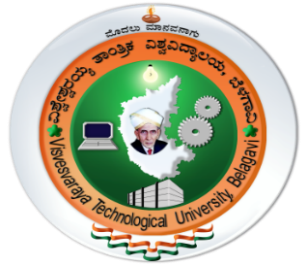
VISVESVARAYA TECHNOLOGICAL UNIVERSITY

 Jnana Sangama, Belagavi - 590018

Project Synopsis

On

“**VISUAL CRYPTOGRAPHY FOR BIOMETRIC PRIVACY**”

Submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF ENGINEERING

in

ELECTRONICS & COMMUNICATION ENGINEERING

By

SHRAVAN KUMAR 4MT18EC079

SUPRABHA 4MT18EC089

SOORAJ SHETTY 4MT18EC088

M B SACHIN 4MT18EC045

Under the Guidance of

Mr. Ganesh V N

Senior Assistant Professor

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING

Badaga Mijar, Moodabidri-574225, Karnataka

2021-2022

**CONTENTS**

1. ABSTRACT
2. INTRODUCTION
3. PROBLEM STATEMENT
4. OBJECTIVES
5. METHODOLOGY
6. EXPECTED OUTCOME
7. REFERENCES

# **ABSTRACT**

The Cryptography is basically securing the data during the communication between different system . “Biometric”, is used for authentication. To work with the biometrics authentication that is used to collect some raw biometric data (e.g. image) and then that data compares with the data (image) stored in the database for providing access. So, at the same time there may be possibilities of the attackers to attack on the data stored in database. Therefore, the security of the biometrics is very important thing. So, the purpose of this paper is to protect biometrics data from the various attacks. 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. In order to accomplish this, we use Visual Cryptography . Visual Cryptography is a process of creating shares from an image so that it would become unreadable for intruder or unauthenticated person. There are various measures on which performance of VCS depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret image. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. This paper implements visual cryptography for colour images in a biometric application. In this project, face authentication scheme helps in achieving robustness by locating an image face from an input image .

# **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 .

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. [1]. 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 . One of the best techniques for the security of images or text is “Visual Cryptography”. In extended VC, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating VC and biometric security techniques [5]. 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.

# **PROBLEM STATEMENT**

When we transmit data (image) over the network, then any unauthenticated person can read our data. 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. Visual Cryptography comes with the guarantee of the security by means of defining perfect secrecy. Usually, a set of attackers are not allowed to learn any information about the (one) secret image even under the possibility of collusion. [4]

# **OBJECTIVES**

* The main objective of this study is to increase security in communication by encrypting the information using a key that is created through using a data.
* To create a new algorithm to secure connection by using the content of an image.
* The need of reliable and effective security mechanisms to protect information systems is increasing due to the rising magnitude of identity theft in our society.

# **METHODOLOGY**

Biometrics can be used to determine a person’s identity even without his knowledge or consent. Hence, Visual Cryptography is used. In VC, there are some algorithms for encrypting and decrypting the images. In this project we are using one secret image and two cover images, then the secret image and cover images are overlapped with each other. And if both the cover images are simultaneously available only then we can access the secret image. The single share cannot give any data(information) about the secret image [4]. In other words, it is a technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used.

The proposed methodology has been divided into 2 phases, i.e. Image Encryption and Image Decryption [3]. Visual Cryptography is not work for the colour images, it only works for the black and white images. So that we are using Gray scaling method for converting the colour images into grayscale images.

Visual Cryptography Scheme (VCS) includes:

1. Secret Image
2. Host Image
3. Sheet
4. Pixel
5. Gray scaling

Pixel consists of Alpha, Red, Green, Blue.

This can be done by:

1. Face Detection based on skin colour
2. RGB Share generation.
3. Share authentication
4. Image Retrieval from RGB Shares

**Software Requirements:**

1) Operating System - Windows

2) Application Server

3) Front End – HTML, Java, C# / Python

4) Scripts - JavaScript

5) Server-side Script - Java Server Pages

6) Database – MySQL

**Hardware Requirements:**

1) Personal computers with required Configuration

2) Biometrics kit to fetch human biometric data and transform it into an image.

Data Flow:



# **EXPECTED OUTCOME**

At the end of the project we expect,

1. the possibility of hiding a private face image in two unrelated host face images.
2. the successful matching of face images that are reconstructed by superimposing the host images.
3. the inability of the host images, known as sheets, to reveal the identity of the secret face image.
4. using different pairs of host images to encrypt different samples of the same private face.
5. the difficulty of cross database matching for determining identities.

In this project we use visual cryptography for biometric privacy, here during encryption part actual image is decompose into three shares i.e. red share, green share and blue share, so it may be done for C, M, Y shares i.e. cyan, magenta, yellow shares, this can be done for a greater number of share generation in future so that security will enhance.

# **REFERENCES**

[1] 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.

[2] Arun Ross, Asem Othman, “Visual Cryptography for Biometric Privacy”, IEEE Transactions On Information Forensics And Security, VOL.6 No.1, MARCH 2011.

[3] Bhagyashri P. Kandalkar, Gopal D. Dalavi, “Development of Visual Cryptography Technique for Authentication using Facial Images”, International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume 4 Issue 12, December 2016.

[4] Shubhangi Rajanwar1, Shirish Kumbar2, Akshay Jadhav, “Visual Cryptography for Biometric Privacy”, International Journal of Science and Research (IJSR), ISSN: 2319-7064, Volume 3 Issue 12, December 2014.

[5] N. Askari, H.M. Heys, and C.R. Moloney, “AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES”.

[6] Dr. D. Devakumari MCA., M.Phil., PhD.1, K. Geetha, “A Survey of Visual Cryptographic Method for Secure Data Transmission”, ISO 3297:2007 Certified Vol. 6, Issue 6, June 2017.