ACKNOWLEDGMENT

First and foremost, we thank our parents for what we are and where we are today, without whose hard work and sacrifice we would not be here today.

We are thankful to **KSCST** for selecting and providing the funding for the project.

We deem it a privilege to place a deep sense of gratitude to our guide **Mr. Ganesh V N**, Senior Assistant Professor, Electronics & Communication Engineering, who always stood behind us and supported in each and every step of the project work.

Our sincere gratitude to our project coordinators, **Dr. Srikrishna Shastri C**, Associate Professor and **Mr. Ramalingam H M**, Senior Assistant Professor, Electronics & Communication Engineering for their valuable time, patience and suggestions and periodic evaluation.

We are grateful to **Dr. Vinayambika S Bhat**, Head of the Department, Electronics & Communication Engineering, Dean, Quality Assurance, Mangalore Institute of Technology & Engineering, Moodabidri for their support and encouragement.

We are indebted to our respected Principal **Dr. M S Ganesha Prasad**, beloved Chairman **Mr. Rajesh Chouta** and the management of Mangalore Institute of Technology & Engineering, Mangalore for having provided all the facilities that helped us in timely completion of this project report.

Finally, we would like to thank all the teaching and non-teaching staff of the Department of Electronics & Communication Engineering for their valuable help and support.

SUPRABHA
SHRAVAN KUMAR
M B SACHIN
SOORAJ SHETTY

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. The attackers may use these opportunities to attack the data within the database. Therefore, the security of biometrics is of high importance. In this idea, a private image is bifurcated 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 dimensions on which Visual Cryptography Scheme performance relay, i.e., accuracy, brightness, pixel widening, security, computer complexity, productive sharing is logical or pointless, 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 process encrypts a private image into stocks so that it can collect a sufficient number of shares produces a private image. This project uses VC of colored images in a biometric application.

Keywords*: Visual Cryptography, Visual Cryptography scheme, Private image, Biometrics.*

TABLE OF CONTENTS

			Page no. s
Acknowledgement			***i***
Abstract			***ii***
Table of contents			***iii***
List of figures			***v***
List of tables			***vi***
Abbreviation			***vii***
Chapter	*No.*	*Titles*	*Page no. s*
Chapter	***1***	**INTRODUCTION**	**1-14**
	1.1	Biometrics	**1**
	1.2	Applications of Biometric systems	**3**
	1.3	Challenges in biometrics	**3**
	1.4	Cryptographic techniques	**4**
	1.5	Visual Cryptography	**5**
	1.6	Halftoning process	**11**
	1.7	Blowfish algorithm	**12**
	1.8	Multiple image Visual Cryptography	**12**
	1.9	Color Visual Cryptography	**13**
	1.10	Balanced Block Replacement	**13**
	1.11	Face Recognition	**14**
Chapter	***2***	**LITERATURE SURVEY**	**15-20**
	2.1	Literature review	**15**
	2.2	Motivation	**19**
	2.3	Scope of the project	**19**
	2.4	Existing system	**19**
	2.5	Problem statement	**20**

Chapter	***3***	**DESIGN AND IMPLEMENTATION**	**21-30**
	3.1	Introduction	**21**
	3.2	Methodology	**21**
	3.3	Implementation	**25**
Chapter	***4***	**ALGORITHMS USED IN PROJECT DESIGN**	**31-33**
	4.1	Algorithm for Shares Generation	**31**
	4.2	Floyd Steinberg Dithering Algorithm	**31**
	4.2	RANSAC algorithm	**32**
	4.3	XOR – based VCS	**32**
Chapter	***5***	**RESULTS AND DISCUSSION**	**34-42**
	5.1	Snapshots of the project website	**34**
	5.2	Results	**36**
	5.3	Comparison	**41**
Chapter	***6***	**CONCLUSION**	**43**
	6.1	Future scope	**43**
REFERENCES			**44-46**

LIST OF FIGURES

Fig.	*No.*	*Titles*	*Page no. s*
Fig.	1.1	Biometric Component	2
Fig.	1.2	Possible attack points in generic biometric	2
Fig.	1.3	Commonly used traits for biometric authentication	4
Fig.	1.4	Encryption & decryption in VC	6
Fig.	1.5	Pixel share illustration	6
Fig.	1.6	VC Techniques	9
Fig.	1.7	Taxonomy of Visual Cryptography	9
Fig.	1.8	Blowfish Algorithm	12
Fig.	1.9	Additive Mode and Subtractive Model	13
Fig.	1.10	Face Recognition	14
Fig.	3.1	Data Flow diagram for the Proposed System	22
Fig.	3.2	Steps involved in generating 2 random shares	23
Fig.	3.3	Encryption rules	24
Fig.	3.4	Encryption Method	24
Fig.	3.5	Decryption Method	25
Fig.	3.6	Full-Stack Development	26
Fig.	3.7	Sample of 68 datapoints on the user's face	28
Fig.	5.1	Login Page	34
Fig.	5.2	Admin Details	34
Fig.	5.3	Image addition, editing and deletion page	35
Fig.	5.4	Database (Back-End)	35
Fig.	5.5	Sieving of the images	36
Fig.	5.6	Image Division	37
Fig.	5.7	Image Shuffling	37
Fig.	5.8	Image Encryption	38
Fig.	5.9	Adding Images for Decryption	39
Fig.	5.10	Decrypted Image	39
Fig.	5.11	Login Page of the Face Matching Page	40
Fig.	5.12	Face Matching	40

LIST OF TABLES

Table	*No.*	*Titles*	*Page no. s*
Table	5.1	VCS COMPARISON - 1	41
Table	5.2	VCS COMPARISON – 2	41
Table	5.3	VCS COMPARISON - 3	42

ABBREVIATIONS

VC	:	Visual Cryptography
EVC	:	Extended Visual Cryptography
VCS	:	Visual Cryptography Scheme
EVCS	:	Extended Visual Cryptography Scheme
HVS	:	Human Visual System
HVC	:	Halftoning Visual Cryptography
DES	:	Data Encryption Standard
RGB	:	Red, Green, Blue
PSNR	:	Peak Signal to Noise Ratio
MSE	:	Mean Square Error
CSS	:	Cascading Style Sheets
HTML	:	Hypertext Markup Language
SQL	:	Structured Query Language