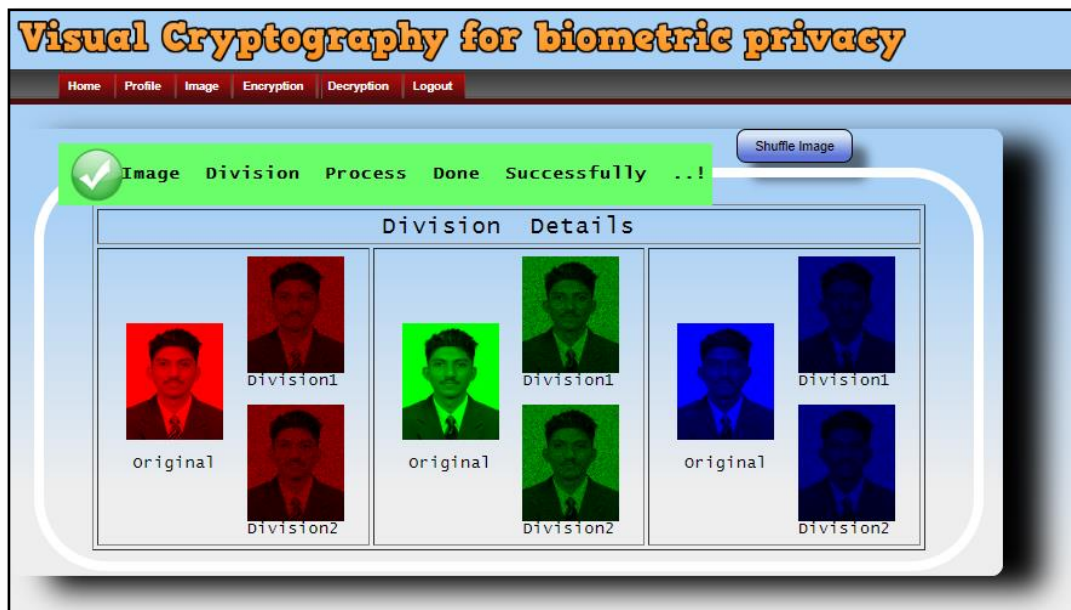


Fig. 5.6: Image Division

- Shuffling: Image Shuffling is shown in Fig. 5.7.  
The divided images are further shuffled to provide more security to the system. For this method we use XOR based VCS.

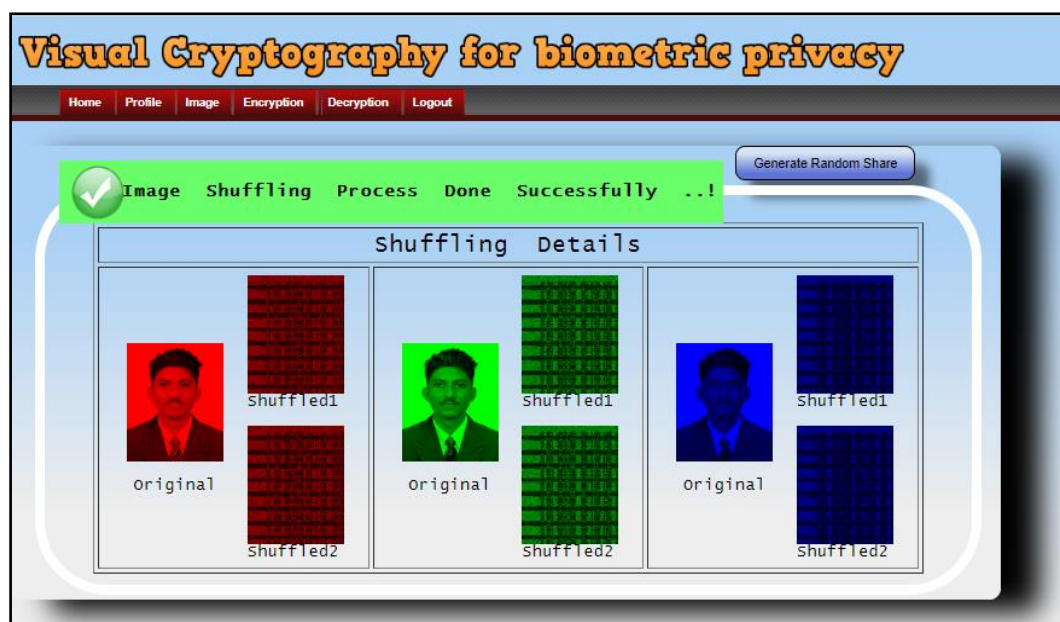


Fig. 5.7: Image Shuffling

- Encryption: The final encryption process and the shares are shown in Fig. 5.8. After all the steps, the last step is combining these shares. The six shuffled shares are combined to form two different random shares which are further saved for the future use. This is called Encryption.

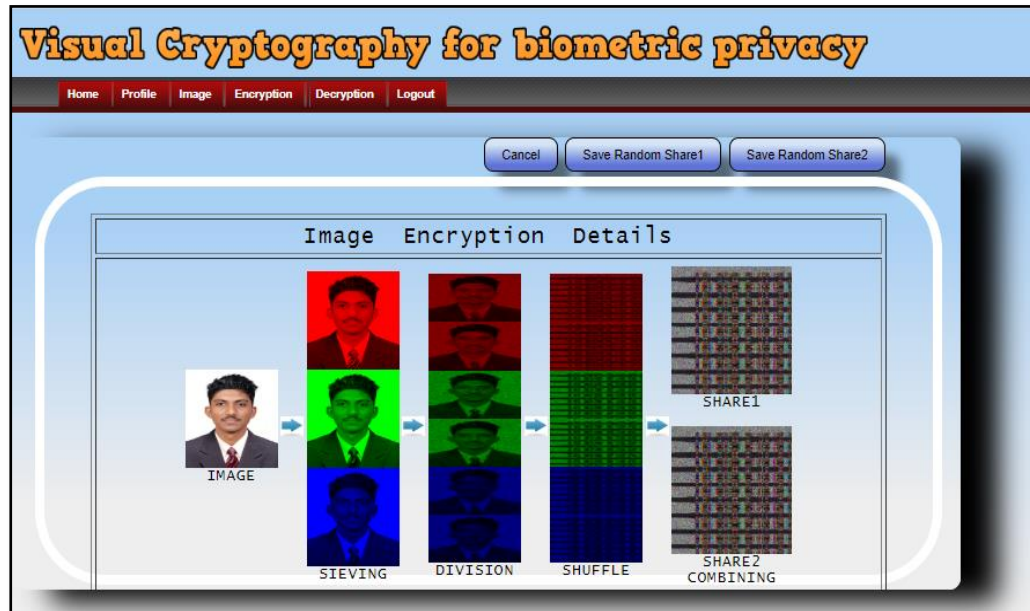


Fig. 5.8: Image Encryption

## 2. Decryption:

Fig. 5.9 shows the shares generated during the encryption process are used and Fig. 5.10 shows the decrypted image.

For decryption process, the two random shares which are obtained at the end of the encryption process are used. Only if these two shares are simultaneously available then we can decrypt the image.

After the two shares are uploaded, the decrypted image is obtained.

For encryption and decryption, we used Floyd-Steinberg algorithm and XOR based VCS for shuffling the shares obtained.

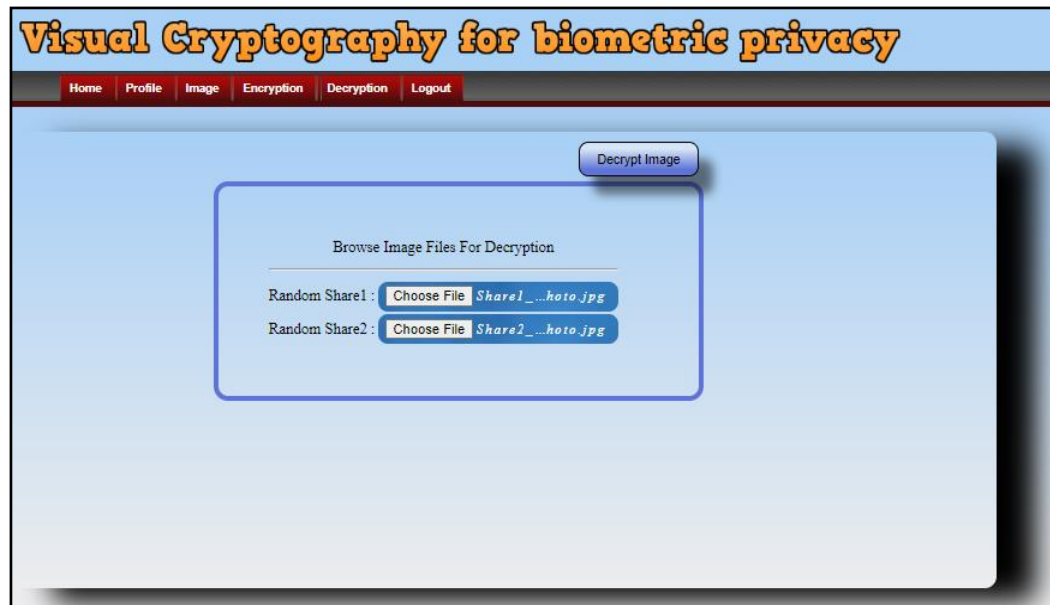


Fig. 5.9: Adding Images for Decryption

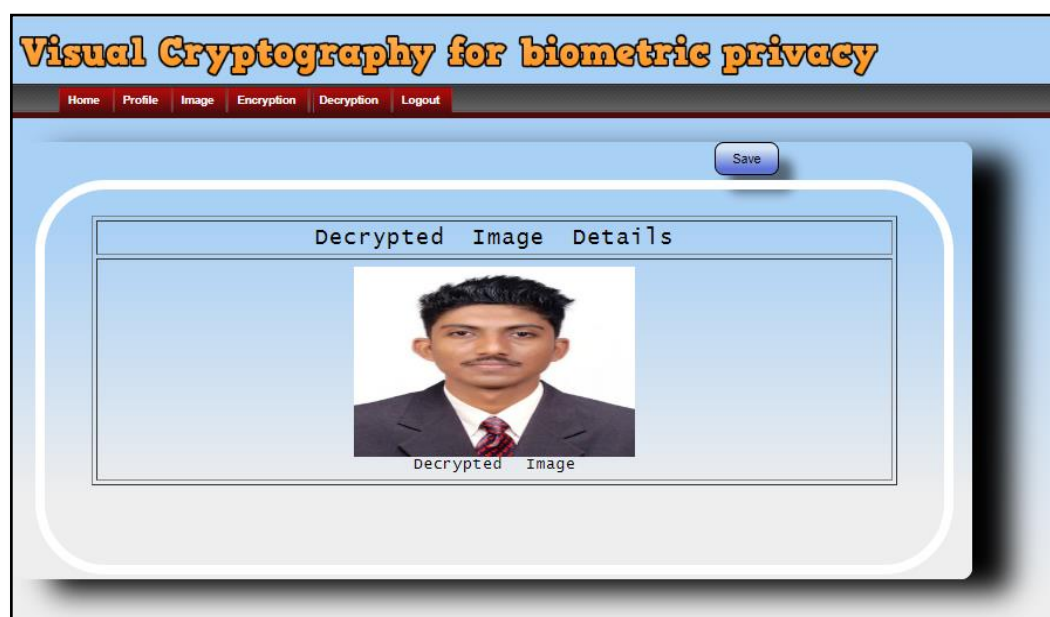


Fig. 5.10: Decrypted Image

### 3. Face Matching:

After the encryption and the decryption process, Fig. 5.11 shows the webpage for the face matching process and Fig. 5.12 shows the matched face.

OpenCV is used for the face matching technique.

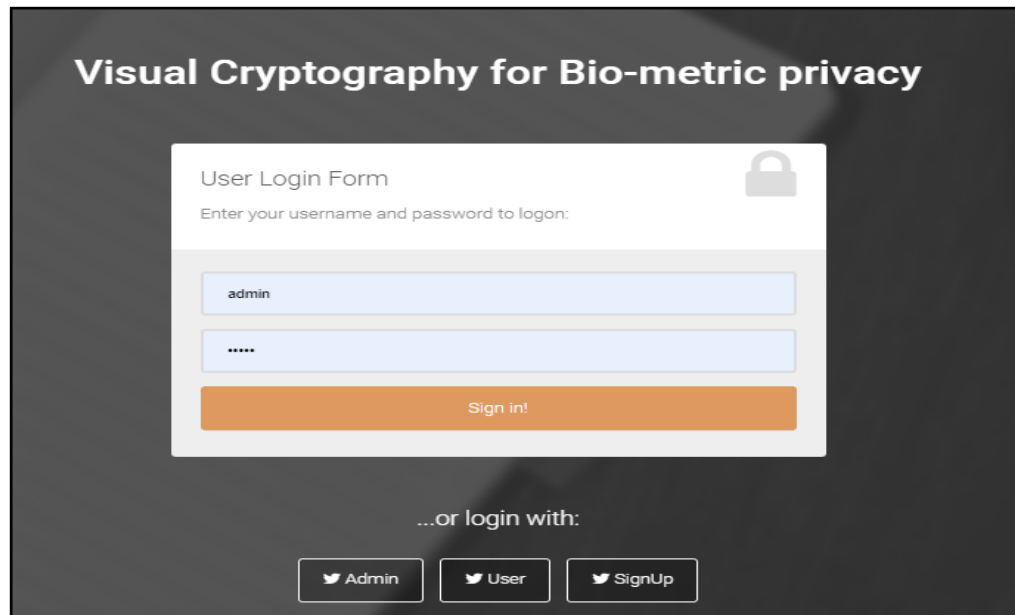


Fig. 5.11: Login Page of the Face Matching Page

After the user has logged in to the account, he can view his profile, images can be searched, if the password needs to changes it can be done here, the matching of the original and decrypted image can be done here.

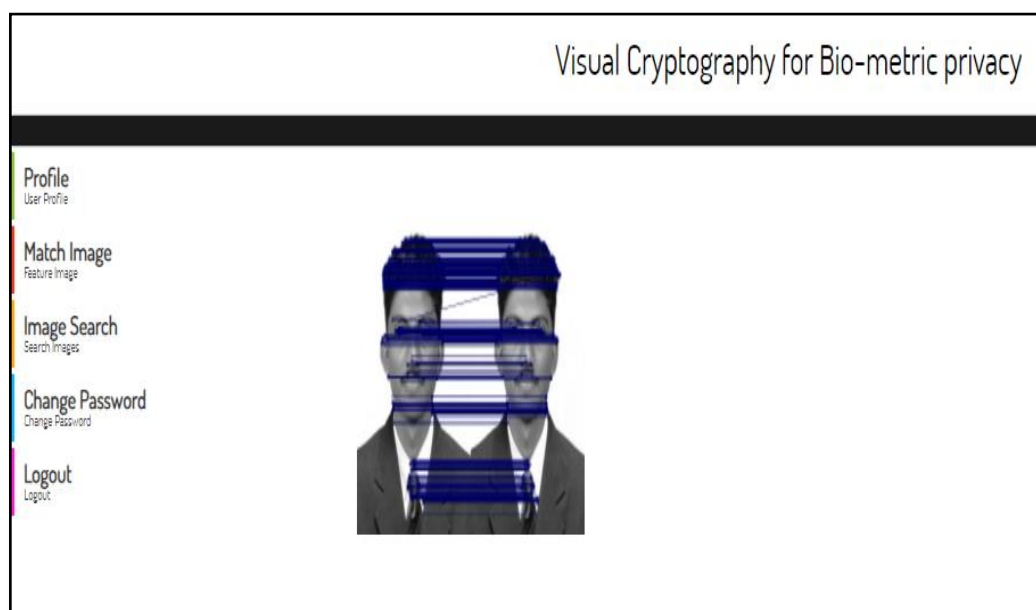


Fig. 5.12: Face Matching

## 5.3 COMPARISON

Different types of algorithms and schemes are compared.

### 5.3.1 VCS COMPARISON – 1

Table 5.1 shows the VCS comparison based on different algorithms and its advantages and disadvantages.

Table 5.1: VCS Comparison - 1

Description	Advantages	Disadvantages
(n; n) threshold non-expansible XOR-based VC	Contrast	Memory complexity, pixel expansion
VC for greyscale images	Computational complexity	Pixel expansion, recovered image quality
Extended CVC	Meaningful shares	Memory complexity, pixel expansion, recovered image quality
XOR-based VC	Recovered image quality	Memory complexity, pixel expansion
Extended VC using halftoning	Security	Recovered image quality, pixel expansion

### 5.3.2 VCS COMPARISON – 2

Table 5.2 shows the VCS comparison based on different techniques and their shares.

Table 5.2: VCS Comparison - 2

Authors	Technique	No. Of shares	Pixel Expansion	Contrast Loss
Naor & Shamir, 1995	Pixel-based VC	2	m	1/m
Hou, 2003	VC for color image	2	m	1/m

Wu & Chang, 2005	Multiple image VC	2	m	1/m
Tuyls et al., 2005	XOR-based VC	2	m	Minimum
Askari et al., 2014	VC for grayscale image using halftoning technique (Block replacement)	2	Nil	Minimum

### 5.3.3 VCS COMPARISON – 3

Table 5.3 shows the VCS comparison based on pixel expansion and encryption method.

Table 5.3: VCS Comparison – 3

Authors	Pixel Expansion	Secret image format	Encryption Method
Naor & Shamir, 1995	Yes	Binary	VC
Hou, 2003	Yes	Grayscale, color	Halftoning, color decomposition method
Hou et al, 2015	No	Binary, Gray scale	PVSSM
Y. Zhao and F.-W. Fu	No	Grayscale	XOR based
M. Karolin and T. Meyyappan, 2019	No	Color	Share generation, XOR

# CHAPTER 6



## **Chapter 6**

# **CONCLUSION**

Visual Cryptography is basically an encryption method which has a merit of decrypting encrypted images rather than cryptographic computations. It is an original VC algorithm is proposed to secure the transmitted images. The significance of VCS in enhancing in the security and integrity of secret information has also been considered. In the proposed system, when the computing devices are available, the secret image can be reconstructed perfectly by XOR-ing the entire shares. The proposed method can be improved by civilizing the colors created and to produce clear resultant image.

## **6.1 FUTURE SCOPE**

In recent years, a lot of research effort has been dedicated towards VC. Despite the advancements that have been achieved, VC still has some significant drawbacks that prevent its adoption in real life applications. To overcome these issues, one possible research direction would be to examine and improve existing schemes for specific types of images or specific applications. It can be used for all of the security related institutions like military, offices, confidential laboratories. It will work for the multiple systems and multiple cover images. It will work for more databases for more security.

In short, the following research directions can be considered for future work:

1. Leveraging upon specific features of VC schemes for targeted real-life applications.
2. Addressing the trade-of between pixel expansion and computational/memory complexity.
3. Improving the efficiency of VC schemes that support multiple secrets or progressive recovery.
4. Designing efficient VC schemes that support two or more desirable features, including multiple shares, multiple secrets, color images and meaningful shares.

# REFERENCES

## REFERENCES

- [1] Arun Ross, Asem Othman, “*Visual Cryptography for Biometric Privacy*”, IEEE Transactions on Information Forensics and Security, VOL.6 No.1, MARCH 2011.
- [2] Naor, M. and Shamir. A, “*Visual Cryptography*”, EUROCRYPT 1994. Lecture Notes in Computer Science, Vol. 950. Springer, Berlin, Heidelberg (1999).
- [3] Shefali Arora & M.P.S Bhatia, “*Challenges and opportunities in biometric security: A survey*”, Information Security Journal: A Global Perspective (2021).
- [4] Jeng-Shyang Pan, Tao Liu, Hong-Mei Yang, Bin Yan, Shu-Chuan Chu, Tongtong Zhu, “*Visual cryptography scheme for secret colour images with colour QR codes*”, Elsevier November 2021.
- [5] Yongkang Zhao, Fang-Wei Fu, “*A contrast improved OR and XOR based  $(k, n)$  visual cryptography scheme without pixel expansion*”, 20 December 2021, Published by Elsevier B.V.
- [6] Jyoti Tripathi, Anu Saini, Kishan, Nikhil, Shazad, “*Enhanced Visual Cryptography: An Augmented Model for Image Security*”, (ICCIDS 2019), Published by Elsevier B.V.
- [7] M. Karolin and T. Meyyappan, “*Secret Multiple Share Creation with Color Images using Visual Cryptography*”, April 4-6, 2019, India, IEEE.
- [8] M. Karolin, T. Meyyappan, “*Image Encryption and Decryption using RSA Algorithm with Share Creation Techniques*”, ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.
- [9] P. Punithavathi & S. Geetha (2017), “*Visual cryptography: A brief survey*”, Information Security Journal: A Global Perspective”, 26:6, 305-317 (Taylor & Francis).
- [10] M.Karolin, Dr. T. Meyyappan, “*RGB Based Secret Sharing Scheme in Color Visual Cryptography*”, Vol. 4, Issue 7, July 2015, DOI: 10.17148/IJARCCE.2015.4734.
- [11] Apurva A. Mohod, Prof. Komal B. Bijwe, “*An Image Database Security Using Multilayer Multi Share Visual Cryptography: A Review*”, ISSN 2319 -4847, Volume 3, Issue 10, October 2014.
- [12] Ms NehaKhatrī – Valmik, Prof. V. K Kshirsagar, “*Blowfish Algorithm*”, ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83.
- [13] Atul Sureshpant Akotkar, Chaitali Choudhary, “*Secure of Face Authentication using Visual Cryptography*”, International Journal of Innovative Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-2, Issue-5, April 2014.

- [14] Shubhangi Rajanwar<sup>1</sup>, Shirish Kumbar<sup>2</sup>, Akshay Jadhav, “*Visual Cryptography for Biometric Privacy*”, International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume 3 Issue 12, December 2014.
- [15] N. Askari, H.M. Heys, and C.R. Moloney, “*An Extended Visual Cryptography Scheme Without Pixel Expansion for Halftone Images*”, (2010).
- [16] Bhagyashri P. Kandalkar, Gopal D. Dalavi, “*Development of Visual Cryptography Technique for Authentication using Facial Images*”, IJSR, ISSN: 2319-7064, Volume 4 Issue 12, Dec 2016.
- [17] Dr. D. Devakumari MCA., M.Phil., PhD.<sup>1</sup>, K. Geetha, “*A Survey of Visual Cryptographic Method for Secure Data Transmission*”, ISO 3297:2007 Certified Vol. 6, Issue 6, June 2017.
- [18] Tiwari, Meher Gayatri Devi; Kakelli, Anil Kumar. “*Secure Online Voting System using Visual Cryptography*”, Walailak Journal of Science & Technology Vol 18, Issue 15, January 2021.
- [19] Mr. Ravi Kumar, Ms. Namrata Singh, “*A survey based on Enhanced the Security of Image using the combined techniques of steganography and cryptography*”, International Conference on Innovative Computing and Communication (ICICC 2020).
- [20] Santhi, B K.S. Ravichandran, A.P. Arun and L. Chakkrapani, “*A Novel Cryptographic Key Generation Method Using Image Features*”, Research Journal of Information Technology 4(2):88-92, 2012.
- [21] L. N. Pandey and Neeraj Shukla, “*Visual Cryptography Schemes using Compressed Random Shares*”, in International Journal of Advanced Research in Computer Science and Management Studies, Volume 1, Issue 4, September 2013, pp:62 – 66.
- [22] M. Karolin, Dr. T. Meyyappan.SM. Thamarai, “*Image encryption and decryption of color images using visual cryptography*” International Journal of Pure and Applied Mathematics, Volume. 118, No. 8, 2018, 277-281.
- [23] Sozan Abdulla, (2010), “*New Visual Cryptography Algorithm for Colored Image*” Journal of Computing.
- [24] R. Floyd and L. Steinberg, “*An adaptive algorithm for spatial greyscale*”, SPIE Milestone Series 154, pp. 281–283, 1999.
- [25] Ateniese, G., Blundo, C., Santis, A., & Stinson, D. (2001), “*Extended Capabilities for Visual Cryptography*”, Theoretical Computer Science, doi:10.1016/S0304-3975(99)00127-9.

- [26] Manika Sharma & RekhaSaraswat, (2013) “*Secure Visual Cryptography Technique for Color Images Using RSA Algorithm*”, International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2.
- [27] Ram Gopal Sharma, Priti Dimri, Hitendra Garg, “*Visual Cryptographic Techniques for secret image sharing: A Review*”, Vol 27, 2019 (Taylor & Francis).
- [28] Hou, Y. C., & Tu, S. F, “*A visual cryptographic technique for chromatic images using multi-pixel encoding method*”, Journal of Research and Practice in Information Technology, 2005, 37(2), 179–192.
- [29] Hou, Y, “*Visual Cryptography for color images. Pattern Recognition*”, 2003, 36(7), 1619–1629. doi:10.1016/S0031-3203(02) 00258-3.
- [30] Miss. Nuzhat Ansari, Prof. Rahila Shaikh, “*A Keyless Approach for RDH in Encrypted Images using Visual Cryptography*”, ICISP2015, 11-12 December 2015, Nagpur, INDIA.
- [31] Konstantinos G. Derpanis, “*Overview of the RANSAC Algorithm*”, May 13, 2010.
- [32] Anantha Kumar Kondra, Smt. U. V. RatnaKumari, “*An Improved (8, 8) Color Visual Cryptography Scheme Using Floyd Error Diffusion*”, in International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, pp.1090.
- [33] Dyala R. Ibrahim, Je Sen The, Rosni Abdullah, “*An Overview of Visual Cryptography Techniques*”, January 2021.
- [34] G. Ateniese, C. Blundo and D. R. Stinson, “*Constructions and bounds for visual cryptography*”, in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, pp. 416-428, 1996.
- [35] D. Jena and S.K. Jena, “*A Novel Visual Cryptography Scheme*”, In Proceeding of International Conference on Advance Computer Control, pp 207-211(2009).
- [36] Aarti, Pushpendra K Rajput, “*An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding*”, I.J.Computer Network and Information Security, 2014, 2, 54-60.