CHAPTER 1

INTRODUCTION

The impact of security objectives of the information systems can be categorized as low, moderate and high in terms of confidentiality, integrity and availability. The additional two more components are accountability and auditability.

The generalized format for expressing the security category (SC) of an information system is:

\[ SC_{\text{information system}} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\} \]

where the acceptable values for potential impact are low, moderate, or high.

These components are derived from BS 7799 (BS 7799 2002), ISO 27002 (ISO 27002 2005) and ISO 27001 (ISO 27001 2005).

![Diagram](image-url)

Figure 1.1 Relationship between confidentiality, integrity and availability
Best practices that facilitate the implementation of security controls include

- Control Objectives for Information and Related Technology (COBIT),
- ISO/IEC 17799/BS 7799,
- Information Technology Infrastructure Library (ITIL), and
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE).

1.1  INFORMATION SYSTEM SECURITY

The minimum security requirements with regard to protect the confidentiality, integrity and availability of the information processed, stored and transmitted by using information system (Mark Stamp 2005) are as follows:

(i) Access control: Organization can limit the information system access only to authorized users.

(ii) Identification and Authentication – Organizations must identify information system users and authenticate or verify the identified users in order to allow the user for further transactions with the organizational information system.

(iii) Personnel Security – Organization should ensure that the information and the information system are protected during and after personnel actions such as termination or transfer.
(iv) System and Information Integrity: Organization must provide protection from malicious activities by means of security alert and take appropriate actions.

(v) Audit and Accountability: Organization must maintain the information system audit records in order to monitor, analyze, investigate and report about if any inappropriate information system activity as well as to trace those unauthorized users those who are accountable for such kind of illegal activities.

1.2 E-AUTHENTICATION

It is the process of establishing confidence in user identities provided electronically to an information system. But there is a technical challenge when this process involves remote authentication of user over a network. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. It can be achieved by incorporating the following technical requirements while designing the information system.

(i) Tokens such as cryptographic key or password for proving identity

(ii) Identity proofing, registration and delivery of credentials which bind an identity to a token

(iii) Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols

(iv) Assertion mechanism used to communicate the results of a remote authentication to other parties.
The authentication process shall provide sufficient information to the relying party to uniquely identify the registration information provided by the user. As per NIST guidelines, the four assurance levels are defined, numbered 1 to 4. Level 4 provides the highest level of authentication assurance, while Level 1 provides the least assurance.

i. Level 1: In this level, there is no need to fully fill the identity proofing. Also, there are no requirements to use cryptographic techniques. It permits any token methods of levels 2, 3, and 4. So, the eavesdropper will often be able to find the password with a straightforward dictionary attack, and this vulnerability is independent of the strength of the operations.

ii. Level 2: It permits to use any of the token methods of level 3 or 4, as well as passwords. In this level, the security attacks such as eavesdropper, replay shall be prevented, since approved cryptography shall be used.

iii. Level 3: This level of authentication assurance requires cryptography strength mechanisms that protect the primary authentication secret key or private key. It requires two-factor authentication; it means that the user must use a password or biometric to activate the key.

iv. Level 4: In this shall provide remote network authentication assurance. It is based on the proof of possession of a key through cryptographic methods. Level 4 is same as level 3; but in this level it requires hard cryptographic authentication of the user for all transactions. This level ensures good, two factor authentications. Either public key or symmetric key technology may be used.
The level of protections should be proved in Information system against security attacks are provided below:

**Table 1.1 Level comparison**

<table>
<thead>
<tr>
<th>Protect against</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-line guessing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Replay</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Eavesdropper</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Verifier impersonation</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Man-in-the middle</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Session hijacking</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 1.3 BIOMETRIC SYSTEM

Biometric systems provide verification ("Is this person who they claim to be?") and identification ("Who is this person?") functions by analyzing "who a person is" (bio- metric characteristic) rather than by "what a person has or remembers" (smartcard, password, etc.) (Uludag et al 2004). Though any physical or behavioral characteristics of an individual can be considered a biometric, an ideal biometric must exhibit the following attributes:

i. Universality: The biometrics is common throughout the entire population.

ii. Uniqueness: Biometric can very well distinguish one individual from another?

iii. Permanence: Biometric shall not change with time (aging)
iv. Collectability: Easy to acquire the biometric.

v. Performance: Indications of how accurate, fast and robust the biometric is.

vi. Acceptability: Is Biometric accepted by the end-users?

1.3.1 Multi Biometrics

By incorporating multiple sources of information into an identification system, the limitations of a single identity management solution can be overcome. A popular trend is to integrate a biometric system with an additional identification technology (smart cards, passwords, RFID, etc.) to form a dual-factor authentication system. Though this is an effective way to increase system performance, it now requires users to possess an item (smart card) or remember a password which are drawbacks that are not present in a biometric system. A multi biometric system, instead, increases the number of sources from which biometric information is collected (Marasco 2010 and Bhanu 2011). Multibiometric systems offer a multitude of benefits compared to traditional uni-modal biometric system. Some of the benefits are described below:

i. Multi biometrics can potentially offer a significant increase in matching performance. The potential for improvement is dependent on the biometric modalities present as well as the fusion algorithm.

ii. Multiple biometric systems may address the issue of non-universality and lack of population coverage. It is likely that if a person fails to enroll into a single biometric they will still have the ability to enroll into the second and, hence, still be capable of using the identification system.
iii. The addition of multiple biometric systems increases the difficulty of spoofing the system.

iv. By including multiple sources of information the system can more effectively address noisy data. The ability to negotiate noisy data is especially important when data is collected in adverse conditions.

v. Multibiometric systems also increase the ability to continuously monitor or track individuals over a period of time. As an example, monitoring through audio/video may be implemented via face and voice recognition. If the system simply relied on face recognition, the ability to track would be lost once the face is occluded and voice recognition would fail if the individual fails to talk. By combining the two technologies it is more likely that the individual can be continuously identified either by a single trait or a combination of both traits.

vi. Multi biometrics increases the redundancy of the system allowing for the recognition system to work continuously even after the failure of one of the biometric sources.

The four most popular biometric modalities deployed today are face, fingerprint, and iris and hand geometry for large scale applications. The proposed system uses finger print, signature, iris and hand geometry.

1.3.2 Fingerprint

A fingerprint is the feature pattern of one finger. It is believed with strong evidences that each fingerprint is unique. Each person has his/her
fingerprints with the permanent uniqueness. So fingerprints have been used for identification.

1.3.3 Signature

A Signature is the behavioral biometric. Signature also has been used for authentication to improve the signature recognition performance by capturing dynamic or online signatures that require pressure-sensitive penpad. Dynamic signatures help in acquiring the shape, speed, acceleration, pen pressure, order and speed of strokes, during the actual act of signing. This additional information seems to improve the verification performance.

1.3.4 Hand Geometry

It is claimed that individuals can be discriminated based on the shape of their hands. Person identification using hand geometry utilizes low resolution (~20 ppi) hand images -to extract a number of geometrical features such as finger length, width, thickness, perimeter, and finger area. The discriminatory power of these features is quite limited, and therefore hand geometry systems are employed only for verification applications (1:1 matching) in low security access control and times such as attendance applications.

1.3.5 Iris

The iris is the colored annular ring that surrounds the pupil. Iris images acquired under infrared illumination consists of complex texture pattern with numerous individual attributes, e.g. stripes, pits, and furrows, which allow for highly reliable personal identification. The iris is a protected internal organ whose texture is stable and distinctive, even among identical twins (similar to fingerprints), and extremely difficult to surgically spoof.
1.4 SECURITY THREATS

1) Intrusion attack: If an attacker can hack into a biometric database, hackers can easily obtain the stored biometric information of a user. This information can be used to gain unauthorized access to the system by either reverse engineering the template to create a physical spoof or replaying the stolen template (Karthik 2008).

2) Function creep: An adversary can exploit the biometric template information for unintended purposes (e.g., covertly track a user across different applications by cross-matching the templates from the associated databases) leading to violation of user privacy. Security of multi biometric templates is especially crucial as they contain information regarding multiple traits of the same user. Hence, multi biometric template protection is the main focus of this work. The fundamental challenge in designing a biometric template protection scheme is to overcome the large intra user variability among multiple acquisitions of the same biometric trait as in Jain et al (2008).

<table>
<thead>
<tr>
<th>Security Level (bits)</th>
<th>Ratio of D1 Cost : EC Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>3:1</td>
</tr>
<tr>
<td>112</td>
<td>6:1</td>
</tr>
<tr>
<td>128</td>
<td>10:1</td>
</tr>
<tr>
<td>192</td>
<td>32:1</td>
</tr>
<tr>
<td>256</td>
<td>64:1</td>
</tr>
</tbody>
</table>
While securing the biometric template, the secure template should satisfy the following two properties:

(i) Non invariability—given a secure template, it must be computationally difficult to find a biometric feature set that will match with the given template, and

(ii) Revocability—given two secure templates generated from the same biometric data, it must be computationally hard to identify that they are derived from the same data or obtain the original biometric data. While biometric cryptosystems generally tend to have stronger non invariability, template transformation schemes typically have better revocability.

1.5 AIM OF RESEARCH WORK

Enhancing the security and privacy of Biometric based Information system by using Cryptography and Information hiding techniques

1.5.1 Motives of Research

Information security is mainly concern about how to protect the user possession and control the access with the user identity. Also it should ensure the privacy and integrity of information for secure communication. In any information system, policies are required to protect privacy and it should be followed by everyone effectively. But, technology shall add confidence or ensure that the policies are followed.
Figure 1.2 Security vulnerabilities of a biometric system

Recent development of Information System, secured communication has become necessary. Most of the researchers were demonstrating that biometric is the ultimate solution for identification and authentication, since it is reliable and universally acceptable in many application areas. While using biometrics for authentication or verification process, it is compromised or once the privacy is violated, it is very difficult to fix it. Biometrics may be abused without the knowledge of an authenticated person.

Multi biometric systems are expected to enhance the recognition accuracy of a personal authentication system by reconciling the evidence presented by multiple sources of information. A multi biometric system should be protected from the hacker or the imposter. Biometric vulnerability refers to Ratha et al (2001) and Sec (2001) is the potential for the biometric system and associated data to be compromised, usage error, fraudulent activity, hardware failure, or external environmental condition which is
shown in Figure 1.2. Cryptosystem can be applied to enhance the security of biometrics. This research work proposes an authentication system by using multiple biometrics with cryptosystem and it address the security issues.

Therefore it is a primary responsibility while designing a technology and it should be sure that it is used properly. Further, technologist should be more concerned about existing security vulnerabilities of biometric system such as spoofing, replay attack, substitution attack, tampering, masquerade attack, Trojan horse attacks etc.

Due to the popularity of biometrics and cryptography, the information security is becoming as a common demand in all application areas. Since the mid-90s, the Biometric Encryption has been researched. Still the following issues such as (i) select a proper biometrics (ii) improving the image quality exist. The major drawback of biometric recognition systems is contact nature of sensors such as inability of the sensing process to accommodate dirt and other environment. The ability of the system to perform well is based almost solely upon the quality of the biometric captured. A well captured biometric is rich in distinguishing information, which in turn gives the feature extraction algorithms the best chance of finding a match with existing records. The desired system performance shall be obtained by using multi-modality based biometric system. In such cases, biometric samples are needed to be collected and stored. It will get processed and transmitted during transactions on Information system. Here, the privacy issue will arise. Therefore, building privacy enhanced technologies are insisted by the global privacy community.

In recent researches, various technological choices are proposed which shall be used to increase privacy and improve security. (Maiorana & Campisi et al 2010). The accuracy, efficiency and usefulness are related with
security. These are mainly to be addressed while designing a technology. Also, from the privacy point of view, identify protection, attribute protection, limits abuse of sensitive details such as patient details are highly to be achieved. The Secret Key generation plays a vital role in secure communication. The widespread use of biometric authentication systems includes the way for the generation of secret key based on the biometric feature. Especially Multimodal biometrics has become popular in deriving the cryptographic secret key (Fierrez et al 2003). Combination of biometrics will harden the Biometric Encryption System.

In recent trends, the generation of secret key using biometrics is very popular Rebecca Heyer (2008). Therefore a technology which will perfectly suitable for one-to-one access the information system needs to be addressed. The user needs to have the control over the information system. However, cryptography demands for converting the clandestine data into a non-recognizable cipher. Besides protection of data, the quantity of data that can be concealed in a single bearing medium is also very important.

Many algorithms are proposed in Cryptography, which are based on symmetric and asymmetric key. In asymmetric cryptography system, private and public keys are involved, which is based on mathematical functions rather than on substitution and permutation. Elliptic Curve Cryptography (ECC) is a public-key cryptography system, in which a key pair is selected so that the problem of deriving the private key from the corresponding public key is equivalent to solve a computational problem that is believed to be intractable.

In general, the keys are protected by user passwords, which will compromise the integrity of sensitive data due to poor selection of the password by the user. Combining biometric with cryptography could be the
solution by generating deterministic bit sequences for generating a reliable key. But it is essential to generate the key with minimum possibility of uncertainty due to poor image quality.

Biometrics is also used for diagnosing the human diseases. Especially the retinal fundus photograph is widely used in the diagnosis and treatment of various eye diseases such as diabetic retinopathy and glaucoma. The originality of the hidden protected retinal image is being tested in segmenting its OD region by using anatomical evidences considered relevant by the experts.

Enhancing the identification and authentication system using cryptography and biometrics are providing high assurance in terms of Information and Information System security. Thus the focus of this research work is to provide security and privacy to an information system by using multimodal biometrics, Genetic Algorithm and ECC. Genetic algorithm (GAs) is a class of optimization algorithm. Many problems can be solved using genetic algorithm through modeling a simplified version of genetic processes. The keys generated will always be purely random and non-repeating and hence increasing the strength of keys and security. In order to protect the biometric template and generating non-repeating key, Genetic algorithm based cryptographic key generation shall be used. ECC is one of the best cryptographic techniques, which could be the solution for generating a reliable secret key.

Thus the focus of this research work is to provide security to an information system by using multimodal biometrics and ECC and to protect biometric information by using information hiding techniques.
1.5.2 Objectives

The general objective of this research work is to address the security vulnerabilities such as substitution attack, tampering, masquerade attack, Trojan horse, overriding in a biometric system. The specific objectives are as follows:

i. To address the image quality issues by using decision rule based image fusion technique at sensor level. Thus issue related with FAR/FRR will be addressed.

ii. To investigate the uniqueness and privacy level of the ECC key by using single fingerprint image and multiple fingerprint images which will address the issue of intercepting during communication between storage and matching process. It does not use any score either to allow or deny. Thus the possibilities of Trojan horse attacks will get reduced.

iii. To secure the privacy of encryption key by using Genetic algorithm. It will address the issue of function creep. The use of single biometrics for multiple transactions with information system is an issue related with privacy. So the user identity may be cancelled and it can be substituted by newly generated biometric key by using GA while generating digital signatures by using ECC key. This technique will protect the biometric template. Therefore, the possibilities of substitution attack will get reduced.

iv. To address the issue such as tampering template and revealing diseases by introducing a novel information hiding technique such as steganography and to achieve Eminent Concealing
capacity through Adaptive Engrafting. Thus there is no possibility of masquerade attack.

v. To check the accuracy of stored biometric image in detecting the Glaucoma level of the secured retinal image by detecting the Optic Disc and Cup to Disc ratio based on LDA and Medial Axis Detection techniques.

1.6 ORGANIZATION OF CHAPTERS

The organizations of further chapters are described below:

Chapter -2: It deals about, how the image quality can be improved by introducing image fusion technique at sensor levels by using Decision Rule based Image Fusion (DRIF) technique. The test results of multi-instance and multiple biometric images from the dataset Biosecure DS2 and CASIA are recorded. The performance of DRIF technique is being analyzed with the measures of entropy and RMSE.

Chapter -3: In this chapter, a novel method for generating a secured key has been provided by using ECC and fingerprint image. The ECC keys have been generated by using CASIA dataset. It is found that a unique/irrevocable key has been generated for each user.

In chapter – 4, cancellable cryptography key generation from Multi-biometries and multi-modal biometrics have been tested by using appropriate biometric images. AAA architecture is proposed for protecting biometric based information system. GA has been used in the ECC key generation to enhance the security and privacy of the key.

In chapter -5, a noise based embedding technique by using salt and pepper noise is proposed for steganography which is entirely different from
the available techniques. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. In this work, the disease details of the patient shall not be revealed while it is stored in the database.

Chapter – 6 represents the detection of OD region and Cup-to-Disc Ratio by using LDA and Medial Axis Detection for detecting eye diseases. The CDR-F-score should lie between the ranges of 0-1. The DRIVE dataset has been used to test the performance of retrieved image from stego image. This system will be authenticated by using the One Time Pass word which is generated by using ECC. The accuracy of the retrieved information from the hidden image is tested through the F-score of the retinal image which is used to detect the eye diseases.